Cybersecurity Maturity Model Certification (CMMC)

August 20, 2020

LogRhythm Inc.

4780 Pearl East Circle

Boulder, CO 80301

(303) 413-8745

www.logrhythm.com

Phone Support (7am - 6pm, Monday-Friday)

Toll Free in North America (MT) +1-866-255-0862

Direct Dial in the Americas (MT) +1-720-407-3990

EMEA (GMT) +44 (0) 844 3245898

META (GMT+4) +971 8000-3570-4506

APAC (SGT) +65 31572044

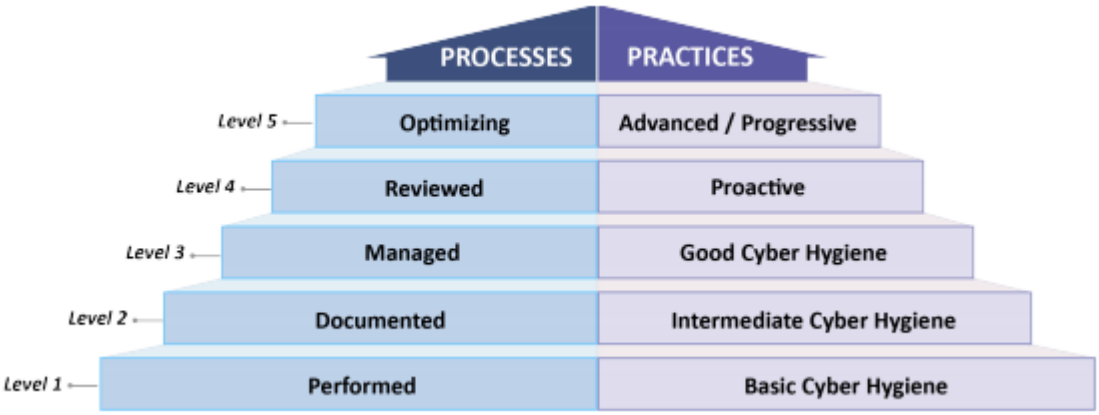
Table of Contents

Disclaimer: Organizations are not required as a matter of law to comply with this document, unless legislation, or a direction given under legislation or by some other lawful authority, compels them to comply. This document does not override any obligations imposed by legislation or law. Furthermore, if this document conflicts with legislation or law, the latter takes precedence.

The Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) developed the Cybersecurity Maturity Model Certification (CMMC) to assess and certify a company's maturity of cybersecurity practices and processes. The objective and mandate of the CMMC is that Department of Defense (DoD) contractors obtain third-party certification to ensure appropriate levels of cybersecurity practices are in place to meet a "basic cyber hygiene" and to protect controlled unclassified information (CUI) residing on partner systems. The cybersecurity practices and CUI protection already exist in regulations like Defense Federal Acquisition Regulation Supplement (DFARS) and NIST; however, those standards do not stipulate a third-party assessment to validate cybersecurity effectiveness and maturity, and to provide certification.

The CMMC builds upon established NIST special publications and DFAR regulations (with some additional sources, including UK Cyber Essentials and the Australia Cyber Security Centre Essential Eight maturity model). CMMC comprises 17 capability domains that include 171 practices or controls. The 17 capability domains are shown in the diagram below.

Organizations seeking certification will be certified at one of five levels that measure both technical control capacity and process maturity. The lowest level of the certification (Level 1) requires entities to adhere to a sub-set of the 171 controls (as prescribed by the (OUSD(A&S))) and to demonstrate they are performing the required processes. The five certification levels are briefly summarized below.



Each certification level requires increased process maturity and additional control practices. The DoD will assess which CMMC level is appropriate for a particular contract and deliver that level in contract Sections L and M of the corresponding request for proposal (RFP). The DoD will use the assessment as a “go/no go” evaluative determination. The level of certification required in each contract will depend upon the amount of CUI a company will handle or process. Independent third-party organizations (C3PAOs) will evaluate customers' environments for certification. A company will specify the level of the certification requested and will be certified at the appropriate CMMC level upon demonstrating the appropriate maturity to the satisfaction of the assessor and certifier.

All contractors within the Defense Industrial Base (DIB) are required to comply with some level of CMMC, depending upon the amount of unclassified networks that handle, process, and/or store federal contract information (FCI) or CUI and as stipulated by their specific contract. Companies that solely produce Commercial-Off-The-Shelf (COTS) products will not be required to obtain a certification. For more detailed information on CMMC, see the (OUSD(A&S)) website. The website provides the most current version of the CMMC regulation (1.02) and offers an overview powerpoint with background on the CMMC and details on the processes and practices for each certification level.

The LogRhythm platform enables your organization to meet many CMMC practices by collecting, managing, and analyzing log data. LogRhythm AI Engine (AIE) rules, alarms, reports, investigations, and general SIEM functionality also helps your organization satisfy certain control practices outlined by the CMMC.

LogRhythm understands that organizations may be at different points of compliance maturity, so the CMMC module gives organizations the flexibility to realize value at any point along that maturity scale. The CMMC module is focused on the control requirements traditionally used for best practice purposes. LogRhythm supports some CMMC recommendations and decreases the cost to meet others through pre-built content and functionality. Using advanced LogRhythm functionality such as NetMon, TrueIdentity, SysMon, Threat Research content, and Case Management may enhance pre-built content to better support an organization's compliance efforts.

IT environments consist of heterogeneous devices, systems, and applications—all reporting log data. Millions of individual log entries can be generated daily, if not hourly. The task of organizing this information can be overwhelming. Additional recommendations to analyze and report on log data render manual processes or homegrown remedies inadequate and cost prohibitive for many organizations. LogRhythm delivers log collection, archiving, and recovery across the entire IT infrastructure and automates the first level of log analysis. Log data is categorized, identified, and normalized for easy analysis and reporting. LogRhythm’s powerful alerting capabilities automatically identify the most critical issues and notify relevant personnel. The CMMC module and associated reporting package works out of the box with some level of customization available. Utilizing the CMMC module assists in building and maintaining a sound compliance program

CMMC – AI Engine Rules

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Abnormal Amount of Data Transferred	1230	This rule alerts whenever a significant change (400% increase or 75% decrease) in Bytes In or Bytes Out from a specific host.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	No	Operations : Warning	1. Include All Log Sources 2. Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Abnormal Origin Location	1208	First tracks geographic locations for logins. Afterwards, triggers when a new origin location is seen for a user.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	No	Security : Attack	1. Include All Log Sources 2. Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Account Deleted Rule	1367	This rule provides details of accounts that have been deleted	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	No	Audit: Account Deleted	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Account Disabled Rule	1369	This AIE Rule alerts on the occurrence of any access revoking to accounts.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	No	Audit: Access Revoked	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Account Enabled Rule	1368	This AIE Rule alerts on the occurrence of any access granting to accounts.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Yes	Audit: Access Granted	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Account Modification	1377	This AIE Rule creates a common event and provides detail around account modification activity.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	No	Audit : Account Modified	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Admin Password Modified	1326	User changes the password of a different privileged user account.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	No	Security: Suspicious	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Attack then External Connection	1211	An observed external attack or compromise followed by data leaving the system and going to the attacker.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	No	Security : Compromise	1. Include All Log Sources 2. Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Audit Logging Stopped Alarm	1328	This AIE Rule provides details on audit logging being stopped.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Yes	Audit : Configuration	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Auth After Numerous Failed Auths	1199	Multiple external unique login attempts are seen on the same impacted host within a short period of time, followed by a successful authentication.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	No	Security : Compromise	1. Include All Log Sources 2. Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Auth After Security Event	1200	An observed attack, compromise, or other security event followed by successful access or authentication from the attacking host.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	No	Security : Compromise	1. Include All Log Sources 2. Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Backup Failure Alarm	1236	More than 10 backup failure events are detected.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	Yes	Operations : Error	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Backup Information	1237	This AIE Rule creates events for information from backup software.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	No	Operations : Information	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Blacklist Location Auth	1204	Authentication success from a blacklisted location.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	No	Security : Compromise	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Blacklisted Account Alarm	1334	This AIE creates an alarm when a blacklisted account activity occurs within the environment. This requires the CCF: User Blacklist to be populated and updated regularly.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Yes	Audit : Other Audit Success	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Compromise Detected Alarm	1335	This AIE rule creates an event and alerts on potential compromises across the environment.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Yes	Security : Compromise	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Concurrent VPN from Multiple Locations	1205	Multiple VPN authentication successes from the same origin login are observed from different regions within a given time period (default 3 hours).	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	No	Security : Compromise	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Concurrent VPN from Same User	1373	This AIE Rule alerts on the occurrence of concurrent VPN from the same user.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	No	Security : Suspicious	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Config Change After Attack	1214	Attack event on a host followed by a configuration change made to that host within 3 minutes.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	No	Security : Compromise	1. Include All Log Sources 2. Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Config Change then Critical Error	1216	Configuration change followed by a critical error on the same host indicating an erroneous configuration, malicious intent or otherwise.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	No	Security : Compromise	1. Include All Log Sources 2. Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Config Deleted/ Disabled	1219	Configuration deleted or disabled within the organization infrastructure.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC. 2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC. 3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU. 3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM. 2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA. 2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP. 3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM. 2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM. 4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC. 3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC. 4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI. 1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI. 3.219, SI.4.221, SI.5.222, SI.5.223	No	Security : Compromise	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Config Modified	1221	Configuration modified within the organization infrastructure.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	No	Security : Compromise	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Corroborated Account Anomalies	1207	3 or more unique behavioral anomalies for a given user within a 3 hour period. This rule requires Rule IDs 285 - 289 be turned on. Use Case : An account has been compromised.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	No	Security : Compromise	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Corroborated Data Access Anomalies	1201	2 or more unique behavioral anomalies for data within a 3 hour periods. The alarm requires rule IDs 300-302 be turned on for this alarm to trigger.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	No	Security : Compromise	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Critical Event After Attack	1206	An external attack or compromise followed by a critical event on the same host. Action: This alarm can identify when an error message is generated as the result of a successful attack. This can be unexpected process termination or a hardware fail	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	No	Security : Compromise	1. Include All Log Sources 2. Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Critical/ PRD Envir Patch Failure Alarm	1212	This AIE rule creates an alert any time a patch fails to apply to the critical or production environments (entity structure).	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC. 2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC. 3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU. 3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM. 2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA. 2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP. 3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM. 2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM. 4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC. 3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC. 4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI. 1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI. 3.219, SI.4.221, SI.5.222, SI.5.223	Yes	Operations : Error	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Data Destruction	1202	Attack event followed by a FIM delete/modify event on the same host.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	No	Security : Compromise	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Data Exfiltration Observed	1193	External attack or compromise followed by data leaving the same system.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	No	Security : Compromise	1. Include All Log Sources 2. Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Data Loss Prevention	1232	This AIE Rule provides details of data generated by the LogRhythm Data Loss Defender or other data loss prevention solutions, when configured.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	No	Operations : Information	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Denial of Service Alert	1376	This AIE Rule alerts on the occurrence of any identified Denial of Service event.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Yes	Security: Denial Of Service	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Disabled Account Auth Success	1194	Recently disabled or deleted account authenticates or accesses resources on the network.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	No	Security : Compromise	1. Include All Log Sources 2. Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Distributed Brute Force	1203	A successful brute force authentication -- multiple failed authentication attempts from different external hosts to the same host using the same origin login, followed by an authentication success.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	No	Security : Compromise	1. Include All Log Sources 2. Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Early TLS/ SSL Alarm	1238	This AIE Rule alerts on the occurrence of any identified TLS LogRhythm Network Monitor event.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC. 2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC. 3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU. 3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM. 2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA. 2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP. 3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM. 2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM. 4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC. 3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC. 4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI. 1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI. 3.219, SI.4.221, SI.5.222, SI.5.223	Yes	Security : Activity	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Excessive Authentication Failures Rule	1370	This AIE Rule supports alerting on >10 authentication failures in 30 minutes (login failures). Match this threshold to your organization's specific authentication failure policies.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Yes	Audit : Authentication Failure	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: External Brute Force Auths	1197	Successful authentication after multiple failed attempts from different external origin hosts to the same impacted host.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	No	Security : Compromise	1. Include All Log Sources 2. Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: FIM Abnormal Activity	1233	This AIE Rule creates events for all abnormal file integrity monitoring activity.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	No	Security : Suspicious	1. Include All Log Sources 2. Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: FIM Add Activity	1234	This AIE Rule creates events for all file integrity monitoring add activity.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	No	Security : Activity	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: FIM Delete Activity Alarm	1235	This AIE Rule alarms on file integrity monitoring delete activity.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Yes	Security : Activity	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: FIM General Activity	1239	This rule creates an event fir file integrity monitoring activity including adds, deletes, modifies, group changes, owner changes, and permissions. The FIM log source can be established from LogRhythm's FIM or other FIM solutions.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC. 2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC. 3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU. 3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM. 2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA. 2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP. 3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM. 2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM. 4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC. 3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC. 4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI. 1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI. 3.219, SI.4.221, SI.5.222, SI.5.223	No	Operations : Information	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: FIM Information	1229	This AIE Rule creates events for general file integrity monitoring information.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	No	Operations : Information	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: GeoIP Blacklisted Region Activity	1241	This rule tracks activity associated with Blacklisted Regions (list).	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	No	Security : Suspicious	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: GeoIP General Activity	1240	This rule is designed to use with the Data Processor's GeoIP functionality, to represent general GeoIP activity.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	No	Security : Suspicious New: Operations : Information	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Large Outbound Transfer	1195	Single host is seen sending over 1GB of data within 30 minutes out of the network.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	No	Security : Compromise	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Linux sudo Privilege Escalation	1330	User not in the LogRhythm list "CCF: Privileged Accounts" and not in the local 'sudoers' file tries to use sudo on a Linux host.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	No	Security : Suspicious	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Local Account Created and Used	1196	An account is created on a host and then used shortly thereafter on the same host.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	No	Security : Compromise	1. Include All Log Sources 2. Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: LogRhythm Silent Log Source Error Alarm	1209	This AIE Rule creates an alert and provides information when a LogRhythm Log Source has not received logs from a critical or production server-system during the defined error period.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	Yes	Operations : Warning	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Malware Alarm	1217	This AIE Rule provides details on malware activity across the organization's environment where malware detection/prevention is applied.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	Yes	Security : Malware	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Misuse	1231	This AIE Rule provides details on misuse activity.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	No	Security : Misuse	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Multiple Account Passwords Modified by Admin	1327	An observed login by a user in the privileged user list followed by the change of two or more other account passwords.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	No	Security: Suspicious	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Non-Encrypted Protocol Alarm	1222	This investigation provides details of unencrypted applications being utilized within the critical and production systems or environments (entity structure).	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	Yes	Operations : Information	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Password Modified by Admin	1325	Privileged user changes the password of another account.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	No	Security: Suspicious	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Password Modified by Another User	1333	User changes the password of another account (not their own).	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	No	Audit: Account Modified	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Physical Access Rule	1498	This AIE rule creates an event for any access attempts (success or failure) to the defined physical security boundary.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	No	Audit: Access Failure	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: PRD Envir Config/Policy Change Alarm	1210	This AIE rule creates an alert any time a configuration or policy modification logs are received from a critical or production environment (entity structure).	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Yes	Audit : Policy	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: PRD Envir Signature Failure Alarm	1213	This AIE Rule creates an alert on signature update failures on critical or production environments (entity structure).	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	Yes	Operations : Error	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Priv Group Access Granted Alarm	1324	This AIE Rule provides details on access granted to privileged groups (administrators, dnsadmins, domain admins, enterprise admins, schema admins) within the organization infrastructure.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Yes	Audit: Access Granted	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Privilege Escalation After Attack Alarm	1329	Compromised host event followed by a new account created or account modified on the same host.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Yes	Security : Compromise	1. Include All Log Sources 2. Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Rogue Access Point Alarm	1220	This AIE Rule alerts on the occurrence of any rogue access point detection events against the organization's environment.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	Yes	Security: Suspicious	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Social Media Event	1242	This rule tracks social media activity, to help identify if private or personal data that should not be in transmission is present within the environment's traffic.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	No	Security : Suspicious	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Software Install Failure Alarm	1375	This alerts on failed and incomplete updates attempts to update or install in the organization.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	Yes	Audit: Configuration	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Software Install Rule	1371	This AIE rule creates an event and alerts on any software installation activity across the environment.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	No	Audit : Configuration	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Software Uninstall Failure Alarm	1374	This alerts on failed or interrupted software uninstallations.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	Yes	Audit: Configuration	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Software Uninstall Rule	1372	This AIE rule creates an event and alerts on any software uninstallation activity across the environment.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	No	Audit : Configuration	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Suspected Wireless Attack Alarm	1223	This AIE Rule creates an event and alerts on suspected wireless attacks (success/failure) against the boundary monitoring devices.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	Yes	Security: Attack	CCF: Wireless IDS

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Time Sync Error Alarm	1215	This AIE Rule creates an event and alerts for any time sync errors occurring on any Log Source.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	Yes	Operations: Warning	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Unknown User Account Alarm	1243	This rule identifies activity originating from unknown user accounts, based off of the CCF user lists.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Yes	Security : Suspicious	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Vulnerability Detected Alarm	1218	This AIE Rule alerts on the occurrence of vulnerabilities or suspicious events across the organization's environment.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Yes	Security: Vulnerability	Include All Log Sources

AI Engine Rules	Rule ID	Description	Control Support	Alarming	Classifications	Log Sources
CCF: Windows RunAs Privilege Escalation	1321	User not in the LogRhythm List "Privileged Users" chooses to Run a Windows program as an administrator using the "Run as administrator" option.	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	No	Security : Suspicious	1. Include All Log Sources 2. Include All Log Sources

CMMC – Investigations

> The Intelligent Indexing settings are recommendations. The default configuration is No.

Name	Description	Investigation ID	Control Support	Data Source	Classifications	Log Sources
CCF: Account Modification Inv	This investigation provides details around account modifications across the environment.	709	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Platform Manager(s)	Audit	All Available Log Sources

Name	Description	Investigation ID	Control Support	Data Source	Classifications	Log Sources
CCF: Applications Accessed By User Inv	This investigation provides information about user accessed applications.	689	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Data Processor(s)	Audit	All Available Log Sources

Name	Description	Investigation ID	Control Support	Data Source	Classifications	Log Sources
CCF: Audit Log Inv	This investigation provides details around potential control failures around auditing systems. This requires the configuration and enablement of the CCF: Audit Logging Stopped Alarm, CCF: Audit Log Cleared Alarm, CCF: Failed Audit Log Write Alarms.	701	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Platform Manager(s)	Audit	All Available Log Sources

Name	Description	Investigation ID	Control Support	Data Source	Classifications	Log Sources
CCF: Backup Activity Inv	This investigation provides detail around activity from backup events.	688	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	Data Processor(s)	Operations	All Available Log Sources
CCF: Compromises Detected Inv	This investigation provides a summary of detected compromises of security by Entity and Impacted Host.	690	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	LogMart(s)	Security	All Available Log Sources

Name	Description	Investigation ID	Control Support	Data Source	Classifications	Log Sources
CCF: Config/ Policy Change Inv	This investigation provides a summary of the occurrence of configuration or policy changes across critical and production environments (entity structure).	675	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU. 3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM. 2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA. 2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR. 2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR. 4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP. 2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM. 4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC. 1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC. 3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC. 4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI. 1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Data Processor(s)	Audit	All Available Log Sources

Name	Description	Investigation ID	Control Support	Data Source	Classifications	Log Sources
CCF: Critical Environment Error Inv	This investigation provides summary details around critical or error messages received from critical servers or systems (entity structure) to support change management procedures.	676	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	Platform Manager(s)	Operations	All Available Log Sources

Name	Description	Investigation ID	Control Support	Data Source	Classifications	Log Sources
CCF: Deleted Account Inv	This investigation provides detailed information when any new accounts are deleted across any logged environments (entity structure).	706	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Platform Manager(s)	Audit	All Available Log Sources

Name	Description	Investigation ID	Control Support	Data Source	Classifications	Log Sources
CCF: Denial of Service Inv	This investigation provides details of detected denial of service attempts.	707	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	Data Processor(s)	Security	All Available Log Sources

Name	Description	Investigation ID	Control Support	Data Source	Classifications	Log Sources
CCF: Disabled Account Inv	This investigation provides detailed information when any new accounts are revoked (disabled) across any logged environments (entity structure).	705	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Platform Manager(s)	Audit	All Available Log Sources

Name	Description	Investigation ID	Control Support	Data Source	Classifications	Log Sources
CCF: Enabled Account Inv	This investigation provides detailed information when any new accounts are granted (enabled) across any logged environments (entity structure).	704	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	Platform Manager(s)	Audit	All Available Log Sources

Name	Description	Investigation ID	Control Support	Data Source	Classifications	Log Sources
CCF: Excessive Authentication Failure Inv	This investigation provides detailed information around excessive user account authentication failures (>10 authentication failures in 30 minutes) across any logged environments (entity structure).	708	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Platform Manager(s)	Security	All Available Log Sources

Name	Description	Investigation ID	Control Support	Data Source	Classifications	Log Sources
CCF: GeoIP Inv	This report summarizes GeoIP activity that is associated with AI Engine GeoIP rules, in the CCF compliance automation suite.	696	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Platform Manager(s)	Security	All Available Log Sources

Name	Description	Investigation ID	Control Support	Data Source	Classifications	Log Sources
CCF: Host Access Granted And Revoked Inv	This investigation details all access granted and revoked for production systems.	691	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Data Processor(s)	Audit	All Available Log Sources

Name	Description	Investigation ID	Control Support	Data Source	Classifications	Log Sources
CCF: LogRhythm Data Loss Defender Log Inv	This investigation provides information on data generated by the LogRhythm Data Loss Defender. Data is grouped by Entity, Impacted Host, Common Event, and Object with a count of how many times that condition has been experienced within the investigation period.	692	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	Data Processor(s)	Audit	All Available Log Sources

Name	Description	Investigation ID	Control Support	Data Source	Classifications	Log Sources
CCF: Malware Detected Inv	This investigation provides a summary of malware activity by entity and impacted host within the organization's critical and production environments (entity structure).	677	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	Platform Manager(s)	Security	All Available Log Sources
CCF: Object Access Inv	This investigation summarizes object access by Impacted Host.	693	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	Data Processor(s)	Audit	All Available Log Sources

Name	Description	Investigation ID	Control Support	Data Source	Classifications	Log Sources
CCF: Password Modification Inv	This investigation provides detail around password modification to accounts within the environment.	702	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	Platform Manager(s)	Audit	All Available Log Sources

Name	Description	Investigation ID	Control Support	Data Source	Classifications	Log Sources
CCF: Patch Activity Inv	This investigation provides a summary of applied patches grouped by Origin Host. It can demonstrate that all system components have the latest security patches installed.	678	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Data Processor(s)	Security	All Available Log Sources

Name	Description	Investigation ID	Control Support	Data Source	Classifications	Log Sources
CCF: Physical Access Inv	This investigation summarizes physical door access/ authentication success and failures within the organization's physical security perimeter.	679	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM. 2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA. 2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR. 2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR. 5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM. 4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC. 1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC. 3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC. 4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI. 2.216, SI.2.217, SI.3.218, SI.5.223	Platform Manager(s)	Audit	All Available Log Sources

Name	Description	Investigation ID	Control Support	Data Source	Classifications	Log Sources
CCF: Privileged Account Escalation Inv	This investigation provides detail around privileged access escalation within a Linux and Windows OS. This requires configuration and enablement of CCF: Windows RunAs Privilege Escalation & CCF: Linux sudo Privilege Escalation AIE rules.	700	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Platform Manager(s)	Security	All Available Log Sources

Name	Description	Investigation ID	Control Support	Data Source	Classifications	Log Sources
CCF: Privileged Account Modification Inv	This investigation provides details around modifications made to privileged accounts within the environment. This investigation requires the CCF: Privileged Accounts (user list) to be established and updated periodically.	703	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	Data Processor(s)	Audit	All Available Log Sources

Name	Description	Investigation ID	Control Support	Data Source	Classifications	Log Sources
CCF: Rogue Access Point Inv	This investigation provides a summary of all detected rogue wireless access points by Impacted Host across critical, production, and online banking environments (entity structure).	680	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Platform Manager(s)	Security	All Available Log Sources

Name	Description	Investigation ID	Control Support	Data Source	Classifications	Log Sources
CCF: Signature Activity Inv	This investigation provides summary information on signature update activity across critical and production environments (entity structure).	681	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	LogMart(s)	Operations	All Available Log Sources
CCF: Social Media Inv	Summarizes the top URLs related to Social Media activity.	695	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	Platform Manager(s)	Audit	All Available Log Sources

Name	Description	Investigation ID	Control Support	Data Source	Classifications	Log Sources
CCF: Suspected Wireless Attack Inv	This investigation provides information on suspected wireless attacks at the internal boundary including the type of attack and impacted (targeted) host and application (if applicable). This is based on Critical and Production environments (can be defined with entity structure).	682	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	Platform Manager(s)	Security	All Available Log Sources

Name	Description	Investigation ID	Control Support	Data Source	Classifications	Log Sources
CCF: Suspicious Users Inv	This investigation lists all users generating suspicious activity ordered by the number of events detected highest to lowest.	685	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Data Processor(s)	Security	All Available Log Sources

Name	Description	Investigation ID	Control Support	Data Source	Classifications	Log Sources
CCF: Time Sync Error Inv	This investigation provides a summary of time sync errors occurring within critical and production environments (can be defined with entity structure).	683	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Platform Manager(s)	Audit	All Available Log Sources

Name	Description	Investigation ID	Control Support	Data Source	Classifications	Log Sources
CCF: Unknown User Account Inv	This investigation provides detail of activity from unknown user accounts, based off of CCF user lists.	697	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Data Processor(s)	Security	All Available Log Sources

Name	Description	Investigation ID	Control Support	Data Source	Classifications	Log Sources
CCF: Use Of Non-Encrypted Protocols Inv	This investigation lists any use of non-encrypted protocols.	686	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	LogMart(s)	Audit	All Available Log Sources

Name	Description	Investigation ID	Control Support	Data Source	Classifications	Log Sources
CCF: User Misuse Inv	This investigation summarizes detected misuse by user.	687	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Platform Manager(s)	Security	All Available Log Sources

Name	Description	Investigation ID	Control Support	Data Source	Classifications	Log Sources
CCF: User Object Access Inv	This investigation summarizes successful object access activity by user.	694	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	Data Processor(s)	Audit	All Available Log Sources
CCF: Vulnerability Detected Inv	This investigation provides a summary of potential vulnerabilities detected across the critical and production environments (can be defined with entity structure).	684	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	Platform Manager(s)	Security	All Available Log Sources

CMMC – Reports and Reporting Packages

The Intelligent Indexing settings are recommendations. The default configuration is No.

Summary Reports

Report Name	Report ID	Control Support	Data Source	Log Sources
CCF: Access Failure Summary	2089	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Platform Manager	All Available Log Sources

Report Name	Report ID	Control Support	Data Source	Log Sources
CCF: Access Success Summary	2091	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Platform Manager	All Available Log Sources
CCF: Account Disabled Summary	2084	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	LogMart	All Available Log Sources

Report Name	Report ID	Control Support	Data Source	Log Sources
CCF: Account Enabled Summary	2085	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Platform Manager	All Available Log Sources
CCF: Account Modification Summary	2092	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Platform Manager	All Available Log Sources

Report Name	Report ID	Control Support	Data Source	Log Sources
CCF: Applications Accessed By User Summary	2063	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	Data Processor(s)	All Available Log Sources
CCF: Audit Log Summary	2076	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	Platform Manager	All Available Log Sources

Report Name	Report ID	Control Support	Data Source	Log Sources
CCF: Auth Failure Summary	2088	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Platform Manager	All Available Log Sources
CCF: Auth Success Summary	2090	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Platform Manager	All Available Log Sources

Report Name	Report ID	Control Support	Data Source	Log Sources
CCF: Backup Activity Summary	2062	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	Data Processor(s)	All Available Log Sources
CCF: Compromises Detected Summary	2064	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	LogMart	All Available Log Sources

Report Name	Report ID	Control Support	Data Source	Log Sources
CCF: Config/Policy Change Summary	2049	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	LogMart	All Available Log Sources
CCF: Critical Environment Error Summary	2050	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	Platform Manager	All Available Log Sources

Report Name	Report ID	Control Support	Data Source	Log Sources
CCF: GeoIP Summary	2069	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Platform Manager	All Available Log Sources
CCF: LogRhythm Data Loss Defender Log Summary	2066	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	LogMart	All Available Log Sources

Report Name	Report ID	Control Support	Data Source	Log Sources
CCF: Malware Detected Summary	2051	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Platform Manager	All Available Log Sources
CCF: Object Access Summary	2067	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Data Processor(s)	All Available Log Sources

Report Name	Report ID	Control Support	Data Source	Log Sources
CCF: Patch Activity Summary	2052	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Data Processor(s)	All Available Log Sources
CCF: Physical Access Summary	2053	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Platform Manager	All Available Log Sources

Report Name	Report ID	Control Support	Data Source	Log Sources
CCF: Priv Account Management Activity Summary	2080	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Data Processor(s)	All Available Log Sources
CCF: Priv Authentication Activity Summary	2079	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Platform Manager	All Available Log Sources

Report Name	Report ID	Control Support	Data Source	Log Sources
CCF: Rogue Access Point Summary	2054	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Platform Manager	All Available Log Sources
CCF: Signature Activity Summary	2055	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	LogMart	All Available Log Sources

Report Name	Report ID	Control Support	Data Source	Log Sources
CCF: Social Media Summary	2070	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	Platform Manager	All Available Log Sources
CCF: Suspected Wireless Attack Summary	2056	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	Platform Manager	All Available Log Sources

Report Name	Report ID	Control Support	Data Source	Log Sources
CCF: Term Account Activity Summary	2087	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Data Processor(s)	All Available Log Sources
CCF: Time Sync Error Summary	2057	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Platform Manager	All Available Log Sources

Report Name	Report ID	Control Support	Data Source	Log Sources
CCF: Top Suspicious Users	2059	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Data Processor(s)	All Available Log Sources
CCF: Use Of Non-Encrypted Protocols Summary	2060	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	LogMart	All Available Log Sources

Report Name	Report ID	Control Support	Data Source	Log Sources
CCF: User Misuse Summary	2061	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.5.223	Platform Manager	All Available Log Sources
CCF: User Object Access Summary	2068	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Data Processor(s)	All Available Log Sources

Report Name	Report ID	Control Support	Data Source	Log Sources
CCF: User Priv Escalation (SU & SUDO) Summary	2078	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Data Processor(s)	All Available Log Sources
CCF: User Priv Escalation (Windows) Summary	2077	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Data Processor(s)	All Available Log Sources

Report Name	Report ID	Control Support	Data Source	Log Sources
CCF: Vulnerability Detected Summary	2058	AC.1.001, AC.1.002, AC.1.003, AC.2.006, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.014, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AM.4.226, AU.2.041, AU.2.042, AU.2.043, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.063, CM.2.064, CM.2.065, CM.3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.2.081, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR.2.093, IR.2.094, IR.2.096, IR.2.097, IR.3.098, IR.3.099, IR.4.100, IR.4.101, IR.5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MA.2.114, MP.2.119, MP.2.120, MP.2.121, MP.3.123, MP.3.124, PS.2.128, PE.1.131, PE.1.132, PE.1.133, PE.1.134, PE.2.135, RE.2.137, RE.2.138, RE.3.139, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.177, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.3.191, SC.3.192, SC.4.197, SC.4.228, SC.4.199, SC.5.198, SC.5.230, SI.1.210, SI.1.211, SI.1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.222, SI.5.223	Platform Manager	All Available Log Sources

Detailed Reports

Report Name	Report Description	Augmented Requirements	Data Source	Intelligent Indexing	Classification	Log Sources	Report ID
CCF: Host Access Granted And Revoked Detail	This report details all access granted and revoked for production systems.	AC.1.001, AC.1.002, AC.1.003, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AU.2.041, AU.2.042, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.064, CM.2.065, CM. 3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA. 2.080, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR. 2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR. 5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP. 2.120, PS.2.128, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI. 1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.223	Data Processor(s)	Yes	Audit	All Available Log Sources	2065

Report Name	Report Description	Augmented Requirements	Data Source	Intelligent Indexing	Classification	Log Sources	Report ID
CCF: Unknown User Account Detail	This report provides detail of activity from unknown user accounts, based off CCF user lists.	AC.1.001, AC.1.002, AC.1.003, AC.2.007, AC.2.008, AC.2.009, AC.2.010, AC.2.011, AC.2.013, AC.2.015, AC.2.016, AC.3.018, AC.3.012, AC.3.020, AC.3.021, AC.3.022, AC.4.023, AC.4.032, AC.5.024, AM.3.036, AU.2.041, AU.2.042, AU.2.044, AU.3.045, AU.3.046, AU.3.048, AU.3.050, AU.3.051, AU.3.052, AU.4.053, AU.4.054, AU.5.055, CM.2.062, CM.2.064, CM.2.065, CM. 3.069, CM.5.074, IA.1.076, IA.1.077, IA.2.078, IA.2.079, IA. 2.080, IA.3.083, IA.3.084, IA.3.085, IA.3.086, IR.2.092, IR. 2.093, IR.2.094, IR.2.096, IR.3.098, IR.3.099, IR.4.101, IR. 5.106, IR.5.102, IR.5.108, MA.2.111, MA.2.112, MP.2.119, MP. 2.120, PS.2.128, RE.5.140, RM.2.141, RM.2.143, RM.3.144, RM.4.149, RM.4.150, RM.4.151, RM.5.152, CA.2.158, CA.3.161, SA.4.171, SA.4.173, SC.1.175, SC.1.176, SC.2.178, SC.2.179, SC.3.180, SC.3.181, SC.3.182, SC.3.183, SC.3.184, SC.3.185, SC.3.188, SC.3.190, SC.4.197, SC.4.228, SI.1.210, SI.1.211, SI. 1.212, SI.1.213, SI.2.214, SI.2.216, SI.2.217, SI.3.218, SI.3.219, SI.4.221, SI.5.223	Data Processor(s)	Yes	Security	All Available Log Sources	2071

Reporting Packages

Report Package Name	Report Package Description	Report Package ID
CCF: Daily IT Operations Reporting Package	This Reporting Package is a template to deliver pertinent content for IT Operations on a daily basis.	89
CCF: Daily IT Security Reporting Package	This Reporting Package is a template to deliver pertinent content for IT Security on a daily basis.	90
CCF: Executive Reporting Package	This reporting package is a template to deliver pertinent content for Executives on a monthly basis.	87
CCF: Weekly Audit Reporting Package	This Reporting Package is a template to deliver pertinent content for Internal and/or External Audit groups on a weekly basis	88

CMMC – Requirements

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
AC.1.002	CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: Disabled Account Auth Success CCF: GeoIP General Activity CCF: Corroborated Data Access Anomalies CCF: GeoIP Blacklisted Region Activity CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Abnormal Origin Location CCF: Auth After Security Event CCF: Large Outbound Transfer CCF: Data Exfiltration Observed CCF: Data Destruction CCF: Corroborated Account Anomalies CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Excessive	CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Blacklisted Account Alarm CCF: Privilege Escalation After Attack Alarm CCF: FIM Delete Activity Alarm CCF: Early TLS/SSL Alarm CCF: Non-Encrypted Protocol Alarm	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: Suspicious Users Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: User Object Access Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Audit Log Inv CCF: Object Access Inv CCF: Password Modification Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Rogue Access Point Inv CCF: User Misuse Inv	CCF: Physical Access Summary CCF: Applications Accessed By User Summary CCF: Top Suspicious Users CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: User Object Access Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Term Account Activity Summary CCF: Account Deleted Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Audit Log Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Modification	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Password Modified by Admin CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified CCF: Password Modified by Another User CCF: Auth After Numerous Failed Auths CCF: Abnormal Amount of Data Transferred CCF: Misuse			Summary CCF: Object Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: User Misuse Summary CCF: Rogue Access Point Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
AC.1.003	CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: FIM Information CCF: Data Destruction CCF: Data Loss Prevention CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies CCF: Config Change After Attack CCF: Abnormal Amount of Data Transferred CCF: Large Outbound Transfer CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Social Media Event CCF: Disabled Account Auth Success CCF: Corroborated Account Anomalies CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User	CCF: LogRhythm Silent Log Source Error Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Early TLS/SSL Alarm CCF: Non-Encrypted Protocol Alarm CCF: Blacklisted Account Alarm CCF: Rogue Access Point Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: FIM Delete Activity Alarm CCF: Privilege Escalation After Attack Alarm CCF: Suspected Wireless Attack Alarm	CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: User Object Access Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Escalation Inv CCF: Privileged Account Modification Inv CCF: Audit Log Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Object Access Inv CCF: Suspected Wireless Attack Inv CCF: Password Modification Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: User Object Access Summary CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Rogue Access Point Summary CCF: Audit Log Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event			Summary CCF: Term Account Activity Summary CCF: Object Access Summary CCF: Suspected Wireless Attack Summary	
AC.1.004					
AC.2.005					

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
AC.2.006	CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: FIM Information CCF: Large Outbound Transfer CCF: Data Exfiltration Observed CCF: Data Destruction CCF: Data Loss Prevention CCF: Corroborated Data Access Anomalies CCF: Abnormal Amount of Data Transferred CCF: Large Outbound Transfer	CCF: FIM Delete Activity Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm	CCF: User Object Access Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Audit Log Inv CCF: Object Access Inv	CCF: User Object Access Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Audit Log Summary CCF: Object Access Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
AC.2.007	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Corroborated Data Access Anomalies CCF: Social Media Event CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Data Loss Prevention CCF: Config Modified CCF: Large Outbound Transfer CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Config Deleted/ Disabled CCF: Critical Event After	CCF: FIM Delete Activity Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Rogue Access Point Alarm CCF: Blacklisted Account Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm CCF: Suspected Wireless Attack Alarm CCF: Backup Failure Alarm	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Social Media Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Patch Activity Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Audit Log Inv CCF: Suspected Wireless Attack Inv CCF: Backup Activity Inv CCF: Password Modification Inv	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Social Media Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Patch Activity Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Attack CCF: Software Install CCF: Software Uninstall CCF: Corroborated Account Anomalies CCF: Disabled Account Auth Success CCF: Abnormal Origin Location CCF: Auth After Security Event CCF: Password Modified by Admin CCF: Admin Password Modified CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Backup Information CCF: Excessive Authentication Failure Rule CCF: Attack then External Connection CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event			CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Audit Log Summary CCF: Suspected Wireless Attack Summary CCF: Backup Activity Summary CCF: Rogue Access Point Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
AC.2.008	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Corroborated Data Access Anomalies CCF: Social Media Event CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Data Loss Prevention CCF: Config Modified CCF: Large Outbound Transfer CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Config Deleted/ Disabled CCF: Critical Event After	CCF: FIM Delete Activity Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Rogue Access Point Alarm CCF: Blacklisted Account Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm CCF: Suspected Wireless Attack Alarm CCF: Backup Failure Alarm	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Social Media Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Patch Activity Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Audit Log Inv CCF: Suspected Wireless Attack Inv CCF: Backup Activity Inv CCF: Password Modification Inv	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Social Media Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Patch Activity Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Attack CCF: Software Install CCF: Software Uninstall CCF: Corroborated Account Anomalies CCF: Disabled Account Auth Success CCF: Abnormal Origin Location CCF: Auth After Security Event CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Admin Password Modified CCF: Multiple Account Passwords Modified by Admin CCF: Backup Information CCF: Excessive Authentication Failure Rule CCF: Attack then External Connection CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event			CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Audit Log Summary CCF: Suspected Wireless Attack Summary CCF: Backup Activity Summary CCF: Rogue Access Point Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
AC.2.009	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Corroborated Data Access Anomalies CCF: Social Media Event CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Data Loss Prevention CCF: Config Modified CCF: Large Outbound Transfer CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Config Deleted/ Disabled CCF: Critical Event After	CCF: FIM Delete Activity Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Rogue Access Point Alarm CCF: Blacklisted Account Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm CCF: Suspected Wireless Attack Alarm CCF: Backup Failure Alarm	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Social Media Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Patch Activity Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Account Modification Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Audit Log Inv	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Social Media Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Patch Activity Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Attack CCF: Software Install CCF: Software Uninstall CCF: Corroborated Account Anomalies CCF: Disabled Account Auth Success CCF: Abnormal Origin Location CCF: Auth After Security Event CCF: Password Modified by Admin CCF: Admin Password Modified CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Backup Information CCF: Account Modification CCF: Attack then External Connection CCF: Concurrent VPN from Same User CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event		CCF: Suspected Wireless Attack Inv CCF: Backup Activity Inv CCF: Password Modification Inv	CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Audit Log Summary CCF: Suspected Wireless Attack Summary CCF: Backup Activity Summary CCF: Rogue Access Point Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
AC.2.010	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Corroborated Data Access Anomalies CCF: Social Media Event CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: FIM Abnormal Activity CCF: FIM Add Activity CCF: FIM General Activity CCF: Data Loss Prevention CCF: Config Modified CCF: Large Outbound Transfer CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Config Change After Attack CCF: Config Change then Critical Error	CCF: FIM Delete Activity Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Rogue Access Point Alarm CCF: Blacklisted Account Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm CCF: Suspected Wireless Attack Alarm CCF: Backup Failure Alarm	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Social Media Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Patch Activity Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Audit Log Inv CCF: Suspected Wireless Attack Inv CCF: Backup Activity Inv CCF: Password Modification Inv	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Social Media Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Patch Activity Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Config Deleted/ Disabled CCF: Critical Event After Attack CCF: Software Install CCF: Software Uninstall CCF: Corroborated Account Anomalies CCF: Disabled Account Auth Success CCF: Abnormal Origin Location CCF: Auth After Security Event CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Admin Password Modified CCF: Attack then External Connection CCF: Multiple Account Passwords Modified by Admin CCF: Backup Information CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User			CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Audit Log Summary CCF: Suspected Wireless Attack Summary CCF: Backup Activity Summary CCF: Rogue Access Point Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event				
AC.2.011	CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: FIM Information CCF: Data Destruction CCF: Data Loss Prevention CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies CCF: Config Change After Attack CCF: Abnormal Amount of Data Transferred CCF: Large Outbound Transfer CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Social Media Event CCF: Disabled Account Auth Success CCF: Corroborated Account Anomalies CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth	CCF: LogRhythm Silent Log Source Error Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Early TLS/SSL Alarm CCF: Non-Encrypted Protocol Alarm CCF: Blacklisted Account Alarm CCF: Rogue Access Point Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: FIM Delete Activity Alarm CCF: Privilege Escalation After Attack Alarm CCF: Suspected Wireless Attack Alarm	CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: User Object Access Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Escalation Inv CCF: Privileged Account Modification Inv CCF: Audit Log Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Object Access Inv CCF: Suspected Wireless Attack Inv CCF: Password Modification Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: User Object Access Summary CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Rogue Access Point Summary CCF: Audit Log Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified CCF: Password Modified by Another User CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event			Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Object Access Summary CCF: Suspected Wireless Attack Summary	
AC.2.013	CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: FIM Information CCF: Data Destruction CCF: Data Loss Prevention CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies	CCF: FIM Delete Activity Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared	CCF: Use Of Non-Encrypted Protocols Inv CCF: Object Access Inv CCF: Audit Log Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Config/Policy Change Inv CCF: Critical Environment Error Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Object Access Summary CCF: User Object Access Summary CCF: Audit Log Summary CCF: Config/Policy Change Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Backup Information CCF: Abnormal Amount of Data Transferred CCF: Large Outbound Transfer CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Social Media Event CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Config Deleted/ Disabled CCF: Disabled Account Auth Success CCF: Corroborated Account Anomalies CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User	Alarm CCF: Failed Audit Log Write Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Backup Failure Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Signature Activity Inv CCF: Patch Activity Inv CCF: Backup Activity Inv CCF: Time Sync Error Inv CCF: Social Media Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Social Media Summary CCF: Applications Accessed By User Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified			CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Backup Activity Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
AC.2.015	CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: FIM Information CCF: Data Destruction CCF: Data Loss Prevention CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies CCF: Config Change After Attack CCF: Abnormal Amount of Data Transferred CCF: Large Outbound Transfer CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Social Media Event CCF: Disabled Account Auth Success CCF: Corroborated Account Anomalies CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User	CCF: LogRhythm Silent Log Source Error Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Early TLS/SSL Alarm CCF: Non-Encrypted Protocol Alarm CCF: Blacklisted Account Alarm CCF: Rogue Access Point Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: FIM Delete Activity Alarm CCF: Privilege Escalation After Attack Alarm CCF: Suspected Wireless Attack Alarm	CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: User Object Access Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Escalation Inv CCF: Privileged Account Modification Inv CCF: Audit Log Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Object Access Inv CCF: Suspected Wireless Attack Inv CCF: Password Modification Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: User Object Access Summary CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Rogue Access Point Summary CCF: Audit Log Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified CCF: Password Modified by Another User CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event			Summary CCF: Term Account Activity Summary CCF: Object Access Summary CCF: Suspected Wireless Attack Summary	
AC.2.016	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Config Change After Attack CCF: Config Change then	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Backup Failure Alarm CCF: LogRhythm Silent Log	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Critical Error CCF: Critical Event After Attack CCF: Config Deleted/ Disabled CCF: Social Media Event CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Backup Information CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies CCF: Large Outbound Transfer CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Disabled Account Auth Success CCF: Corroborated Account Anomalies CCF: Corroborated Account Anomalies CCF: Disabled Account Auth Success CCF: Config Modified CCF: Excessive Authentication Failure Rule CCF: Account Modification	Source Error Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm	Inv CCF: GeoIP Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Social Media Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Patch Activity Inv CCF: Time Sync Error Inv CCF: Backup Activity Inv CCF: Audit Log Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Backup Activity Summary CCF: Audit Log Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Software Install CCF: Software Uninstall CCF: Account Deleted Rule CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified CCF: Password Modified by Another User			CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	
AC.3.017					

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
AC.3.018	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Corroborated Data Access Anomalies CCF: Social Media Event CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Data Loss Prevention CCF: Config Modified CCF: Large Outbound Transfer CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Config Deleted/ Disabled CCF: Critical Event After	CCF: FIM Delete Activity Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Rogue Access Point Alarm CCF: Blacklisted Account Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm CCF: Suspected Wireless Attack Alarm CCF: Backup Failure Alarm	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Social Media Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Patch Activity Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Audit Log Inv CCF: Suspected Wireless Attack Inv CCF: Backup Activity Inv CCF: Password Modification Inv	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Social Media Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Patch Activity Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Attack CCF: Software Install CCF: Software Uninstall CCF: Corroborated Account Anomalies CCF: Disabled Account Auth Success CCF: Abnormal Origin Location CCF: Auth After Security Event CCF: Password Modified by Admin CCF: Admin Password Modified CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Backup Information CCF: Excessive Authentication Failure Rule CCF: Attack then External Connection CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event			CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Audit Log Summary CCF: Suspected Wireless Attack Summary CCF: Backup Activity Summary CCF: Rogue Access Point Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
AC.3.019					
AC.3.012	CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: FIM Information CCF: Data Destruction CCF: Data Loss Prevention CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies CCF: Config Change After Attack CCF: Abnormal Amount of Data Transferred CCF: Large Outbound Transfer CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Social Media Event CCF: Disabled Account Auth Success CCF: Corroborated Account Anomalies CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Concurrent VPN from Multiple Locations	CCF: LogRhythm Silent Log Source Error Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Early TLS/SSL Alarm CCF: Non-Encrypted Protocol Alarm CCF: Blacklisted Account Alarm CCF: Rogue Access Point Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: FIM Delete Activity Alarm CCF: Privilege Escalation After Attack Alarm CCF: Suspected Wireless Attack Alarm	CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: User Object Access Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Escalation Inv CCF: Privileged Account Modification Inv CCF: Audit Log Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Object Access Inv CCF: Suspected Wireless Attack Inv CCF: Password Modification Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: User Object Access Summary CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Rogue Access Point Summary CCF: Audit Log Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Concurrent VPN from Same User CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified CCF: Password Modified by Another User CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event			Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Object Access Summary CCF: Suspected Wireless Attack Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
AC.3.020	CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: FIM Information CCF: Data Destruction CCF: Data Loss Prevention CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies CCF: Config Change After Attack CCF: Abnormal Amount of Data Transferred CCF: Large Outbound Transfer CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Social Media Event CCF: Disabled Account Auth Success CCF: Corroborated Account Anomalies CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User	CCF: LogRhythm Silent Log Source Error Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Early TLS/SSL Alarm CCF: Non-Encrypted Protocol Alarm CCF: Blacklisted Account Alarm CCF: Rogue Access Point Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: FIM Delete Activity Alarm CCF: Privilege Escalation After Attack Alarm CCF: Suspected Wireless Attack Alarm	CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: User Object Access Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Escalation Inv CCF: Privileged Account Modification Inv CCF: Audit Log Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Object Access Inv CCF: Suspected Wireless Attack Inv CCF: Password Modification Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: User Object Access Summary CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Rogue Access Point Summary CCF: Audit Log Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified CCF: Password Modified by Another User CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event			Summary CCF: Term Account Activity Summary CCF: Object Access Summary CCF: Suspected Wireless Attack Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
AC.3.014	CCF: FIM Abnormal Activity CCF: FIM Add Activity CCF: FIM General Activity CCF: FIM Information CCF: Data Loss Prevention CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Large Outbound Transfer CCF: Abnormal Amount of Data Transferred CCF: Corroborated Data Access Anomalies CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Config Deleted/ Disabled CCF: Critical Event After Attack CCF: Attack then External Connection	CCF: FIM Delete Activity Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: PRD Envir Config/Policy Change Alarm	CCF: Use Of Non-Encrypted Protocols Inv CCF: Audit Log Inv CCF: Config/Policy Change Inv CCF: LogRhythm Data Loss Defender Log Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: Audit Log Summary CCF: Config/Policy Change Summary CCF: LogRhythm Data Loss Defender Log Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
AC.3.021	CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: FIM Information CCF: Data Destruction CCF: Data Loss Prevention CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies CCF: Config Change After Attack CCF: Abnormal Amount of Data Transferred CCF: Large Outbound Transfer CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Social Media Event CCF: Disabled Account Auth Success CCF: Corroborated Account Anomalies CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User	CCF: LogRhythm Silent Log Source Error Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Early TLS/SSL Alarm CCF: Non-Encrypted Protocol Alarm CCF: Blacklisted Account Alarm CCF: Rogue Access Point Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: FIM Delete Activity Alarm CCF: Privilege Escalation After Attack Alarm CCF: Suspected Wireless Attack Alarm	CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: User Object Access Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Escalation Inv CCF: Privileged Account Modification Inv CCF: Audit Log Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Object Access Inv CCF: Suspected Wireless Attack Inv CCF: Password Modification Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: User Object Access Summary CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Rogue Access Point Summary CCF: Audit Log Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified CCF: Password Modified by Another User CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event			Summary CCF: Term Account Activity Summary CCF: Object Access Summary CCF: Suspected Wireless Attack Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
AC.3.022	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Social Media Event CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Blacklist Location Auth CCF: Corroborated Account Anomalies CCF: Data Destruction CCF: Corroborated Data Access Anomalies CCF: Data Exfiltration Observed CCF: Abnormal Origin Location CCF: Large Outbound Transfer CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: FIM Delete Activity Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Blacklisted Account Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: User Object Access Inv CCF: Object Access Inv CCF: GeoIP Inv CCF: Social Media Inv CCF: Audit Log Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Host Access Granted And Revoked Inv CCF: Unknown User Account Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Password Modification Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: User Object Access Summary CCF: GeoIP Summary CCF: Social Media Summary CCF: Audit Log Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Object Access Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Concurrent VPN from Same User CCF: Password Modified by Admin CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified CCF: Password Modified by Another User CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event				

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
AC.4.023	CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Social Media Event CCF: Blacklist Location Auth CCF: FIM Abnormal Activity CCF: FIM Information CCF: FIM Add Activity CCF: FIM General Activity CCF: Data Loss Prevention CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Large Outbound Transfer CCF: Abnormal Amount of Data Transferred CCF: Corroborated Data Access Anomalies CCF: Config Modified CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Config Deleted/ Disabled CCF: Critical Event After Attack CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Corroborated Account Anomalies CCF: Software Install CCF: Software Uninstall	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Audit Logging Stopped Alarm CCF: Compromise Detected Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: FIM Delete Activity Alarm CCF: Denial Of Service Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm	CCF: Use Of Non-Encrypted Protocols Inv CCF: GeoIP Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Social Media Inv CCF: Audit Log Inv CCF: Compromises Detected Inv CCF: User Object Access Inv CCF: Patch Activity Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Host Access Granted And Revoked Inv CCF: Unknown User Account Inv CCF: Object Access Inv CCF: Password Modification Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: GeoIP Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Audit Log Summary CCF: User Object Access Summary CCF: Patch Activity Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Auth Failure Summary CCF: Access Failure Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified CCF: Local Account Created and Used	CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm		CCF: Auth Success Summary CCF: Access Success Summary CCF: Top Suspicious Users CCF: Object Access Summary	
AC.4.025					

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
AC.4.032	CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Config Change After Attack CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Concurrent VPN from Multiple Locations CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Corroborated Account Anomalies CCF: Disabled Account Auth Success CCF: Corroborated Data Access Anomalies CCF: Concurrent VPN from Same User CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User	CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Early TLS/SSL Alarm CCF: Non-Encrypted Protocol Alarm CCF: Blacklisted Account Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: User Object Access Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Escalation Inv CCF: Privileged Account Modification Inv CCF: Audit Log Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Object Access Inv CCF: Password Modification Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: Top Suspicious Users CCF: User Object Access Summary CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Audit Log Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Object Access Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event				
AC.5.024	CCF: FIM Abnormal Activity CCF: FIM Add Activity CCF: FIM General Activity CCF: FIM Information CCF: Data Loss Prevention CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Large Outbound Transfer CCF: Abnormal Amount of Data Transferred CCF: Corroborated Data Access Anomalies CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Config Deleted/ Disabled	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Backup Failure Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Social Media Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Critical Environment	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Social Media Event CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Backup Information CCF: Software Install CCF: Software Uninstall CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Corroborated Account Anomalies CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin	CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm CCF: Blacklisted Account Alarm	CCF: Config/Policy Change Inv CCF: Patch Activity Inv CCF: Time Sync Error Inv CCF: Backup Activity Inv CCF: Audit Log Inv CCF: Compromises Detected Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Backup Activity Summary CCF: Audit Log Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified				

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
AM.3.036	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Config Modified CCF: Large Outbound Transfer CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Config Deleted/ Disabled CCF: Critical Event After Attack CCF: Software Install CCF: Software Uninstall CCF: Excessive Authentication Failure Rule	CCF: FIM Delete Activity Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Rogue Access Point Alarm CCF: Blacklisted Account Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm CCF: Suspected Wireless Attack Alarm	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: User Object Access Inv CCF: Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Patch Activity Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Audit Log Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Suspected Wireless Attack Inv CCF: Password Modification Inv	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Patch Activity Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Audit Log Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Corroborated Account Anomalies CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified CCF: Password Modified by Another User CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Misuse			CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Suspected Wireless Attack Summary CCF: Rogue Access Point Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
AM.4.226	CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Config Deleted/ Disabled CCF: Config Modified CCF: Software Install CCF: Software Uninstall	CCF: PRD Envir Config/Policy Change Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm	CCF: Config/Policy Change Inv CCF: Patch Activity Inv CCF: Signature Activity Inv CCF: Audit Log Inv	CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Signature Activity Summary CCF: Audit Log Summary	
AU.2.041	CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: FIM Information CCF: Data Destruction CCF: Data Loss Prevention CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies CCF: Backup Information CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After	CCF: FIM Delete Activity Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm	CCF: Use Of Non-Encrypted Protocols Inv CCF: Object Access Inv CCF: Audit Log Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Config/Policy Change Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Patch Activity Inv CCF: Backup Activity Inv CCF: Time Sync Error Inv CCF: Social Media Inv CCF: Host Access Granted	CCF: Use Of Non-Encrypted Protocols Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Object Access Summary CCF: User Object Access Summary CCF: Audit Log Summary CCF: Config/Policy Change Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Attack CCF: Config Deleted/ Disabled CCF: Abnormal Amount of Data Transferred CCF: Large Outbound Transfer CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Social Media Event CCF: Misuse CCF: Disabled Account Auth Success CCF: Corroborated Account Anomalies CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Blacklist Location Auth CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule	CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Backup Failure Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Privilege Escalation After Attack Alarm	And Revoked Inv CCF: Applications Accessed By User Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Social Media Summary CCF: Applications Accessed By User Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified			CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Backup Activity Summary	
AU.2.042	CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: FIM Information CCF: Data Destruction CCF: Data Loss Prevention CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies CCF: Backup Information CCF: Config Change After Attack CCF: Abnormal Amount of Data Transferred CCF: Large Outbound Transfer CCF: GeoIP General Activity	CCF: FIM Delete Activity Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm	CCF: Use Of Non-Encrypted Protocols Inv CCF: Object Access Inv CCF: Audit Log Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Config/Policy Change Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Patch Activity Inv CCF: Backup Activity Inv CCF: Time Sync Error Inv CCF: Social Media Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed	CCF: Use Of Non-Encrypted Protocols Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Object Access Summary CCF: User Object Access Summary CCF: Audit Log Summary CCF: Config/Policy Change Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: GeoIP Blacklisted Region Activity CCF: Social Media Event CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Config Deleted/ Disabled CCF: Disabled Account Auth Success CCF: Corroborated Account Anomalies CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule	CCF: PRD Envir Signature Failure Alarm CCF: Backup Failure Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Privilege Escalation After Attack Alarm	By User Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	Summary CCF: Social Media Summary CCF: Applications Accessed By User Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified			CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Backup Activity Summary	
AU.2.043	CCF: Config Modified	CCF: Time Sync Error Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm	CCF: Time Sync Error Inv CCF: Audit Log Inv	CCF: Time Sync Error Summary CCF: Audit Log Summary	
AU.2.044	CCF: FIM Abnormal Activity CCF: FIM Add Activity CCF: FIM General Activity CCF: FIM Information CCF: Data Loss Prevention CCF: Data Destruction CCF: Data Exfiltration Observed	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Large Outbound Transfer CCF: Abnormal Amount of Data Transferred CCF: Corroborated Data Access Anomalies CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Config Deleted/ Disabled CCF: Critical Event After Attack CCF: Social Media Event CCF: Config Change After Attack CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Backup Information CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Software Install CCF: Software Uninstall CCF: Excessive Authentication Failure Rule	Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Backup Failure Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm CCF: Blacklisted Account Alarm	Defender Log Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Social Media Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Patch Activity Inv CCF: Time Sync Error Inv CCF: Backup Activity Inv CCF: Audit Log Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv	CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Backup Activity Summary CCF: Audit Log Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Attack then External Connection CCF: Corroborated Account Anomalies CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified		CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	Management Activity Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	
AU.3.045	CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: FIM Information CCF: Data Destruction CCF: Data Loss Prevention CCF: Data Exfiltration Observed	CCF: FIM Delete Activity Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped	CCF: Use Of Non-Encrypted Protocols Inv CCF: Object Access Inv CCF: Audit Log Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Config/Policy Change Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Object Access Summary CCF: User Object Access Summary CCF: Audit Log Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Corroborated Data Access Anomalies CCF: Backup Information CCF: Abnormal Amount of Data Transferred CCF: Large Outbound Transfer CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Social Media Event CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Config Deleted/ Disabled CCF: Disabled Account Auth Success CCF: Corroborated Account Anomalies CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Blacklist Location Auth CCF: Concurrent VPN from Multiple Locations	Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Backup Failure Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Patch Activity Inv CCF: Backup Activity Inv CCF: Time Sync Error Inv CCF: Social Media Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv	CCF: Config/Policy Change Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Social Media Summary CCF: Applications Accessed By User Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Concurrent VPN from Same User CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified		CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	Summary CCF: Social Media Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Backup Activity Summary	
AU.3.046	CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: FIM Information CCF: Data Destruction CCF: Data Loss Prevention CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies	CCF: FIM Delete Activity Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared	CCF: Use Of Non-Encrypted Protocols Inv CCF: Object Access Inv CCF: Audit Log Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Config/Policy Change Inv CCF: Critical Environment Error Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Object Access Summary CCF: User Object Access Summary CCF: Audit Log Summary CCF: Config/Policy Change Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Backup Information CCF: Abnormal Amount of Data Transferred CCF: Large Outbound Transfer CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Social Media Event CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Config Deleted/ Disabled CCF: Disabled Account Auth Success CCF: Corroborated Account Anomalies CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User	Alarm CCF: Failed Audit Log Write Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Backup Failure Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Signature Activity Inv CCF: Patch Activity Inv CCF: Backup Activity Inv CCF: Time Sync Error Inv CCF: Social Media Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Social Media Summary CCF: Applications Accessed By User Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified			CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Backup Activity Summary	
AU.3.048	CCF: FIM Abnormal Activity CCF: FIM Add Activity CCF: FIM General Activity CCF: FIM Information CCF: Data Loss Prevention CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Large Outbound Transfer CCF: Abnormal Amount of Data Transferred	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Privileged Account Modification Inv CCF: Privileged Account	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Corroborated Data Access Anomalies CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Config Deleted/ Disabled CCF: Critical Event After Attack CCF: Social Media Event CCF: Config Change After Attack CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Backup Information CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Software Install CCF: Software Uninstall CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule	CCF: Backup Failure Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm CCF: Blacklisted Account Alarm	Escalation Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Social Media Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Patch Activity Inv CCF: Time Sync Error Inv CCF: Backup Activity Inv CCF: Audit Log Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	CCF: User Misuse Summary CCF: GeoIP Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Backup Activity Summary CCF: Audit Log Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Auth Failure Summary CCF: Access Failure	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Attack then External Connection CCF: Corroborated Account Anomalies CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified			Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
AU.3.049	CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: FIM Information CCF: Data Destruction CCF: Data Loss Prevention CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies CCF: Backup Information CCF: Config Modified CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Config Deleted/ Disabled CCF: Software Install CCF: Software Uninstall CCF: Excessive Authentication Failure Rule CCF: Attack then External Connection	CCF: FIM Delete Activity Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Backup Failure Alarm	CCF: Use Of Non-Encrypted Protocols Inv CCF: User Object Access Inv CCF: Audit Log Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Backup Activity Inv CCF: Config/Policy Change Inv CCF: Physical Access Inv CCF: Object Access Inv CCF: Excessive Authentication Failure Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: User Object Access Summary CCF: Audit Log Summary CCF: Backup Activity Summary CCF: Config/Policy Change Summary CCF: Physical Access Summary CCF: Object Access Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
AU.3.050	CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Password Modified by Admin CCF: Admin Password Modified CCF: Multiple Account Passwords Modified by Admin CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Abnormal Origin Location CCF: Corroborated Account Anomalies	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Blacklisted Account Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Use Of Non-Encrypted Protocols Inv CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Audit Log Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	CCF: Physical Access Summary CCF: Applications Accessed By User Summary CCF: Top Suspicious Users CCF: GeoIP Summary CCF: Physical Access Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: User Object Access Summary CCF: Object Access Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Audit Log Summary CCF: User Misuse Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Password Modified by Admin CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified CCF: Password Modified by Another User CCF: Misuse				
AU.3.051	CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: FIM Information CCF: Data Destruction CCF: Data Loss Prevention CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies CCF: Backup Information CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Config Deleted/ Disabled CCF: Abnormal Amount of Data Transferred CCF: Large Outbound Transfer CCF: GeoIP General Activity CCF: GeoIP Blacklisted	CCF: FIM Delete Activity Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Backup Failure Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm	CCF: Use Of Non-Encrypted Protocols Inv CCF: Object Access Inv CCF: Audit Log Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Config/Policy Change Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Patch Activity Inv CCF: Backup Activity Inv CCF: Time Sync Error Inv CCF: Social Media Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Object Access Summary CCF: User Object Access Summary CCF: Audit Log Summary CCF: Config/Policy Change Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Social Media Summary CCF: Applications Accessed By User Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Misuse Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Region Activity CCF: Social Media Event CCF: Misuse CCF: Critical Event After Attack CCF: Disabled Account Auth Success CCF: Corroborated Account Anomalies CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin	CCF: Priv Group Access Granted Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Privilege Escalation After Attack Alarm	CCF: GeoIP Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified			Summary CCF: Backup Activity Summary	
AU.3.052	CCF: FIM Abnormal Activity CCF: FIM Add Activity CCF: FIM General Activity CCF: FIM Information CCF: Data Loss Prevention CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Large Outbound Transfer CCF: Abnormal Amount of Data Transferred CCF: Corroborated Data Access Anomalies CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Corroborated Account	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Backup Failure Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Social Media Inv CCF: Critical Environment Error Inv	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Anomalies CCF: Config Deleted/ Disabled CCF: Social Media Event CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Backup Information CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by	Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Privilege Escalation After Attack Alarm CCF: Blacklisted Account Alarm	CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Patch Activity Inv CCF: Time Sync Error Inv CCF: Backup Activity Inv CCF: Audit Log Inv CCF: Compromises Detected Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Backup Activity Summary CCF: Audit Log Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified				
AU.4.053	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Config Deleted/ Disabled CCF: Social Media Event CCF: Config Change After Attack CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Backup Failure Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Social Media Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Patch Activity Inv	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Backup Information CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies CCF: Large Outbound Transfer CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Corroborated Account Anomalies CCF: Disabled Account Auth Success CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by	Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Time Sync Error Inv CCF: Backup Activity Inv CCF: Audit Log Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Backup Activity Summary CCF: Audit Log Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified				
AU.4.054	CCF: FIM Abnormal Activity CCF: FIM Add Activity CCF: FIM General Activity CCF: FIM Information CCF: Data Loss Prevention CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Large Outbound Transfer CCF: Abnormal Amount of Data Transferred CCF: Corroborated Data Access Anomalies CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Config Deleted/ Disabled CCF: Social Media Event CCF: Config Change After Attack	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Backup Failure Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Social Media Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Patch Activity Inv	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Backup Information CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Corroborated Account Anomalies CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account	Alarm CCF: Priv Group Access Granted Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Privilege Escalation After Attack Alarm CCF: Blacklisted Account Alarm	CCF: Time Sync Error Inv CCF: Backup Activity Inv CCF: Audit Log Inv CCF: Compromises Detected Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Denial Of Service Inv CCF: Password Modification Inv	CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Backup Activity Summary CCF: Audit Log Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Passwords Modified by Admin CCF: Admin Password Modified				
AU.5.055	CCF: FIM Abnormal Activity CCF: FIM Add Activity CCF: FIM General Activity CCF: FIM Information CCF: Data Loss Prevention CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Large Outbound Transfer CCF: Abnormal Amount of Data Transferred CCF: Corroborated Data Access Anomalies CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Config Deleted/ Disabled CCF: Critical Event After Attack CCF: Social Media Event CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Backup Failure Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Social Media Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Config/Policy Change	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Backup Information CCF: Software Install CCF: Software Uninstall CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Corroborated Account Anomalies CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified	Granted Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm CCF: Blacklisted Account Alarm	Inv CCF: Patch Activity Inv CCF: Time Sync Error Inv CCF: Backup Activity Inv CCF: Audit Log Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Backup Activity Summary CCF: Audit Log Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
AT.2.056					
AT.2.057					
AT.3.058					
AT.4.059					
AT.4.060					
CM.2.061					

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
CM.2.062	CCF: FIM Abnormal Activity CCF: FIM Add Activity CCF: FIM General Activity CCF: FIM Information CCF: Data Loss Prevention CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Large Outbound Transfer CCF: Abnormal Amount of Data Transferred CCF: Corroborated Data Access Anomalies CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Config Modified CCF: Social Media Event CCF: Windows RunAs Privilege Escalation CCF: Blacklist Location Auth CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Config Deleted/ Disabled CCF: Software Install CCF: Software Uninstall CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Excessive	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Privilege Escalation After Attack Alarm CCF: Priv Group Access Granted Alarm CCF: Unknown User Account Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Use Of Non-Encrypted Protocols Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: User Object Access Inv CCF: Object Access Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Modification Inv CCF: Config/Policy Change Inv CCF: Patch Activity Inv CCF: Signature Activity Inv CCF: Critical Environment Error Inv CCF: Privileged Account Escalation Inv CCF: Privileged Account Escalation Inv CCF: Audit Log Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Object Access Summary CCF: User Object Access Summary CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Patch Activity Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Critical Environment Error Summary CCF: Audit Log Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Abnormal Origin Location CCF: Corroborated Account Anomalies CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event			CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
CM.2.063	CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Config Deleted/ Disabled CCF: Config Modified CCF: Software Install CCF: Software Uninstall	CCF: PRD Envir Config/Policy Change Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm	CCF: Config/Policy Change Inv CCF: Patch Activity Inv CCF: Signature Activity Inv CCF: Audit Log Inv	CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Signature Activity Summary CCF: Audit Log Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
CM.2.064	CCF: FIM Abnormal Activity CCF: FIM Add Activity CCF: FIM General Activity CCF: FIM Information CCF: Data Loss Prevention CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Large Outbound Transfer CCF: Abnormal Amount of Data Transferred CCF: Corroborated Data Access Anomalies CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Config Modified CCF: Social Media Event CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Blacklist Location Auth CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Config Deleted/ Disabled CCF: Corroborated Account Anomalies CCF: Software Install CCF: Software Uninstall CCF: Excessive	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Unknown User Account Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Use Of Non-Encrypted Protocols Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: User Object Access Inv CCF: Object Access Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Config/Policy Change Inv CCF: Patch Activity Inv CCF: Signature Activity Inv CCF: Critical Environment Error Inv CCF: Audit Log Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Object Access Summary CCF: User Object Access Summary CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Patch Activity Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Critical Environment Error Summary CCF: Audit Log Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified CCF: Password Modified by Another User CCF: Local Account Created and Used CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event			CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
CM.2.065	CCF: FIM Abnormal Activity CCF: FIM Add Activity CCF: FIM General Activity CCF: FIM Information CCF: Data Loss Prevention CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Large Outbound Transfer CCF: Abnormal Amount of Data Transferred CCF: Corroborated Data Access Anomalies CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Config Modified CCF: Social Media Event CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Blacklist Location Auth CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Config Deleted/ Disabled CCF: Software Install CCF: Software Uninstall CCF: Excessive Authentication Failure Rule CCF: Account Modification	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Unknown User Account Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Use Of Non-Encrypted Protocols Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: User Object Access Inv CCF: Object Access Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Config/Policy Change Inv CCF: Patch Activity Inv CCF: Signature Activity Inv CCF: Critical Environment Error Inv CCF: Audit Log Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Object Access Summary CCF: User Object Access Summary CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Patch Activity Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Critical Environment Error Summary CCF: Audit Log Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified CCF: Password Modified by Another User CCF: Local Account Created and Used CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event			CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	
CM.2.066					
CM.3.067					
CM.3.068					
CM.3.069	CCF: FIM Abnormal Activity CCF: FIM Add Activity CCF: FIM General Activity CCF: FIM Information	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Data Loss Prevention CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Large Outbound Transfer CCF: Abnormal Amount of Data Transferred CCF: Corroborated Data Access Anomalies CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Config Deleted/ Disabled CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Social Media Event CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Backup Information CCF: Software Install CCF: Software Uninstall	Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Backup Failure Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation	Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Social Media Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Patch Activity Inv CCF: Time Sync Error Inv CCF: Backup Activity Inv CCF: Audit Log Inv CCF: Compromises Detected Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Denial Of Service Inv CCF: Excessive	CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Backup Activity Summary CCF: Audit Log Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Corroborated Account Anomalies CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified	After Attack Alarm CCF: Blacklisted Account Alarm	Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	& SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	
CM.4.073					
CM.5.074	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Social Media Event CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Config Deleted/ Disabled CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Backup Information CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies CCF: Large Outbound Transfer CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Corroborated Account Anomalies	Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Backup Failure Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Privilege Escalation After Attack Alarm	Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Social Media Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Patch Activity Inv CCF: Time Sync Error Inv CCF: Backup Activity Inv CCF: Audit Log Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive	CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Backup Activity Summary CCF: Audit Log Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Corroborated Account Anomalies CCF: Disabled Account Auth Success CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified		Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	& SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
IA.1.076	CCF: Disabled Account Auth Success CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Abnormal Origin Location CCF: Auth After Security Event CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Corroborated Account Anomalies CCF: Password Modified by Admin CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified	CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Blacklisted Account Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: Suspicious Users Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: User Object Access Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Audit Log Inv CCF: Object Access Inv CCF: Password Modification Inv	CCF: Physical Access Summary CCF: Applications Accessed By User Summary CCF: Top Suspicious Users CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: User Object Access Summary CCF: Audit Log Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Object Access Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Password Modified by Another User CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event				

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
IA.1.077	CCF: Disabled Account Auth Success CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Abnormal Origin Location CCF: Auth After Security Event CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Corroborated Account Anomalies CCF: Password Modified by Admin CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified	CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Blacklisted Account Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: Suspicious Users Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: User Object Access Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Audit Log Inv CCF: Object Access Inv CCF: Password Modification Inv	CCF: Physical Access Summary CCF: Applications Accessed By User Summary CCF: Top Suspicious Users CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: User Object Access Summary CCF: Audit Log Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Object Access Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Password Modified by Another User CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event				

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
IA.2.078	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Corroborated Data Access Anomalies CCF: Social Media Event CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: FIM Abnormal Activity CCF: FIM Add Activity CCF: FIM General Activity CCF: Data Loss Prevention CCF: Config Modified CCF: Large Outbound Transfer CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Config Change After Attack CCF: Config Change then Critical Error	CCF: FIM Delete Activity Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Rogue Access Point Alarm CCF: Blacklisted Account Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm CCF: Suspected Wireless Attack Alarm	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Social Media Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Patch Activity Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Audit Log Inv CCF: Suspected Wireless Attack Inv CCF: Password Modification Inv	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Social Media Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Patch Activity Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Term Account Activity Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Config Deleted/ Disabled CCF: Critical Event After Attack CCF: Software Install CCF: Software Uninstall CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Attack then External Connection CCF: Corroborated Account Anomalies CCF: Concurrent VPN from Same User CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified CCF: Password Modified by Another User CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event			CCF: Account Deleted Summary CCF: Audit Log Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Suspected Wireless Attack Summary CCF: Rogue Access Point Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
IA.2.079	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Corroborated Data Access Anomalies CCF: Social Media Event CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: FIM Abnormal Activity CCF: FIM Add Activity CCF: FIM General Activity CCF: Data Loss Prevention CCF: Config Modified CCF: Large Outbound Transfer CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Config Change After Attack CCF: Config Change then Critical Error	CCF: FIM Delete Activity Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Rogue Access Point Alarm CCF: Blacklisted Account Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm CCF: Suspected Wireless Attack Alarm	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Social Media Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Patch Activity Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Audit Log Inv CCF: Suspected Wireless Attack Inv CCF: Password Modification Inv	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Social Media Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Patch Activity Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Term Account Activity Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Config Deleted/ Disabled CCF: Critical Event After Attack CCF: Software Install CCF: Software Uninstall CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Attack then External Connection CCF: Corroborated Account Anomalies CCF: Concurrent VPN from Same User CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified CCF: Password Modified by Another User CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event			CCF: Account Deleted Summary CCF: Audit Log Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Suspected Wireless Attack Summary CCF: Rogue Access Point Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
IA.2.080	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Corroborated Data Access Anomalies CCF: Social Media Event CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: FIM Abnormal Activity CCF: FIM Add Activity CCF: FIM General Activity CCF: Data Loss Prevention CCF: Config Modified CCF: Large Outbound Transfer CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Config Change After Attack CCF: Config Change then Critical Error	CCF: FIM Delete Activity Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Rogue Access Point Alarm CCF: Blacklisted Account Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm CCF: Suspected Wireless Attack Alarm	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Social Media Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Patch Activity Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Audit Log Inv CCF: Suspected Wireless Attack Inv CCF: Password Modification Inv	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Social Media Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Patch Activity Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Term Account Activity Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Config Deleted/ Disabled CCF: Critical Event After Attack CCF: Software Install CCF: Software Uninstall CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Attack then External Connection CCF: Corroborated Account Anomalies CCF: Concurrent VPN from Same User CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified CCF: Password Modified by Another User CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event			CCF: Account Deleted Summary CCF: Audit Log Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Suspected Wireless Attack Summary CCF: Rogue Access Point Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
IA.2.081		CCF: Early TLS/SSL Alarm CCF: Non-Encrypted Protocol Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm	CCF: Use Of Non-Encrypted Protocols Inv CCF: Audit Log Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: Audit Log Summary	
IA.2.082					

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
IA.3.083	CCF: Disabled Account Auth Success CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Abnormal Origin Location CCF: Auth After Security Event CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Corroborated Account Anomalies CCF: Password Modified by Admin CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified	CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Blacklisted Account Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: Suspicious Users Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: User Object Access Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Audit Log Inv CCF: Object Access Inv CCF: Password Modification Inv	CCF: Physical Access Summary CCF: Applications Accessed By User Summary CCF: Top Suspicious Users CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: User Object Access Summary CCF: Audit Log Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Object Access Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Password Modified by Another User CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event				

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
IA.3.084	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Corroborated Data Access Anomalies CCF: Social Media Event CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: FIM Abnormal Activity CCF: FIM Add Activity CCF: FIM General Activity CCF: Data Loss Prevention CCF: Config Modified CCF: Large Outbound Transfer CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Config Change After Attack CCF: Config Change then Critical Error	CCF: FIM Delete Activity Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Rogue Access Point Alarm CCF: Blacklisted Account Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm CCF: Suspected Wireless Attack Alarm	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Misuse Inv CCF: User Object Access Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Social Media Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Patch Activity Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Audit Log Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Suspected Wireless Attack Inv CCF: Password Modification Inv	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Social Media Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Patch Activity Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Audit Log Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Config Deleted/ Disabled CCF: Critical Event After Attack CCF: Software Install CCF: Software Uninstall CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Corroborated Account Anomalies CCF: Attack then External Connection CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event			Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Suspected Wireless Attack Summary CCF: Rogue Access Point Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
IA.3.085	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Corroborated Data Access Anomalies CCF: Social Media Event CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: FIM Abnormal Activity CCF: FIM Add Activity CCF: FIM General Activity CCF: Data Loss Prevention CCF: Config Modified CCF: Large Outbound Transfer CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Config Change After Attack CCF: Config Change then Critical Error	CCF: FIM Delete Activity Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Rogue Access Point Alarm CCF: Blacklisted Account Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm CCF: Suspected Wireless Attack Alarm	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Social Media Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Patch Activity Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Audit Log Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Suspected Wireless Attack Inv CCF: Password Modification Inv	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Social Media Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Patch Activity Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Audit Log Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Config Deleted/ Disabled CCF: Critical Event After Attack CCF: Software Install CCF: Software Uninstall CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Attack then External Connection CCF: Corroborated Account Anomalies CCF: Concurrent VPN from Same User CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified CCF: Password Modified by Another User CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event			Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Suspected Wireless Attack Summary CCF: Rogue Access Point Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
IA.3.086	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Corroborated Data Access Anomalies CCF: Social Media Event CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: FIM Abnormal Activity CCF: FIM Add Activity CCF: FIM General Activity CCF: Data Loss Prevention CCF: Config Modified CCF: Large Outbound Transfer CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Config Change After Attack CCF: Config Change then Critical Error	CCF: FIM Delete Activity Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Rogue Access Point Alarm CCF: Blacklisted Account Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm CCF: Suspected Wireless Attack Alarm	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Social Media Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Patch Activity Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Audit Log Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Suspected Wireless Attack Inv CCF: Password Modification Inv	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Social Media Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Patch Activity Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Audit Log Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Config Deleted/ Disabled CCF: Critical Event After Attack CCF: Software Install CCF: Software Uninstall CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Attack then External Connection CCF: Corroborated Account Anomalies CCF: Concurrent VPN from Same User CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified CCF: Password Modified by Another User CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event			Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Suspected Wireless Attack Summary CCF: Rogue Access Point Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
IR.2.092	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Config Deleted/ Disabled CCF: Social Media Event CCF: Config Change After Attack CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Backup Information CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Backup Failure Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: Compromise Detected	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Social Media Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Patch Activity Inv CCF: Time Sync Error Inv CCF: Backup Activity Inv CCF: Audit Log Inv CCF: Privileged Account Modification Inv CCF: Privileged Account	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Backup Activity	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Large Outbound Transfer CCF: Corroborated Account Anomalies CCF: Corroborated Account Anomalies CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Disabled Account Auth Success CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified	Alarm CCF: Denial Of Service Alarm CCF: Privilege Escalation After Attack Alarm	Escalation Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	Summary CCF: Audit Log Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
IR.2.093	CCF: FIM Abnormal Activity CCF: FIM Add Activity CCF: FIM General Activity CCF: FIM Information CCF: Data Loss Prevention CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Large Outbound Transfer CCF: Abnormal Amount of Data Transferred CCF: Corroborated Data Access Anomalies CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Config Deleted/ Disabled CCF: Critical Event After Attack CCF: Social Media Event CCF: Config Change After Attack CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Backup Failure Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: Compromise Detected	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Social Media Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Patch Activity Inv CCF: Time Sync Error Inv CCF: Backup Activity Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Backup Activity	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Blacklist Location Auth CCF: Backup Information CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Corroborated Account Anomalies CCF: Software Install CCF: Software Uninstall CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified	Alarm CCF: Denial Of Service Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Audit Log Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Audit Log Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
IR.2.094	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Corroborated Data Access Anomalies CCF: Social Media Event CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: FIM Abnormal Activity CCF: FIM Add Activity CCF: FIM General Activity CCF: Data Loss Prevention CCF: Config Modified CCF: Large Outbound Transfer CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Config Change After Attack CCF: Config Change then Critical Error	CCF: FIM Delete Activity Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Rogue Access Point Alarm CCF: Blacklisted Account Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm CCF: Suspected Wireless Attack Alarm	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Social Media Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Patch Activity Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Audit Log Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Suspected Wireless Attack Inv CCF: Password Modification Inv	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Social Media Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Patch Activity Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Audit Log Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Config Deleted/ Disabled CCF: Critical Event After Attack CCF: Software Install CCF: Software Uninstall CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Attack then External Connection CCF: Corroborated Account Anomalies CCF: Concurrent VPN from Same User CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified CCF: Password Modified by Another User CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event			Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Suspected Wireless Attack Summary CCF: Rogue Access Point Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
IR.2.096	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Corroborated Data Access Anomalies CCF: Social Media Event CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: FIM Abnormal Activity CCF: FIM Add Activity CCF: FIM General Activity CCF: Data Loss Prevention CCF: Config Modified CCF: Large Outbound Transfer CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Config Change After Attack CCF: Config Change then Critical Error	CCF: FIM Delete Activity Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Rogue Access Point Alarm CCF: Blacklisted Account Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm CCF: Suspected Wireless Attack Alarm	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Social Media Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Patch Activity Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Audit Log Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Suspected Wireless Attack Inv CCF: Password Modification Inv	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Social Media Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Patch Activity Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Audit Log Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Config Deleted/ Disabled CCF: Critical Event After Attack CCF: Software Install CCF: Software Uninstall CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Attack then External Connection CCF: Corroborated Account Anomalies CCF: Concurrent VPN from Same User CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified CCF: Password Modified by Another User CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event			Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Suspected Wireless Attack Summary CCF: Rogue Access Point Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
IR.2.097					
IR.3.098	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Config Deleted/ Disabled CCF: Social Media Event CCF: Config Change After Attack CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Backup Information CCF: Data Destruction CCF: Data Exfiltration Observed	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Backup Failure Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Social Media Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Patch Activity Inv CCF: Time Sync Error Inv CCF: Backup Activity Inv CCF: Audit Log Inv CCF: Privileged Account	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Corroborated Data Access Anomalies CCF: Large Outbound Transfer CCF: Corroborated Account Anomalies CCF: Corroborated Account Anomalies CCF: Disabled Account Auth Success CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account	Granted Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Privilege Escalation After Attack Alarm	Modification Inv CCF: Privileged Account Escalation Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	Summary CCF: Backup Activity Summary CCF: Audit Log Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Passwords Modified by Admin CCF: Admin Password Modified				
IR.3.099	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Config Deleted/ Disabled CCF: Social Media Event CCF: Config Change After Attack CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Backup Information CCF: Data Destruction	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Backup Failure Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Social Media Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Patch Activity Inv CCF: Time Sync Error Inv CCF: Backup Activity Inv	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies CCF: Large Outbound Transfer CCF: Corroborated Account Anomalies CCF: Corroborated Account Anomalies CCF: Disabled Account Auth Success CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by	Alarm CCF: Priv Group Access Granted Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Audit Log Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Backup Activity Summary CCF: Audit Log Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified				
IR.4.100	TIS	TIS	TIS	TIS	TIS
IR.4.101	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Config Deleted/ Disabled CCF: Social Media Event CCF: Config Change After Attack CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Backup Failure Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Social Media Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Config/Policy Change	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Critical Environment Error Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	and Used CCF: Blacklist Location Auth CCF: Backup Information CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies CCF: Large Outbound Transfer CCF: Corroborated Account Anomalies CCF: Corroborated Account Anomalies CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Disabled Account Auth Success CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin	Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Privilege Escalation After Attack Alarm	Inv CCF: Patch Activity Inv CCF: Time Sync Error Inv CCF: Backup Activity Inv CCF: Audit Log Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Backup Activity Summary CCF: Audit Log Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified				
IR.5.106	CCF: FIM Abnormal Activity CCF: FIM Add Activity CCF: FIM General Activity CCF: FIM Information CCF: Data Loss Prevention CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Large Outbound Transfer CCF: Abnormal Amount of Data Transferred CCF: Corroborated Data Access Anomalies CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Config Deleted/ Disabled CCF: Critical Event After	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Backup Failure Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Attack CCF: Social Media Event CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Backup Information CCF: Software Install CCF: Software Uninstall CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Corroborated Account Anomalies CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by	Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm CCF: Blacklisted Account Alarm	Inv CCF: Social Media Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Patch Activity Inv CCF: Time Sync Error Inv CCF: Backup Activity Inv CCF: Audit Log Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Backup Activity Summary CCF: Audit Log Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified				
IR.5.102	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Critical Event After Attack CCF: Social Media Event CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Config Deleted/ Disabled CCF: Critical Event After Attack CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Blacklist Location Auth	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Backup Failure Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Social Media Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Config/Policy Change	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Critical Environment Error Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Backup Information CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies CCF: Large Outbound Transfer CCF: Disabled Account Auth Success CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Corroborated Account Anomalies CCF: Disabled Account Auth Success CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by	Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm	Inv CCF: Patch Activity Inv CCF: Time Sync Error Inv CCF: Backup Activity Inv CCF: Audit Log Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Backup Activity Summary CCF: Audit Log Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Admin CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified CCF: Password Modified by Another User CCF: Local Account Created and Used CCF: Software Install CCF: Software Uninstall				
IR.5.108	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Config Deleted/ Disabled CCF: Social Media Event CCF: Config Change After Attack CCF: Windows RunAs	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Backup Failure Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Audit Logging Stopped	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Social Media Inv	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Backup Information CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies CCF: Large Outbound Transfer CCF: Corroborated Account Anomalies CCF: Corroborated Account Anomalies CCF: Disabled Account Auth Success CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Attack then External Connection CCF: Auth After Numerous	Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Patch Activity Inv CCF: Time Sync Error Inv CCF: Backup Activity Inv CCF: Audit Log Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	Summary CCF: Social Media Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Backup Activity Summary CCF: Audit Log Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified			Summary CCF: Term Account Activity Summary	
IR.5.110					

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
MA.2.111	CCF: FIM Abnormal Activity CCF: FIM Add Activity CCF: FIM General Activity CCF: FIM Information CCF: Data Loss Prevention CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Large Outbound Transfer CCF: Abnormal Amount of Data Transferred CCF: Corroborated Data Access Anomalies CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Config Modified CCF: Social Media Event CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Blacklist Location Auth CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Config Deleted/ Disabled CCF: Software Install CCF: Software Uninstall CCF: Auth After Numerous Failed Auths CCF: Auth After Security	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Unknown User Account Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Use Of Non-Encrypted Protocols Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: User Object Access Inv CCF: Object Access Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Config/Policy Change Inv CCF: Patch Activity Inv CCF: Signature Activity Inv CCF: Critical Environment Error Inv CCF: Audit Log Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Object Access Summary CCF: User Object Access Summary CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Patch Activity Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Critical Environment Error Summary CCF: Audit Log Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Event CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Corroborated Account Anomalies CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified CCF: Password Modified by Another User CCF: Local Account Created and Used			CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
MA.2.112	CCF: FIM Abnormal Activity CCF: FIM Add Activity CCF: FIM General Activity CCF: FIM Information CCF: Data Loss Prevention CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Large Outbound Transfer CCF: Abnormal Amount of Data Transferred CCF: Corroborated Data Access Anomalies CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Config Modified CCF: Social Media Event CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Blacklist Location Auth CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Config Deleted/ Disabled CCF: Software Install CCF: Software Uninstall CCF: Excessive Authentication Failure Rule CCF: Account Modification	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Unknown User Account Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: User Object Access Inv CCF: Object Access Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Config/Policy Change Inv CCF: Patch Activity Inv CCF: Signature Activity Inv CCF: Critical Environment Error Inv CCF: Audit Log Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Object Access Summary CCF: User Object Access Summary CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Patch Activity Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Critical Environment Error Summary CCF: Audit Log Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Abnormal Origin Location CCF: Corroborated Account Anomalies CCF: Password Modified by Admin CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified CCF: Password Modified by Another User CCF: Local Account Created and Used CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event			CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	
MA.2.113					

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
MA.2.114	CCF: Excessive Authentication Failure Rule	CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm	CCF: Physical Access Inv CCF: Audit Log Inv CCF: Excessive Authentication Failure Inv	CCF: Physical Access Summary CCF: Audit Log Summary	
MA.3.115					
MA.3.116					
MP.1.118					

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
MP.2.119	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Social Media Event CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Config Modified CCF: Large Outbound Transfer CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Config Deleted/ Disabled CCF: Critical Event After Attack CCF: Excessive Authentication Failure Rule	CCF: FIM Delete Activity Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Rogue Access Point Alarm CCF: Blacklisted Account Alarm CCF: Privilege Escalation After Attack Alarm CCF: Suspected Wireless Attack Alarm	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Social Media Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Patch Activity Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Audit Log Inv CCF: Suspected Wireless Attack Inv CCF: Password Modification Inv	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Social Media Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Patch Activity Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Term Account Activity Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Abnormal Origin Location CCF: Corroborated Account Anomalies CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified CCF: Corroborated Data Access Anomalies CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event			CCF: Account Deleted Summary CCF: Audit Log Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Suspected Wireless Attack Summary CCF: Rogue Access Point Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
MP.2.120	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Social Media Event CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Config Modified CCF: Large Outbound Transfer CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Config Deleted/ Disabled CCF: Critical Event After Attack CCF: Excessive Authentication Failure Rule	CCF: FIM Delete Activity Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Rogue Access Point Alarm CCF: Blacklisted Account Alarm CCF: Privilege Escalation After Attack Alarm CCF: Suspected Wireless Attack Alarm	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Social Media Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Patch Activity Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Audit Log Inv CCF: Suspected Wireless Attack Inv CCF: Password Modification Inv	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Social Media Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Patch Activity Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Term Account Activity Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Abnormal Origin Location CCF: Corroborated Account Anomalies CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified CCF: Corroborated Data Access Anomalies CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event			CCF: Account Deleted Summary CCF: Audit Log Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Suspected Wireless Attack Summary CCF: Rogue Access Point Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
MP.2.121	CCF: FIM Abnormal Activity CCF: FIM Add Activity CCF: FIM General Activity CCF: FIM Information CCF: Data Loss Prevention CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Large Outbound Transfer CCF: Abnormal Amount of Data Transferred CCF: Corroborated Data Access Anomalies CCF: Config Modified CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Config Deleted/ Disabled CCF: Software Install CCF: Software Uninstall CCF: Attack then External Connection CCF: Excessive Authentication Failure Rule	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm	CCF: Use Of Non-Encrypted Protocols Inv CCF: User Object Access Inv CCF: Audit Log Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Config/Policy Change Inv CCF: Physical Access Inv CCF: Object Access Inv CCF: Excessive Authentication Failure Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: User Object Access Summary CCF: Audit Log Summary CCF: Config/Policy Change Summary CCF: Physical Access Summary CCF: Object Access Summary	
MP.3.122					

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
MP.3.123	CCF: FIM Abnormal Activity CCF: FIM Add Activity CCF: FIM General Activity CCF: FIM Information CCF: Data Loss Prevention CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Large Outbound Transfer CCF: Abnormal Amount of Data Transferred CCF: Corroborated Data Access Anomalies CCF: Config Modified CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Config Deleted/ Disabled CCF: Software Install CCF: Software Uninstall CCF: Attack then External Connection CCF: Excessive Authentication Failure Rule	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm	CCF: Use Of Non-Encrypted Protocols Inv CCF: User Object Access Inv CCF: Audit Log Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Config/Policy Change Inv CCF: Physical Access Inv CCF: Object Access Inv CCF: Excessive Authentication Failure Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: User Object Access Summary CCF: Audit Log Summary CCF: Config/Policy Change Summary CCF: Physical Access Summary CCF: Object Access Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
MP.3.124	CCF: Excessive Authentication Failure Rule	CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm	CCF: Physical Access Inv CCF: Audit Log Inv CCF: Excessive Authentication Failure Inv	CCF: Physical Access Summary CCF: Audit Log Summary	
MP.3.125					
PS.2.127					

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
PS.2.128	CCF: Disabled Account Auth Success CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Abnormal Origin Location CCF: Auth After Security Event CCF: Password Modified by Admin CCF: Disabled Account Auth Success CCF: Abnormal Amount of Data Transferred CCF: Large Outbound Transfer CCF: Data Exfiltration Observed CCF: Data Destruction CCF: Corroborated Data Access Anomalies CCF: Data Loss Prevention CCF: FIM Information CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule	CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Blacklisted Account Alarm CCF: Privilege Escalation After Attack Alarm CCF: FIM Delete Activity Alarm	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: Suspicious Users Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: User Object Access Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Audit Log Inv CCF: Object Access Inv CCF: Password Modification Inv	CCF: Physical Access Summary CCF: Applications Accessed By User Summary CCF: Top Suspicious Users CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: User Object Access Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Term Account Activity Summary CCF: Account Deleted Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Audit Log Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Corroborated Account Anomalies CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event			Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Object Access Summary	
PE.1.131	CCF: Excessive Authentication Failure Rule	CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm	CCF: Physical Access Inv CCF: Audit Log Inv CCF: Excessive Authentication Failure Inv	CCF: Physical Access Summary CCF: Audit Log Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
PE.1.132	CCF: Excessive Authentication Failure Rule	CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm	CCF: Physical Access Inv CCF: Audit Log Inv CCF: Excessive Authentication Failure Inv	CCF: Physical Access Summary CCF: Audit Log Summary	
PE.1.133	CCF: Excessive Authentication Failure Rule	CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm	CCF: Physical Access Inv CCF: Audit Log Inv CCF: Excessive Authentication Failure Inv	CCF: Physical Access Summary CCF: Audit Log Summary	
PE.1.134	CCF: Excessive Authentication Failure Rule	CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm	CCF: Physical Access Inv CCF: Audit Log Inv CCF: Excessive Authentication Failure Inv	CCF: Physical Access Summary CCF: Audit Log Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
PE.2.135	CCF: Excessive Authentication Failure Rule	CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm	CCF: Physical Access Inv CCF: Audit Log Inv CCF: Excessive Authentication Failure Inv	CCF: Physical Access Summary CCF: Audit Log Summary	
PE.3.136					

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
RE.2.137	CCF: Backup Information CCF: FIM Abnormal Activity CCF: FIM Add Activity CCF: FIM General Activity CCF: FIM Information CCF: Data Loss Prevention CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Large Outbound Transfer CCF: Abnormal Amount of Data Transferred CCF: Corroborated Data Access Anomalies CCF: Software Install CCF: Software Uninstall CCF: Excessive Authentication Failure Rule CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Config Deleted/ Disabled CCF: Critical Event After Attack CCF: Attack then External Connection	CCF: Backup Failure Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: FIM Delete Activity Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm	CCF: Critical Environment Error Inv CCF: Backup Activity Inv CCF: Physical Access Inv CCF: Audit Log Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Time Sync Error Inv CCF: Applications Accessed By User Inv CCF: User Object Access Inv CCF: Object Access Inv CCF: Excessive Authentication Failure Inv	CCF: Critical Environment Error Summary CCF: Backup Activity Summary CCF: Physical Access Summary CCF: Audit Log Summary CCF: Config/Policy Change Summary CCF: User Object Access Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Object Access Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
RE.2.138	CCF: FIM Abnormal Activity CCF: FIM Add Activity CCF: FIM General Activity CCF: FIM Information CCF: Data Loss Prevention CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Large Outbound Transfer CCF: Abnormal Amount of Data Transferred CCF: Corroborated Data Access Anomalies CCF: Backup Information CCF: Config Change After Attack CCF: Excessive Authentication Failure Rule	CCF: FIM Delete Activity Alarm CCF: Backup Failure Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm	CCF: Physical Access Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Critical Environment Error Inv CCF: Config/Policy Change Inv CCF: Backup Activity Inv CCF: Audit Log Inv CCF: Excessive Authentication Failure Inv	CCF: Physical Access Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Critical Environment Error Summary CCF: Time Sync Error Summary CCF: Backup Activity Summary CCF: Audit Log Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
RE.3.139	CCF: Backup Information CCF: FIM Abnormal Activity CCF: FIM Add Activity CCF: FIM General Activity CCF: FIM Information CCF: Data Loss Prevention CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Large Outbound Transfer CCF: Abnormal Amount of Data Transferred CCF: Corroborated Data Access Anomalies CCF: Software Install CCF: Software Uninstall CCF: Excessive Authentication Failure Rule CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Config Deleted/ Disabled CCF: Critical Event After Attack CCF: Attack then External Connection	CCF: Backup Failure Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: FIM Delete Activity Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm	CCF: Critical Environment Error Inv CCF: Backup Activity Inv CCF: Physical Access Inv CCF: Audit Log Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Time Sync Error Inv CCF: Applications Accessed By User Inv CCF: User Object Access Inv CCF: Object Access Inv CCF: Excessive Authentication Failure Inv	CCF: Critical Environment Error Summary CCF: Backup Activity Summary CCF: Physical Access Summary CCF: Audit Log Summary CCF: Config/Policy Change Summary CCF: User Object Access Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Object Access Summary	
RE.5.140	CCF: FIM Abnormal Activity CCF: FIM Add Activity CCF: FIM General Activity CCF: FIM Information CCF: Data Loss Prevention	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Large Outbound Transfer CCF: Abnormal Amount of Data Transferred CCF: Corroborated Data Access Anomalies CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Social Media Event CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Config Deleted/ Disabled CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Backup Information CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Excessive Authentication Failure Rule CCF: Account Modification	CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Backup Failure Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Social Media Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Patch Activity Inv CCF: Time Sync Error Inv CCF: Backup Activity Inv CCF: Audit Log Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv	By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Backup Activity Summary CCF: Audit Log Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Corroborated Account Anomalies CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified		CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	
RM.2.141	CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: FIM Information CCF: Data Destruction CCF: Data Loss Prevention CCF: Data Exfiltration Observed CCF: Corroborated Data	CCF: FIM Delete Activity Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm	CCF: Use Of Non-Encrypted Protocols Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: Audit Log Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Config/Policy Change Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Object Access Summary CCF: User Object Access Summary CCF: Audit Log Summary CCF: Config/Policy Change	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Access Anomalies CCF: Backup Information CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Config Deleted/ Disabled CCF: Critical Event After Attack CCF: Abnormal Amount of Data Transferred CCF: Large Outbound Transfer CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Social Media Event CCF: Misuse CCF: Disabled Account Auth Success CCF: Corroborated Account Anomalies CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from	CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Backup Failure Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Patch Activity Inv CCF: Backup Activity Inv CCF: Time Sync Error Inv CCF: Social Media Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv	Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Social Media Summary CCF: Applications Accessed By User Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Same User CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Password Modified by Another User CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified		CCF: Deleted Account Inv CCF: Password Modification Inv	CCF: Social Media Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Backup Activity Summary CCF: Term Account Activity Summary	
RM.2.142					
RM.2.143	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: Rogue Access Point Alarm	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Config Deleted/ Disabled CCF: Social Media Event CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Backup Information CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies CCF: Large Outbound Transfer CCF: Corroborated Account Anomalies CCF: Disabled Account Auth Success CCF: Multiple Account	CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Backup Failure Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm	CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Social Media Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Patch Activity Inv CCF: Time Sync Error Inv CCF: Backup Activity Inv CCF: Audit Log Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv	Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Backup Activity Summary CCF: Audit Log Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Passwords Modified by Admin CCF: Admin Password Modified CCF: Password Modified by Another User CCF: Password Modified by Admin CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Software Install CCF: Software Uninstall CCF: Concurrent VPN from Same User CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location		CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	CCF: Priv Account Management Activity Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	
RM.3.144	CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: FIM Information CCF: Data Destruction CCF: Data Loss Prevention CCF: Data Exfiltration	CCF: FIM Delete Activity Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: LogRhythm Silent Log Source Error Alarm	CCF: Use Of Non-Encrypted Protocols Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: Audit Log Inv CCF: LogRhythm Data Loss Defender Log Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Object Access Summary CCF: User Object Access Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Observed CCF: Corroborated Data Access Anomalies CCF: Backup Information CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Config Deleted/ Disabled CCF: Critical Event After Attack CCF: Abnormal Amount of Data Transferred CCF: Large Outbound Transfer CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Social Media Event CCF: Misuse CCF: Disabled Account Auth Success CCF: Corroborated Account Anomalies CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Concurrent VPN from	CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Backup Failure Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Config/Policy Change Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Patch Activity Inv CCF: Backup Activity Inv CCF: Time Sync Error Inv CCF: Social Media Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv	CCF: Audit Log Summary CCF: Config/Policy Change Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Social Media Summary CCF: Applications Accessed By User Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Multiple Locations CCF: Concurrent VPN from Same User CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Password Modified by Another User CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified		CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Backup Activity Summary CCF: Term Account Activity Summary	
RM.3.146					
RM.3.147					

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
RM.4.149	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Social Media Event CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Config Deleted/ Disabled CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Backup Information CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies CCF: Large Outbound Transfer	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Backup Failure Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: Compromise Detected	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Social Media Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Patch Activity Inv CCF: Time Sync Error Inv CCF: Backup Activity Inv CCF: Audit Log Inv CCF: Privileged Account Modification Inv CCF: Privileged Account	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Backup Activity	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Corroborated Account Anomalies CCF: Config Change After Attack CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Corroborated Account Anomalies CCF: Disabled Account Auth Success CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified	Alarm CCF: Denial Of Service Alarm CCF: Privilege Escalation After Attack Alarm	Escalation Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	Summary CCF: Audit Log Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
RM.4.150	CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: FIM Information CCF: Data Destruction CCF: Data Loss Prevention CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies CCF: Backup Information CCF: Config Change After Attack CCF: Abnormal Amount of Data Transferred CCF: Large Outbound Transfer CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Social Media Event CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Config Deleted/ Disabled CCF: Disabled Account Auth Success CCF: Corroborated Account Anomalies CCF: Windows RunAs	CCF: FIM Delete Activity Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Backup Failure Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Compromise Detected	CCF: Use Of Non-Encrypted Protocols Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: Audit Log Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Config/Policy Change Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Patch Activity Inv CCF: Backup Activity Inv CCF: Time Sync Error Inv CCF: Social Media Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected	CCF: Use Of Non-Encrypted Protocols Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: User Object Access Summary CCF: Object Access Summary CCF: Audit Log Summary CCF: Config/Policy Change Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Social Media Summary CCF: Applications Accessed By User Summary CCF: Top Suspicious Users CCF: User Misuse Summary CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Compromises Detected	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Concurrent VPN from Multiple Locations CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified	Alarm CCF: Denial Of Service Alarm CCF: Privilege Escalation After Attack Alarm	Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Backup Activity Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
RM.4.151	CCF: FIM Abnormal Activity CCF: FIM Add Activity CCF: FIM General Activity CCF: FIM Information CCF: Data Loss Prevention CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Large Outbound Transfer CCF: Abnormal Amount of Data Transferred CCF: Corroborated Data Access Anomalies CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Config Deleted/ Disabled CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Social Media Event CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Backup Failure Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Social Media Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Patch Activity Inv CCF: Time Sync Error Inv CCF: Backup Activity Inv CCF: Audit Log Inv CCF: Compromises Detected Inv CCF: Privileged Account	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Backup Activity	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	and Used CCF: Blacklist Location Auth CCF: Backup Information CCF: Software Install CCF: Software Uninstall CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Corroborated Account Anomalies CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified	CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm CCF: Blacklisted Account Alarm	Modification Inv CCF: Privileged Account Escalation Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	Summary CCF: Audit Log Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
RM.4.148					
RM.5.152	CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: FIM Information CCF: Data Destruction CCF: Data Loss Prevention CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies CCF: Backup Information CCF: Abnormal Amount of Data Transferred CCF: Large Outbound Transfer CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Social Media Event CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Config Deleted/ Disabled CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Disabled Account Auth Success	CCF: FIM Delete Activity Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Backup Failure Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected	CCF: Use Of Non-Encrypted Protocols Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: Audit Log Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Config/Policy Change Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Patch Activity Inv CCF: Backup Activity Inv CCF: Time Sync Error Inv CCF: Social Media Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Object Access Summary CCF: User Object Access Summary CCF: Audit Log Summary CCF: Config/Policy Change Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Social Media Summary CCF: Applications Accessed By User Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Corroborated Account Anomalies CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Concurrent VPN from Multiple Locations CCF: Software Install CCF: Software Uninstall CCF: Concurrent VPN from Same User CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified	Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	Management Activity Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Backup Activity Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
RM.5.155					
CA.2.157					
CA.2.158	CCF: FIM Abnormal Activity CCF: FIM Add Activity CCF: FIM General Activity CCF: FIM Information CCF: Data Loss Prevention CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Large Outbound Transfer CCF: Abnormal Amount of Data Transferred CCF: Corroborated Data Access Anomalies CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Config Deleted/ Disabled CCF: Critical Event After Attack CCF: Social Media Event CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Backup Failure Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Social Media Inv CCF: Critical Environment Error Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Signature Activity Inv CCF: Config/Policy Change	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Backup Information CCF: Software Install CCF: Software Uninstall CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Corroborated Account Anomalies CCF: Auth After Security Event CCF: Abnormal Origin Location	Granted Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm CCF: Blacklisted Account Alarm	Inv CCF: Patch Activity Inv CCF: Time Sync Error Inv CCF: Backup Activity Inv CCF: Audit Log Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv	CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Backup Activity Summary CCF: Audit Log Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	
CA.2.159					

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
CA.3.161	CCF: FIM Abnormal Activity CCF: FIM Add Activity CCF: FIM General Activity CCF: FIM Information CCF: Data Loss Prevention CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Large Outbound Transfer CCF: Abnormal Amount of Data Transferred CCF: Corroborated Data Access Anomalies CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Config Deleted/ Disabled CCF: Critical Event After Attack CCF: Social Media Event CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Distributed Brute Force	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Backup Failure Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Social Media Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Patch Activity Inv CCF: Time Sync Error Inv CCF: Backup Activity Inv	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Backup Activity	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: External Brute Force Auths CCF: Backup Information CCF: Software Install CCF: Software Uninstall CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Corroborated Account Anomalies CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified	CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm CCF: Blacklisted Account Alarm	CCF: Audit Log Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	Summary CCF: Audit Log Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
CA.3.162					
CA.4.163					
CA.4.164					
CA.4.227					
SA.3.169					
SA.4.171	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Config Deleted/ Disabled CCF: Social Media Event CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Backup Failure Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Audit Logging Stopped Alarm	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Social Media Inv CCF: Critical Environment	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Backup Information CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies CCF: Large Outbound Transfer CCF: Disabled Account Auth Success CCF: Config Change After Attack CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Corroborated Account Anomalies CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified CCF: Password Modified by Admin CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from	CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Privilege Escalation After Attack Alarm	Error Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Patch Activity Inv CCF: Time Sync Error Inv CCF: Backup Activity Inv CCF: Audit Log Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	CCF: Social Media Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Backup Activity Summary CCF: Audit Log Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Same User CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified				
SA.4.173	CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: FIM Information CCF: Data Destruction CCF: Data Loss Prevention CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies CCF: Backup Information CCF: Config Change After Attack CCF: Abnormal Amount of Data Transferred CCF: Large Outbound Transfer	CCF: FIM Delete Activity Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch	CCF: Use Of Non-Encrypted Protocols Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: Audit Log Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Config/Policy Change Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Patch Activity Inv CCF: Backup Activity Inv CCF: Time Sync Error Inv CCF: Social Media Inv CCF: Host Access Granted	CCF: Use Of Non-Encrypted Protocols Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Object Access Summary CCF: User Object Access Summary CCF: Audit Log Summary CCF: Config/Policy Change Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Social Media Event CCF: Misuse CCF: Config Deleted/ Disabled CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Disabled Account Auth Success CCF: Corroborated Account Anomalies CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Software Install	Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Backup Failure Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm	And Revoked Inv CCF: Applications Accessed By User Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	CCF: Time Sync Error Summary CCF: Social Media Summary CCF: Applications Accessed By User Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Software Uninstall CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified			Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Backup Activity Summary	
SC.1.175	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Backup Failure Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: PRD Envir Config/Policy Change Alarm	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Rogue Access Point Inv	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Compromises Detected Summary CCF: Rogue Access Point	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Config Deleted/ Disabled CCF: Social Media Event CCF: Config Change After Attack CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Backup Information CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Data Loss Prevention CCF: Corroborated Data Access Anomalies CCF: Large Outbound Transfer CCF: Disabled Account Auth Success CCF: Corroborated Account Anomalies CCF: Corroborated Account Anomalies CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified CCF: Password Modified by Another User CCF: Distributed Brute Force CCF: External Brute Force	CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Social Media Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Patch Activity Inv CCF: Time Sync Error Inv CCF: Backup Activity Inv CCF: Audit Log Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Backup Activity Summary CCF: Audit Log Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Auths CCF: Password Modified by Admin CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location			Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	
SC.1.176	CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: FIM Information CCF: Data Destruction CCF: Data Loss Prevention CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies CCF: Backup Information CCF: Config Change After Attack CCF: Abnormal Amount of	CCF: FIM Delete Activity Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: PRD Envir Config/Policy	CCF: Use Of Non-Encrypted Protocols Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: Audit Log Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Config/Policy Change Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Patch Activity Inv CCF: Backup Activity Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Object Access Summary CCF: User Object Access Summary CCF: Audit Log Summary CCF: Config/Policy Change Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Data Transferred CCF: Large Outbound Transfer CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Social Media Event CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Config Deleted/ Disabled CCF: Critical Event After Attack CCF: Disabled Account Auth Success CCF: Corroborated Account Anomalies CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Excessive Authentication Failure Rule	Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Backup Failure Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Time Sync Error Inv CCF: Social Media Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Compromises Detected Inv CCF: Physical Access Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Social Media Summary CCF: Applications Accessed By User Summary CCF: Top Suspicious Users CCF: User Misuse Summary CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Physical Access Summary CCF: Auth Failure Summary CCF: Access Failure Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Software Install CCF: Software Uninstall CCF: Account Deleted Rule CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified			CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Backup Activity Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
SC.2.178	CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Config Change After Attack CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Concurrent VPN from Multiple Locations CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Corroborated Account Anomalies CCF: Disabled Account Auth Success CCF: Corroborated Data Access Anomalies CCF: Concurrent VPN from Same User CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User	CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Early TLS/SSL Alarm CCF: Non-Encrypted Protocol Alarm CCF: Blacklisted Account Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: User Object Access Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Escalation Inv CCF: Privileged Account Modification Inv CCF: Audit Log Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Object Access Inv CCF: Password Modification Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: Top Suspicious Users CCF: User Object Access Summary CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Audit Log Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Object Access Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event				
SC.2.179	CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: FIM Information CCF: Data Destruction CCF: Data Loss Prevention CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies CCF: Backup Information CCF: Abnormal Amount of Data Transferred CCF: Large Outbound Transfer CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Social Media Event CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack	CCF: FIM Delete Activity Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Backup Failure Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access	CCF: Use Of Non-Encrypted Protocols Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: Audit Log Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Config/Policy Change Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Patch Activity Inv CCF: Backup Activity Inv CCF: Time Sync Error Inv CCF: Social Media Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Object Access Summary CCF: User Object Access Summary CCF: Audit Log Summary CCF: Config/Policy Change Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Social Media Summary CCF: Applications Accessed By User Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Config Deleted/ Disabled CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Disabled Account Auth Success CCF: Corroborated Account Anomalies CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Concurrent VPN from Multiple Locations CCF: Software Install CCF: Software Uninstall CCF: Concurrent VPN from Same User CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location	Granted Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Backup Activity Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified				
SC.3.177	CCF: FIM Abnormal Activity CCF: FIM Add Activity CCF: FIM General Activity CCF: FIM Information CCF: Data Loss Prevention CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Large Outbound Transfer CCF: Abnormal Amount of Data Transferred CCF: Corroborated Data Access Anomalies CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Config Deleted/ Disabled CCF: Critical Event After Attack CCF: Attack then External Connection	CCF: FIM Delete Activity Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: PRD Envir Config/Policy Change Alarm	CCF: Use Of Non-Encrypted Protocols Inv CCF: Audit Log Inv CCF: Config/Policy Change Inv CCF: LogRhythm Data Loss Defender Log Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: Audit Log Summary CCF: Config/Policy Change Summary CCF: LogRhythm Data Loss Defender Log Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
SC.3.180	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Config Deleted/ Disabled CCF: Social Media Event CCF: Config Change After Attack CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Backup Information CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Backup Failure Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: Compromise Detected	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Social Media Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Patch Activity Inv CCF: Time Sync Error Inv CCF: Backup Activity Inv CCF: Audit Log Inv CCF: Privileged Account Modification Inv CCF: Privileged Account	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Backup Activity	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Large Outbound Transfer CCF: Corroborated Account Anomalies CCF: Corroborated Account Anomalies CCF: Disabled Account Auth Success CCF: Multiple Account Passwords Modified by Admin CCF: Password Modified by Another User CCF: Admin Password Modified CCF: Password Modified by Admin CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Software Install CCF: Software Uninstall CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths	Alarm CCF: Denial Of Service Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm	Escalation Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	Summary CCF: Audit Log Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Auth After Security Event CCF: Abnormal Origin Location				
SC.3.181	CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: FIM Information CCF: Data Destruction CCF: Data Loss Prevention CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies CCF: Abnormal Amount of Data Transferred CCF: Large Outbound Transfer CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Abnormal Origin Location CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Misuse CCF: Critical Event After Attack CCF: Social Media Event CCF: Disabled Account Auth Success	CCF: FIM Delete Activity Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Backup Failure Alarm CCF: Time Sync Error Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Rogue Access Point Inv CCF: Config/Policy Change Inv CCF: Signature Activity Inv CCF: Patch Activity Inv CCF: Critical Environment Error Inv CCF: Audit Log Inv CCF: Compromises Detected Inv CCF: Malware Detected Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Audit Log Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Corroborated Account Anomalies CCF: Config Change After Attack CCF: Corroborated Account Anomalies CCF: Disabled Account Auth Success CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Backup Information CCF: Software Install CCF: Software Uninstall CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account	Granted Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm CCF: Blacklisted Account Alarm	CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Suspected Wireless Attack Inv CCF: Vulnerability Detected Inv CCF: Backup Activity Inv CCF: Password Modification Inv	Activity Summary CCF: Priv Account Management Activity Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Suspected Wireless Attack Summary CCF: Backup Activity Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Passwords Modified by Admin CCF: Admin Password Modified				
SC.3.182	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: Social Media Event CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies CCF: Large Outbound Transfer CCF: Disabled Account Auth Success CCF: Corroborated Account Anomalies CCF: Social Media Event CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Concurrent VPN from	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Use Of Non-Encrypted Protocols Inv CCF: Object Access Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: User Object Access Inv CCF: Unknown User Account Inv CCF: Social Media Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: GeoIP Inv CCF: Host Access Granted And Revoked Inv CCF: Audit Log Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Object Access Summary CCF: Applications Accessed By User Summary CCF: Top Suspicious Users CCF: User Object Access Summary CCF: Object Access Summary CCF: Social Media Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: GeoIP Summary CCF: Social Media Summary CCF: Audit Log Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Multiple Locations CCF: Concurrent VPN from Same User CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Multiple Account Passwords Modified by Admin CCF: Password Modified by Another User CCF: Admin Password Modified CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event			Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary	
SC.3.183	CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: FIM Information CCF: Data Destruction CCF: Data Loss Prevention CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies CCF: Backup Information	CCF: FIM Delete Activity Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm	CCF: Use Of Non-Encrypted Protocols Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: Audit Log Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Config/Policy Change Inv CCF: Critical Environment Error Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Object Access Summary CCF: User Object Access Summary CCF: Audit Log Summary CCF: Config/Policy Change Summary CCF: Critical Environment	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Config Change After Attack CCF: Abnormal Amount of Data Transferred CCF: Large Outbound Transfer CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Social Media Event CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Config Deleted/ Disabled CCF: Critical Event After Attack CCF: Disabled Account Auth Success CCF: Corroborated Account Anomalies CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from	CCF: Failed Audit Log Write Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Backup Failure Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Signature Activity Inv CCF: Patch Activity Inv CCF: Backup Activity Inv CCF: Time Sync Error Inv CCF: Social Media Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Compromises Detected Inv CCF: Physical Access Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Social Media Summary CCF: Applications Accessed By User Summary CCF: Top Suspicious Users CCF: User Misuse Summary CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Physical Access Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Same User CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Software Install CCF: Software Uninstall CCF: Account Deleted Rule CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified			CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Backup Activity Summary	
SC.3.184	CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: FIM Information CCF: Data Destruction CCF: Data Loss Prevention CCF: Data Exfiltration Observed CCF: Corroborated Data	CCF: FIM Delete Activity Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm	CCF: Use Of Non-Encrypted Protocols Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: Audit Log Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Config/Policy Change Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Object Access Summary CCF: User Object Access Summary CCF: Audit Log Summary CCF: Config/Policy Change	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Access Anomalies CCF: Backup Information CCF: Config Change After Attack CCF: Abnormal Amount of Data Transferred CCF: Large Outbound Transfer CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Social Media Event CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Config Deleted/ Disabled CCF: Critical Event After Attack CCF: Disabled Account Auth Success CCF: Corroborated Account Anomalies CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Concurrent VPN from	CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Backup Failure Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Patch Activity Inv CCF: Backup Activity Inv CCF: Time Sync Error Inv CCF: Social Media Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Compromises Detected Inv CCF: Physical Access Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv	Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Social Media Summary CCF: Applications Accessed By User Summary CCF: Top Suspicious Users CCF: User Misuse Summary CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Multiple Locations CCF: Concurrent VPN from Same User CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Software Install CCF: Software Uninstall CCF: Account Deleted Rule CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified		CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	CCF: Physical Access Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Backup Activity Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
SC.3.185	CCF: Social Media Event CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: Social Media Event CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies CCF: Large Outbound Transfer CCF: Blacklist Location Auth CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Multiple Account	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Blacklisted Account Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Use Of Non-Encrypted Protocols Inv CCF: Social Media Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: GeoIP Inv CCF: Audit Log Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Host Access Granted And Revoked Inv CCF: Unknown User Account Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Password Modification Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: Social Media Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: GeoIP Summary CCF: Audit Log Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Passwords Modified by Admin CCF: Password Modified by Another User CCF: Admin Password Modified CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event				
SC.3.186					
SC.3.187					
SC.3.188	CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: FIM Information CCF: Data Destruction CCF: Data Loss Prevention CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies CCF: Abnormal Amount of Data Transferred CCF: Large Outbound Transfer CCF: Corroborated Account Anomalies	CCF: FIM Delete Activity Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm	CCF: Use Of Non-Encrypted Protocols Inv CCF: Audit Log Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Patch Activity Inv CCF: Backup Activity Inv CCF: Time Sync Error Inv CCF: User Misuse Inv CCF: GeoIP Inv CCF: Privileged Account Modification Inv CCF: Privileged Account	CCF: Use Of Non-Encrypted Protocols Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Audit Log Summary CCF: Critical Environment Error Summary CCF: Time Sync Error Summary CCF: GeoIP Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Config Deleted/ Disabled CCF: Critical Event After Attack CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Software Install CCF: Software Uninstall CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Attack then External Connection	CCF: PRD Envir Signature Failure Alarm CCF: Backup Failure Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm CCF: Priv Group Access Granted Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm	Escalation Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Host Access Granted And Revoked Inv CCF: Unknown User Account Inv CCF: Password Modification Inv	CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Top Suspicious Users CCF: Signature Activity Summary CCF: Patch Activity Summary CCF: User Misuse Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified				
SC.3.189					
SC.3.190	CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: FIM Information CCF: Data Destruction CCF: Data Loss Prevention CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies CCF: Backup Information CCF: Abnormal Amount of Data Transferred CCF: Large Outbound Transfer CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity	CCF: FIM Delete Activity Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm	CCF: Use Of Non-Encrypted Protocols Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: Audit Log Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Config/Policy Change Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Patch Activity Inv CCF: Backup Activity Inv CCF: Time Sync Error Inv CCF: Social Media Inv CCF: Host Access Granted And Revoked Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Object Access Summary CCF: User Object Access Summary CCF: Audit Log Summary CCF: Config/Policy Change Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Social Media Event CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Config Deleted/ Disabled CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Disabled Account Auth Success CCF: Corroborated Account Anomalies CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Concurrent VPN from Multiple Locations CCF: Software Install CCF: Software Uninstall CCF: Concurrent VPN from Same User CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule	CCF: PRD Envir Signature Failure Alarm CCF: Backup Failure Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Applications Accessed By User Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	Summary CCF: Social Media Summary CCF: Applications Accessed By User Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified			CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Backup Activity Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
SC.3.191	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Backup Information CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Large Outbound Transfer CCF: Disabled Account Auth Success CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Config Deleted/ Disabled CCF: Attack then External Connection CCF: Corroborated Account Anomalies	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: Backup Failure Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Critical Environment Error Inv CCF: Backup Activity Inv CCF: Audit Log Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Unknown User Account Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Critical Environment Error Summary CCF: Config/Policy Change Summary CCF: Backup Activity Summary CCF: Audit Log Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
SC.3.192	NetMon	NetMon	NetMon	NetMon	NetMon
SC.3.193					
SC.4.197	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: Social Media Event CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies CCF: Large Outbound Transfer CCF: Disabled Account Auth Success CCF: Corroborated Account Anomalies CCF: Social Media Event CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Concurrent VPN from	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Use Of Non-Encrypted Protocols Inv CCF: Object Access Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: User Object Access Inv CCF: Unknown User Account Inv CCF: Social Media Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: GeoIP Inv CCF: Host Access Granted And Revoked Inv CCF: Audit Log Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Object Access Summary CCF: Applications Accessed By User Summary CCF: Top Suspicious Users CCF: User Object Access Summary CCF: Object Access Summary CCF: Social Media Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: GeoIP Summary CCF: Social Media Summary CCF: Audit Log Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Multiple Locations CCF: Concurrent VPN from Same User CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Multiple Account Passwords Modified by Admin CCF: Password Modified by Another User CCF: Admin Password Modified CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event			Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary	
SC.4.228	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Config Deleted/ Disabled CCF: Social Media Event CCF: Config Change After Attack CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Backup Information CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies CCF: Large Outbound Transfer CCF: Corroborated Account Anomalies CCF: Corroborated Account Anomalies CCF: Disabled Account Auth Success CCF: Multiple Account Passwords Modified by Admin CCF: Password Modified by	Alarm CCF: Backup Failure Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm	CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Social Media Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Patch Activity Inv CCF: Time Sync Error Inv CCF: Backup Activity Inv CCF: Audit Log Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Backup Activity Summary CCF: Audit Log Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Auth Failure Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Another User CCF: Admin Password Modified CCF: Password Modified by Admin CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Software Install CCF: Software Uninstall CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location			CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	
SC.4.199	TIS	TIS	TIS	TIS	TIS
SC.4.202					
SC.4.229					

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
SC.5.198	Netmon	Netmon	Netmon	Netmon	Netmon
SC.5.230	CCF: Excessive Authentication Failure Rule CCF: Distributed Brute Force CCF: External Brute Force Auths	CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm	CCF: Excessive Authentication Failure Inv CCF: Audit Log Inv	CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Audit Log Summary	
SC.5.208					
SI.1.210	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Social Media Event CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Config Deleted/ Disabled CCF: Windows RunAs Privilege Escalation	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Backup Failure Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Backup Information CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies CCF: Large Outbound Transfer CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Corroborated Account Anomalies CCF: Corroborated Account Anomalies CCF: Disabled Account Auth Success CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths	CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Social Media Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Patch Activity Inv CCF: Time Sync Error Inv CCF: Backup Activity Inv CCF: Audit Log Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Backup Activity Summary CCF: Audit Log Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified			CCF: Account Modification Summary CCF: Term Account Activity Summary	
SI.1.211	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Config Deleted/ Disabled CCF: Social Media Event CCF: Config Change After Attack	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Backup Failure Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Backup Information CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies CCF: Large Outbound Transfer CCF: Disabled Account Auth Success CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Corroborated Account Anomalies CCF: Corroborated Account Anomalies CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Attack then External Connection	CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: Denial Of Service Alarm CCF: Privilege Escalation After Attack Alarm CCF: Compromise Detected Alarm	CCF: Social Media Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Patch Activity Inv CCF: Time Sync Error Inv CCF: Backup Activity Inv CCF: Audit Log Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Backup Activity Summary CCF: Audit Log Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified			CCF: Account Modification Summary CCF: Term Account Activity Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
SI.1.212	CCF: FIM Abnormal Activity CCF: FIM Add Activity CCF: FIM General Activity CCF: FIM Information CCF: Data Loss Prevention CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Large Outbound Transfer CCF: Abnormal Amount of Data Transferred CCF: Corroborated Data Access Anomalies CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Config Modified CCF: Social Media Event CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Blacklist Location Auth CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Config Deleted/ Disabled CCF: Software Install CCF: Software Uninstall CCF: Excessive Authentication Failure Rule CCF: Account Modification	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Unknown User Account Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Use Of Non-Encrypted Protocols Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: User Object Access Inv CCF: Object Access Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Config/Policy Change Inv CCF: Patch Activity Inv CCF: Signature Activity Inv CCF: Critical Environment Error Inv CCF: Audit Log Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Object Access Summary CCF: User Object Access Summary CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Patch Activity Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Critical Environment Error Summary CCF: Audit Log Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Abnormal Origin Location CCF: Corroborated Account Anomalies CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified CCF: Local Account Created and Used CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event			CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	
SI.1.213	CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: FIM Information CCF: Data Destruction CCF: Data Loss Prevention CCF: Data Exfiltration Observed CCF: Corroborated Data	CCF: FIM Delete Activity Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm	CCF: Use Of Non-Encrypted Protocols Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: Audit Log Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Config/Policy Change Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Object Access Summary CCF: User Object Access Summary CCF: Audit Log Summary CCF: Config/Policy Change	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Access Anomalies CCF: Backup Information CCF: Config Change After Attack CCF: Abnormal Amount of Data Transferred CCF: Large Outbound Transfer CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Social Media Event CCF: Misuse CCF: Config Deleted/ Disabled CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Disabled Account Auth Success CCF: Corroborated Account Anomalies CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from	CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Backup Failure Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Software Install Fail Alarm CCF: Software Uninstall Fail Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Patch Activity Inv CCF: Backup Activity Inv CCF: Time Sync Error Inv CCF: Social Media Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv	Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Social Media Summary CCF: Applications Accessed By User Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Same User CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Software Install CCF: Software Uninstall CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified		CCF: Deleted Account Inv CCF: Password Modification Inv	CCF: Social Media Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Backup Activity Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	
SI.2.214	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: GeoIP General Activity CCF: GeoIP Blacklisted	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Region Activity CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Config Deleted/ Disabled CCF: Social Media Event CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Backup Information CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies CCF: Large Outbound Transfer CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Corroborated Account Anomalies CCF: Corroborated Account Anomalies CCF: Disabled Account Auth Success CCF: Excessive	CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Backup Failure Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Social Media Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Patch Activity Inv CCF: Time Sync Error Inv CCF: Backup Activity Inv CCF: Audit Log Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv	CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Backup Activity Summary CCF: Audit Log Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified		CCF: Deleted Account Inv CCF: Password Modification Inv	Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	
SI.2.216	CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: FIM Information CCF: Data Destruction CCF: Data Loss Prevention CCF: Data Exfiltration Observed CCF: Corroborated Data	CCF: FIM Delete Activity Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm	CCF: Use Of Non-Encrypted Protocols Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: Audit Log Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Config/Policy Change Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Object Access Summary CCF: User Object Access Summary CCF: Audit Log Summary CCF: Config/Policy Change	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Access Anomalies CCF: Backup Information CCF: Config Change After Attack CCF: Abnormal Amount of Data Transferred CCF: Large Outbound Transfer CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Social Media Event CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Config Deleted/ Disabled CCF: Disabled Account Auth Success CCF: Corroborated Account Anomalies CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Concurrent VPN from	CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Backup Failure Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Patch Activity Inv CCF: Backup Activity Inv CCF: Time Sync Error Inv CCF: Social Media Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv	Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Social Media Summary CCF: Applications Accessed By User Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Multiple Locations CCF: Concurrent VPN from Same User CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified		CCF: Deleted Account Inv CCF: Password Modification Inv	CCF: Social Media Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Backup Activity Summary	
SI.2.217	CCF: FIM Abnormal Activity CCF: FIM Add Activity CCF: FIM General Activity CCF: FIM Information CCF: Data Loss Prevention CCF: Data Destruction CCF: Data Exfiltration Observed CCF: Large Outbound	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Transfer CCF: Abnormal Amount of Data Transferred CCF: Corroborated Data Access Anomalies CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Config Deleted/ Disabled CCF: Social Media Event CCF: Config Change After Attack CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Backup Information CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule	CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Backup Failure Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Privilege Escalation After Attack Alarm CCF: Blacklisted Account Alarm	CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Social Media Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Patch Activity Inv CCF: Time Sync Error Inv CCF: Backup Activity Inv CCF: Audit Log Inv CCF: Compromises Detected Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv	CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Backup Activity Summary CCF: Audit Log Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Corroborated Account Anomalies CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified		CCF: Deleted Account Inv CCF: Password Modification Inv	Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
SI.3.218	CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Abnormal Origin Location CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Config Deleted/ Disabled CCF: Critical Event After Attack CCF: Social Media Event CCF: Disabled Account Auth Success CCF: Corroborated Account Anomalies CCF: Corroborated Account Anomalies CCF: Disabled Account Auth Success CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used	CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Privilege Escalation After Attack Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Backup Failure Alarm	CCF: Suspicious Users Inv CCF: GeoIP Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Audit Log Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Host Access Granted And Revoked Inv CCF: Unknown User Account Inv CCF: Backup Activity Inv CCF: User Misuse Inv CCF: Password Modification Inv	CCF: Top Suspicious Users CCF: User Misuse Summary CCF: GeoIP Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Audit Log Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Backup Activity Summary	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Blacklist Location Auth CCF: Backup Information CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified				

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
SI.3.219	CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Blacklist Location Auth CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified CCF: Password Modified by Another User CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Unknown User Account Alarm CCF: Priv Group Access Granted Alarm CCF: Blacklisted Account Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Use Of Non-Encrypted Protocols Inv CCF: Audit Log Inv CCF: GeoIP Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Host Access Granted And Revoked Inv CCF: Unknown User Account Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Password Modification Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: Audit Log Summary CCF: GeoIP Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Top Suspicious Users CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary	CCF: Unknown User Account Detail CCF: Host Access Granted And Revoked Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
SI.3.220					
SI.4.221	CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: FIM Information CCF: Data Destruction CCF: Data Loss Prevention CCF: Data Exfiltration Observed CCF: Corroborated Data Access Anomalies CCF: Backup Information CCF: Config Change After Attack CCF: Abnormal Amount of Data Transferred CCF: Large Outbound Transfer CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Social Media Event CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Config Deleted/ Disabled CCF: Disabled Account Auth Success CCF: Corroborated Account	CCF: FIM Delete Activity Alarm CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Backup Failure Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access Granted Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected	CCF: Use Of Non-Encrypted Protocols Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: Audit Log Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Config/Policy Change Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Patch Activity Inv CCF: Backup Activity Inv CCF: Time Sync Error Inv CCF: Social Media Inv CCF: Host Access Granted And Revoked Inv CCF: Applications Accessed By User Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Privileged Account Modification Inv CCF: Privileged Account Escalation Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv	CCF: Use Of Non-Encrypted Protocols Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Object Access Summary CCF: User Object Access Summary CCF: Audit Log Summary CCF: Config/Policy Change Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error Summary CCF: Social Media Summary CCF: Applications Accessed By User Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Anomalies CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account Passwords Modified by Admin CCF: Admin Password Modified	Alarm CCF: Compromise Detected Alarm CCF: Denial Of Service Alarm CCF: Privilege Escalation After Attack Alarm	CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	Management Activity Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary CCF: Backup Activity Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
SI.5.222	MITRE	MITRE	MITRE	MITRE	MITRE
SI.5.223	CCF: Abnormal Amount of Data Transferred CCF: FIM Information CCF: Data Loss Prevention CCF: FIM General Activity CCF: FIM Add Activity CCF: FIM Abnormal Activity CCF: GeoIP General Activity CCF: GeoIP Blacklisted Region Activity CCF: Misuse CCF: Config Change After Attack CCF: Config Change then Critical Error CCF: Critical Event After Attack CCF: Config Deleted/ Disabled CCF: Social Media Event CCF: Config Change After Attack CCF: Windows RunAs Privilege Escalation CCF: Linux sudo Privilege Escalation CCF: Local Account Created and Used CCF: Blacklist Location Auth CCF: Backup Information CCF: Data Destruction CCF: Data Exfiltration Observed	CCF: Non-Encrypted Protocol Alarm CCF: Early TLS/SSL Alarm CCF: FIM Delete Activity Alarm CCF: Rogue Access Point Alarm CCF: Suspected Wireless Attack Alarm CCF: Malware Alarm CCF: Vulnerability Detected Alarm CCF: Backup Failure Alarm CCF: LogRhythm Silent Log Source Error Alarm CCF: PRD Envir Config/Policy Change Alarm CCF: Time Sync Error Alarm CCF: Critical/PRD Envir Patch Failure Alarm CCF: PRD Envir Signature Failure Alarm CCF: Audit Logging Stopped Alarm CCF: Audit Log Cleared Alarm CCF: Failed Audit Log Write Alarm CCF: Unknown User Account Alarm CCF: Blacklisted Account Alarm CCF: Priv Group Access	CCF: Physical Access Inv CCF: Host Access Granted And Revoked Inv CCF: Use Of Non-Encrypted Protocols Inv CCF: Applications Accessed By User Inv CCF: LogRhythm Data Loss Defender Log Inv CCF: Suspicious Users Inv CCF: Object Access Inv CCF: User Object Access Inv CCF: User Misuse Inv CCF: Unknown User Account Inv CCF: GeoIP Inv CCF: Rogue Access Point Inv CCF: Suspected Wireless Attack Inv CCF: Malware Detected Inv CCF: Vulnerability Detected Inv CCF: Social Media Inv CCF: Critical Environment Error Inv CCF: Signature Activity Inv CCF: Config/Policy Change Inv CCF: Patch Activity Inv CCF: Time Sync Error Inv CCF: Backup Activity Inv CCF: Audit Log Inv CCF: Privileged Account	CCF: Physical Access Summary CCF: Use Of Non-Encrypted Protocols Summary CCF: Applications Accessed By User Summary CCF: LogRhythm Data Loss Defender Log Summary CCF: Top Suspicious Users CCF: Object Access Summary CCF: User Object Access Summary CCF: User Misuse Summary CCF: GeoIP Summary CCF: Compromises Detected Summary CCF: Rogue Access Point Summary CCF: Suspected Wireless Attack Summary CCF: Malware Detected Summary CCF: Vulnerability Detected Summary CCF: Social Media Summary CCF: Critical Environment Error Summary CCF: Signature Activity Summary CCF: Config/Policy Change Summary CCF: Patch Activity Summary CCF: Time Sync Error	CCF: Host Access Granted And Revoked Detail CCF: Unknown User Account Detail

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	CCF: Corroborated Data Access Anomalies CCF: Large Outbound Transfer CCF: Disabled Account Auth Success CCF: Distributed Brute Force CCF: External Brute Force Auths CCF: Corroborated Account Anomalies CCF: Corroborated Account Anomalies CCF: Excessive Authentication Failure Rule CCF: Account Modification CCF: Account Enabled Rule CCF: Account Disabled Rule CCF: Account Deleted Rule CCF: Concurrent VPN from Multiple Locations CCF: Concurrent VPN from Same User CCF: Attack then External Connection CCF: Auth After Numerous Failed Auths CCF: Auth After Security Event CCF: Abnormal Origin Location CCF: Password Modified by Admin CCF: Password Modified by Another User CCF: Multiple Account	Granted Alarm CCF: Denial Of Service Alarm CCF: Privilege Escalation After Attack Alarm CCF: Compromise Detected Alarm	Modification Inv CCF: Privileged Account Escalation Inv CCF: Compromises Detected Inv CCF: Denial Of Service Inv CCF: Excessive Authentication Failure Inv CCF: Account Modification Inv CCF: Enabled Account Inv CCF: Disabled Account Inv CCF: Deleted Account Inv CCF: Password Modification Inv	Summary CCF: Backup Activity Summary CCF: Audit Log Summary CCF: User Priv Escalation (Windows) Summary CCF: User Priv Escalation (SU & SUDO) Summary CCF: Priv Authentication Activity Summary CCF: Priv Account Management Activity Summary CCF: Auth Failure Summary CCF: Access Failure Summary CCF: Auth Success Summary CCF: Access Success Summary CCF: Account Enabled Summary CCF: Account Disabled Summary CCF: Account Deleted Summary CCF: Account Modification Summary CCF: Term Account Activity Summary	

Control ID	Rules	AIE Alerts	Investigations	Summary Reports	Detailed Report
	Passwords Modified by Admin CCF: Admin Password Modified				

Cybersecurity Maturity Model Certification Deployment Guide

This guide describes how to implement the LogRhythm Cybersecurity Maturity Model Certification (CMMC) module. The CMMC suite provides pre-bundled content such as AI Engine (AIE) rules, alarms, investigations, lists, and reports that help organizations pursuing best practice adherence around the CMMC guidelines. This guide provides control mapping between LogRhythm SIEM content and guidelines within the CMMC publication. Monitoring and awareness of risk exposures across an organization's environment(s) are foundational aspects of CMMC adherence. The LogRhythm SIEM serves as an essential tool as an organization matures its compliance and security posture. Organizations can use the content within this compliance automation suite to facilitate their adherence to certain guidelines of the CMMC.

Many of these phases include key resources that can be leveraged in the deployment of the compliance suite. The CMMC module provides pre-bundled content available through the Knowledge Base and part of the foundation around the Consolidated Compliance Framework (CCF) methodology. An organization, with confirmation from auditors, can use the module content to augment control objectives and support efforts to follow CMMC guidelines. AIE Alarms assist with quickly identifying risk exposures, while Case Management enables centralized collection of forensic data, including audit evidence, to support incident reporting, response time, and remediation requirements. This pre-bundled content is automatically associated with the CMMC control objectives that are supported by LogRhythm Enterprise. Various lists are also available, some of which are pre-configured and others that can be catered to your environment, processes, and system classifications. Collectively, these and other LogRhythm features provide a road map to help organizations transition from compliance readiness to true security, risk-based organizations. Our team’s interpretations of the augmented best practice guidelines can be found in the matrices of this module. LogRhythm’s core set of content offered through the Consolidated Compliance Framework (CCF) is mapped to CMMC guidelines, offering a streamlined approach to compliance through SIEM technology. LogRhythm SIEM technology and content align with the CMMC guideline families to strengthen an organization’s security posture.

After you configure the compliance automation suite, the LogRhythm Platform Manager includes the proper components needed to support CMMC guideline adherence. As AIE rules, alarms, reports, and investigations are correlated with in-scope log sources and hosts, your compliance and security teams can leverage powerful data. You can also schedule reports for periodic generation and delivery or generate them on demand for various audiences. To identify areas of non-compliance in real-time, you can leverage investigations and alarms for immediate analysis of activities that impact your organization's cardholder data systems. Once a control failure or risk exposure is realized, you can quickly use Case Management to organize and understand this event. This helps the organization reduce the mean time to detection (MTTD) and mean time to respond (MTTR) to not only ensure reporting time requirements are met but help limit the time of risk realization and damage.

As with any framework, some controls and best practices offered may require additional tailoring to augment them appropriately as determined by the organization. We encourage our LogRhythm community administrators and analysts to create their own AIE rules, alarms, investigations, and reports to augment more controls than we can provide with pre-bundled content. Many tools are available for this, including the wide range of logs in the LogRhythm MPE Rule Builder, Log Library, and ECHO tool set. Professional services and Analytics Co Pilot services are available as needed to assist with creating and tailoring custom rules and actions.

LogRhythm content is designed to be used by various audiences including internal and external auditors, executive management, control owners, program developers, IT security, IT operations, and other individuals or groups involved in the audit cycle.

Intended Audience

This guide is intended for LogRhythm Enterprise administrators and analysts who are responsible for maintaining compliance with various CMMC best practices. Monthly and weekly reporting packages can be established to provide forensic evidence and audit data to appropriate audiences for distribution, including security operations, security

management, IT operations, audit, and executive management. The reporting packages, the content included, and the frequency can be adjusted according to the needs of your audience.

This guide details the installation, configuration, and verification of objects used in the CMMC module. When this section is complete, the LogRhythm Platform Manager enabled content will begin to provide value around your CMMC compliance efforts. The process involves the following steps:

CMMC Deployment Guide—Install and Enable the Compliance Module

CMMC Deployment Guide—Verify the Installation

CMMC Deployment Guide—Configure the Compliance Module

CMMC Deployment Guide – Install and Enable the Compliance Module

The NIST Compliance Automation Suite is provided as part of the LogRhythm Knowledge Base. Updating the LogRhythm Knowledge Base automatically creates the proper Lists, AIE Rules, Investigations, Reports, Reporting Packages. Follow the instructions below to Import the Knowledge Base.

1. Download the latest Knowledge Base, available under Documentation & Downloads on the LogRhythm Community.
2. Open the LogRhythm Client Console.
3. On the **Tools** menu, click **Knowledge**, and then click **Knowledge Base Manager**.

   > To open the Knowledge Base Manager, the Deployment Manager must be closed.

4. On the **File** menu, click **Import Knowledge Base File**.
5. Select the newly downloaded Knowledge Base file, and then click **Next** to unpack and validate it.
   This step takes a few minutes as the system unpacks the new Knowledge Base.
6. When the import is complete, you may have the option to preview common event changes.
   You should now be on step 4, Import Knowledge Base.
7. To import the Knowledge Base, click **Next**.
   Upon completion, the Import Progress Import Completed message appears.
8. Click **OK**.
   The Knowledge Base Updated message appears.
9. Click **OK**.
10. On the Knowledge Base Import Wizard, click **Close**.
11. In the Knowledge Base Modules grid, scroll down, search for **Compliance Automation Suite: CMMC**.
12. Locate the Enabled column in the grid for the desired module. If the box is checked, the Module is already enabled and available to users in the SIEM deployment. If the Enabled box is not selected, enable the Module by selecting its **Action** check box, right-clicking the Module name, clicking **Actions**, and then clicking **Enable Module**.
13. To import the Knowledge Base, click **Next**.
    You receive confirmation that the import was successful.
14. To review common event changes or close the Knowledge Base import dialog box, click **Next**.

CMMC Deployment Guide – Verify the Installation

After you install the Knowledge Base, you can configure the CMMC Compliance Automation Suite. This section shows how you can verify that the CMMC Compliance Automation Suite was properly installed.

Intelligent Indexing

Intelligent Indexing allows reports, investigations, and tails to keep the appropriate log data online in the Log Manager/Data Processor. Be careful when choosing which object to allow Intelligent Indexing because broad criteria can cause an exceptional amount of online data and overwhelm the Log Manager/Data Processor. For a list of Intelligent Indexing-capable objects and their recommended settings, see the module matrices.

Check Lists

Verify thirty-eight (38) total Lists are contained in the List Manager. The Lists are available in the CCF documentation.

> Establish Lists based on the content that is enabled (see the following three sections).

Check AIE Rules

Verify seventy (70) AI Engine Rules are contained in the Advanced Intelligence (AI) Engine Rule Manager found in the Deployment Manager.

Check Investigations

Verify thirty-three (33) Investigations are contained in the LogRhythm Client Console.

Check Summary Reports

Verify thirty-four (34) Summary Reports are contained in the Reports tab of the Report Center.

Check Detailed Reports

Verify two (2) Detailed Reports are contained in the Reports tab of the Report Center tab.

Check Reporting Packages

Verify four (4) Reporting Packages are contained in the Report Packages tab of the Report Center tab.

CMMC Deployment Guide – Configure the Compliance Module

For more information on configuration, best practices, and advanced feature instructions, see the Consolidated Compliance Framework Deployment Guide, available in the KB section under Documentation & Downloads on the LogRhythm Community. This guide will continually be updated as the functionality CCF can leverage grows and best practices are established.

Cybersecurity Maturity Model Certification User Guide

This section highlights some key reporting capabilities contained within the CMMC Compliance Automation Suite. LogRhythm has adopted the Consolidated Compliance Framework (CCF) approach to find common control approaches across various frameworks. This approach has been applied to the CMMC Compliance Automation Suite to help organizations streamline compliance objectives. Collectively many considered NIST and supporting frameworks making up CMMC as an influencer of compliance frameworks and is a core to LogRhythm's compliance approaches within CCF. All objects associated with this module follow the 'CCF: XXX' naming convention and utilize a restricted view to only allow those appropriate individuals to see CMMC specific content.

New profiles can be created for the Global Administrator, Global Analyst, Restricted Administrator, Restricted Analyst, and Web Service Administrator security roles. The security roles enable the Administrator to assign access to specific objects within the Entity to individual users. For example, many Restricted Analysts can be given access to Entity A, but not access to the same Log Sources within Entity A. Restricted Analyst 1 can have access to Log Sources 1, 2, and 3 on Entity A, while Restricted Analyst 2 has access to Log Sources 4, 5, and 6 on Entity A. This allows the organization to limit access to data and compliance content according to compliance needs.

As the organization identifies the need for a compliance module, in this instance CMMC, it is important to consider where the organization is along the Compliance Maturity Module. How mature the organization is determines what key resources are available to better align the RMiT module deployment with your compliance program. As the organization matures and key internal resources are established, the organization can easily pivot from a strong compliance base to establish strong security practices.

The guide is divided into the following sections:

CMMC User Guide – AI Engine Rules

AI Engine Rules leverage LogRhythm technology to correlate events across your environment, helping to identify events of interest and potential compliance issues. The goal for many of these rules is to quickly identify traffic coming from or going to a country or entity that should have restricted access based on the sensitive nature of the content, such as controlled unclassified information (CUI) for non-appproved entities. This can empower your organization to ensure policies are applied and to limit non-compliance.

Malware Alarm Rule

This alarm is the ability to continuously monitor the environment from all layers. This Alarm (#1217) is configured to alert when malicious activity occurs within the environment. This AIE Rule creates an event and notification alarm for malware detection on devices that have been designated as log sources or devices that support network monitoring.

Data Loss Prevention

Data Loss Prevention (DLP) within CCF is focused on protection of sensitive information within the organization's environment. DLP can be coupled with enabling File Integrity Monitoring (FIM) policies to provide a more robust monitoring of sensitive data and user activities impact that data. For this example, we look at three rules: CCF: Data Loss Prevention, CCF: Corroborated Data Access Anomalies, and Abnormal Amount of Data Transferred. In addition to FIM rules and policies, DLP provides objects that look at suspicious activity that may be indicative of malicious activity impacting sensitive data. For NIST 800-171, Controlled Unclassified Information (CUI) is the data of interest around which more robust controls must be established. Log sources should include systems storing sensitive data (as well as FIM application) to ensure monitoring controls are in place to track tampering of data or unauthorized transfers of data that occur.

LogRhythm Silent Log Source Error Alarm

Since LogRhythm Enterprise may serve as a mitigating control, it is crucial to be able to alarm on any instance where an in-scope log source does not send any logs. This rule (#1209) could be indicative of a control failure that needs to be addressed. This rule, in conjunction with other auditing failures, allows the organization to limit the time of control failure relating to logging and monitoring.

Log Requirements

These AIE rules cover all log sources in your environment but specifically require logs from anti-malware systems, firewalls, servers, workstations, security enforcing devices, access management systems, and vulnerability detection systems. When configured correctly, LogRhythm's advanced correlation and AIE rules provide near real-time alerts for malicious activities and/or attacks.

KB Content

Object Type	**Name**	**ID**
AIE Alarm Rule	CCF: Malware Alarm	1217

AIE Rule	CCF: Data Loss Prevention	1232
AIE Rule	CCF: Corroborated Data Access Anomalies	1201
AIE Rule	CCF: Abnormal Amount of Data Transferred	1230
AIE Alarm Rule	CCF: LogRhythm Silent Log Source Error Alarm	1209

CMMC User Guide – Investigations

Investigations can further assist in gathering vital information about security events. They can also provide basic information about an environment and the processes and activities within it. CMMC investigations can be part of a change control process to identify potential configuration changes, determine whether they are appropriate, and assess the implications for CMMC compliance. Investigations can also leverage defined user lists and examine any suspicious or potentially malicious activities surrounding accounts within the environment. Custom investigations can be configured to supplement those included within this module.

Log Requirements

The CCF: Vulnerability Detected Inv and other investigations related to potential malicious activity cover all log sources in your environment but specifically require logs from network security systems such as anti-malware systems, security enforcing devices, and vulnerability detection systems.

After investigations are configured correctly, IT and security operations can use them to analyze possible security events and evaluate and continuously improve your overall compliance and cyber security program. Further, various changes within data storage, security, and production environments must follow change control procedures to maintain business continuity and ensure that appropriate security protocols are not negatively impacted.

Sample Knowledge Base Content

Investigation Name	Investigation ID
CCF: Compromises Detected Inv	690
CCF: Config/Policy Change Inv	675
CCF: Malware Detected Inv	677
CCF: Patch Activity Inv	678
CCF: Signature Activity Inv	681
CCF: Social Media Inv	695
CCF: Suspicious Users Inv	685
CCF: Use of Non-Encrypted Protocols Inv	686
CCF: Vulnerability Detected Inv	684

Recommended Actions

Use CMMC investigations to pull additional details from log sources related to events of interest, monitor potential malicious activity, assist in reducing the mean time to detection (MTTD), and learn about vulnerabilities or exposure points within the environment. IT Security Operations and Management can leverage these investigations as a learning mechanism and a means to gather vulnerability data to implement controls and reduce the risk to exposure.

On the change control side, the goal is to support IT and security operations to ensure adherence to change control procedures. Assessing patch and signature management helps ensure appropriate security protocols are updated to foster business continuity and begin to establish a stronger security posture as an organization.

CMMC User Guide – Reports and Reporting Packages

Summary Reports and Detailed Reports

CMMC reporting is broken into summary reports and detailed reports to present various audiences with appropriate forensic log data. Summary reports provide a higher-level of information that may be appropriate for some audit and executive management requests. Detailed reports provide additional information, sometimes including raw log data, to facilitate IT and security operations. Additionally, any report can be run as an investigation to delve into forensic information around the activity of interest.

Reports serve as a good source of record for audit requests and can even be used for sample selection from a population of events. If you use reports for audit activities, you may be requested to trace report data back to the original log file to ensure the data is complete and accurate. You can also clone and modify reports to accommodate requests or assign them to reporting packages to meet the needs of a given audience.

Reporting Packages

LogRhythm administrators can easily create or modify reporting packages to provide needed content for auditors, executive management, or other audiences who require output for assessment. Within the CMMC module there are four (4) reporting package templates that you can modify to align with auditing and organizational requirements.

Report Package Name	Report Package Description	Report Package ID
CCF: Executive Reporting Package	This reporting package is a template to deliver pertinent content for executives on a monthly basis.	87
CCF: Weekly Audit Reporting Package	This Reporting Package is a template to deliver pertinent content for internal and/or external audit groups on a weekly basis.	88
CCF: Daily IT Operations Reporting Package	This Reporting Package is a template to deliver pertinent content for IT operations on a daily basis.	89
CCF: Daily IT Security Reporting Package	This Reporting Package is a template to deliver pertinent content for IT security on a daily basis.	90

To create a new Reporting Package to be used at your discretion:

1. On the main toolbar, click the **Report Center**.
2. Click the **Report Packages** tab.
3. Right-click the grid and click **New Report Package**.
4. Within the Select Reports window, select the CCF reports you want to include in this reporting package, and then click **Next**.
5. Click **Next** on the Override Log Source Criteria without making any changes.

> Do not override log source criteria.

6. Select the frequency for which the reporting package will be produced and the timeframe.
7. Configure additional settings for report delivery options, and then click **Next**.
8. Add the name and description of the new CMMC reporting package, and then click **OK**.

To create a cloned Reporting Package to apply the CCF Log Source List:

1. On the main toolbar, click the **Report Center**.
2. Click the **Report Packages** tab.
3. Right click on the reporting package you want, and then click **Clone**.
4. Ensure the correct reports are selected within the reporting package.
5. Click **Next** until you reach the Override Log Source Criteria.
6. Select **Selected Log Source List** and type **CCF** in the Name search field.
7. Select the **CCF: All Log Sources** check box.
8. Select **Next** until you reach Package Details, and then change the Package Name.
9. Set Report Package Permissions, and then click **OK** or **Apply** to save.

CMMC User Guide – LogRhythm GeoIP Functionality

LogRhythm Geolocation is a key function in enterprise log management and SIEM that equips the organization to establish global awareness. You can use network visualization and relationship mapping to establish customized geolocation settings. LogRhythm Professional Services can help you set up the GeoIP Resolution to the country level so you to achieve global event awareness without bogging down your SIEM. With the specific guidelines recommended in the CMMC publication, geolocation functionality can serve many purposes for an organization maturing its security posture.

For example, you can monitor inbound traffic from countries with strict data protection laws or with known high-risk for malicious activity to ensure you are adhering to CMMC regulations and following its policies. The CMMC module contains AIE rules and alarms designed to notify appropriate individuals if new data subjects enter personal data into your environment. This functionality empowers your organization to apply policies and ensure you are in compliance with the CMMC data protection requirements.

To use GeoIP functionality, a LogRhythm administrator must enable the feature in the Data Processor's advanced settings. When applying the GeoIP functionality to the deployment, choose a level of granularity that fits your resources and requirements. From least to most granular, the following settings can be established: Country, Region, and City. When you add this location context to pertinent log data, it can be a vital tool that can be used to meet various log monitoring objectives.

Refer to LogRhythm's Geolocation Feature Description: LogRhythm GeoLocation Visualization

AIE Rules	Notification Area	Corresponding Investigation
CCF: GeoIP Blacklisted Region Activity	Security : Suspicious	CCF: GeoIP Inv
CCF: GeoIP General Activity	Security : Suspicious	CCF: GeoIP Inv

> There are other enhanced LogRhythm capabilities that can be utilized as your organization's compliance and security programs mature. These are discussed in more detail within the CMMC Deployment Guide.

CMMC User Guide – Compliance Maturity Model: A Foundation and Road Map

The Labs Compliance Research team within LogRhythm realizes our customers transition through a maturing process as they implement controls, policies, personnel, and system solutions to achieve compliance within regulatory frameworks. As their compliance programs mature, organizations need a SIEM solution that adapts to the changes they have implemented. A compliance offering through a SIEM that cannot be readily modified detracts value from a customer's experience. While working to build their compliance programs, organizations need the ability to integrate their improvements into the SIEM to a robust cybersecurity infrastructure.

Audits and ongoing compliance programs might be viewed as compulsory, but organizations can actually leverage regulatory frameworks to create competitive advantages. As an organization progresses across the compliance maturity model (below), a security foundation emerges around policies, controls, systems, personnel, and understanding. The organization begins by developing key resources such as system and account classifications, risk assessments, scope definition, process and data flows, and audit results year-over-year. All these factors are ingredients to constructing a solid yet resilient compliance foundation that enables an organization to transition into a more mature security posture. This transition occurs as the organization builds its security program on a holistic and transparent understanding of its environment and risk profile.

LogRhythm aims to provide a road map through which SIEM empowers an organization to grow into a security program. Our approach allows organizations to start basic and transition into more enhanced facets of LogRhythm SIEM and other solutions where data protection not only achieves regulatory compliance but it also becomes a competitive advantage.

Key Resources

As your organization works to achieve compliance with the CMMC, begin by developing the following key resources that you can leverage within the deployment of this compliance automation suite and LogRhythm SIEM as a whole.

- Data Inventory & Privacy Classification
- Asset Inventory & System Classification
- Definition of Key Management Responsibilities

- Security Policies & Procedures
- Information Security & Business Continuity Plans

Key Audiences

Examples of key audiences involved in the CMMC life cycle are listed below. You can use reporting packages, reports, and Case Management to deliver critical information to your key audiences. You can also modify these reporting tools to accommodate specific requests.

- Executive Management
- System Owners
- Control Owners
- Information Security
- IT Operations