OMB Event Logging Requirements

Devo's Log Management Platform Capabilities

PUBLIC SECTOR

INTRODUCTION

The Office of Management and Budget (OMB) released memorandum M-21-31 on August 27, 2021, with the subject of "Improving the Federal Government's Investigation and Remediation Capabilities Related to Cybersecurity Incidents." This memorandum defined certain Event Logging (EL) Tiers and laid out the requirement for the applicable federal departments and agencies to determine their current EL Tier, and then to bring their organizations up to the standards for Event Logging Tier 3 by August 17, 2023.

HOW OMB LAID OUT THE REQUIREMENTS

As written, the memorandum distributes implementation, operational and technical requirements throughout the document. Appendices A and C are the primary sources of requirements that a federal organization would use in the selection and implementation of an event logging capability and are the focus of this document. Appendix A is the Implementation and Centralized Access Requirements and references Appendix C, the Logging Requirements – Technical Details. Section II of the memorandum focuses on the implementation requirements, which Devo does not address in this document.

Devo has grouped the requirements from Appendices A and C into the requirements associated with Event Logging Tiers 1 through 3. This enables the reader to understand all of the requirements needed to go from one tier to another tier.

DEVO LOG MANAGEMENT PLATFORM CAPABILITIES

Devo is a cloud-native logging and data analytics platform provided as a software-as-a-service (SaaS) solution to customers. Devo is agnostic about what logging information customers forward to it and can ingest any type of text-based logging information. Devo stores all log information in its raw format and has hundreds of existing parsers. Customers also can create their own parsers if required.

For simplification, the following tables include only the requirement Log Category, and the Required Data header, and do not include all of the technical details associated with all requirements. The reader is encouraged to read the entire memo from OMB to gain a fuller understanding of the requirements and the context in which OMB presented them.

DEVO CAPABILITIES

The table contains a column labeled "Devo Capabilities." It contains the following statements:

- **Not Applicable** – This requirement is out of scope for Devo, which implies this may be a planning requirement or related to how a federal organization would operate a Devo deployment.
- **Meets** – Devo meets this requirement.
- **Supports** – Devo supports this requirement. The requirement is written such that fully meeting its requirement requires both Devo and one or more additional capabilities.

This analysis assumes the federal organization can generate and forward the required log data to Devo.

Requirements	Tier 1	Tier 1	Tier 3	Devo Capabilities
Implementation and Centralized Access Requirements (Appendix A)				
Minimum Logging Data	x	x	x	**Meets**
Time Standard	x	x	x	**Meets**
Event Forwarding	x	x	x	**Meets**
Protecting and Validating Log Information	x	x	x	**Meets**

Minimum Logging Data	x	x	x	**Meets**
Time Standard	x	x	x	**Meets**
Event Forwarding	x	x	x	**Meets**
Protecting and Validating Log Information	x	x	x	**Meets**
Passive DNS	x	x	x	**Supports[2]**
CISA and FBI Access Requirements	x	x	x	**Meets**
Logging Orchestration, Automation and Response – Planning	x	x		**Supports**
User Behavior Monitoring – Planning	x	x		**Supports**
Basic Centralized Access	x	x	x	**Meets**
Publication of Standardized Log Structure		x	x	**Not Applicable**
Inspection of Encrypted Data		x	x	**Not Applicable**
Intermediate Centralized Access		x	x	**Meets**
Logging Orchestration, Automation and Response – Finalized Implementation			x	**Supports**
User Behavior Monitoring – Finalizing Implementations			x	**Supports**
Application Container Security, Operations and Management			x	**Meets**
Advanced Centralized Access			x	**Meets**

Logging Requirements – Technical Details (Appendix C)

Identity & Credential Management	x	x	x	**Meets**
Privileged Identity & Credential Management	x	x	x	**Meets**
Network Device Infrastructure				
• All Devices	x	x	x	**Supports[2]**
• DNS	x	x	x	**Meets**
• Passive DNS Log	x	x	x	**Supports[2]**
• DNS, DHCP, and Wi-Fi	x	x	x	**Supports[2]**
• General Logging	x	x	x	**Supports[2]**
• Routers and Switches	x	x	x	**Supports[2]**
• Load Balancer / Reverse Proxy	x	x	x	**Meets**
• Proxies and Web Content Filters	x	x	x	**Meets**

• General Information	x	x	x	**Supports[2]**
• Operating System (OS) Events	x	x	x	**Supports[2]**
• OS Audit Records	x	x	x	**Meets**
• Application Account Information	x	x	x	**Meets**
• Application Operations	x	x	x	**Meets**
Operating Systems – Windows Infrastructure and Operating Systems				
• User and Administrator Access to OS Components and Applications	x	x	x	**Meets**
• System Performance and Operational Characteristics	x	x	x	**Meets**
• System Configuration	x	x	x	**Meets**
• File Access	x	x	x	**Meets**
• Host Network Communication	x	x	x	**Meets**
• PowerShell Execution Commands	x	x	x	**Meets**
• WMI Events	x	x	x	**Meets**
• Registry Access	x	x	x	**Meets**
• Command-Line Interface (CLI)	x	x	x	**Meets**
• Basic Input Output System (BIOS), Unified Extensible Firmware Interface (UEFI), and Other Firmware	x	x	x	**Meets**
Operating Systems – MacOS (or Other Apple Desktop and Server Operating Systems)				
• User and Administrator Access to OS Components and Applications	x	x	x	**Meets**
• System Performance and Operational Characteristics	x	x	x	**Meets**
• System Configuration	x	x	x	**Meets**
• File Access	x	x	x	**Meets**
• Host Network Communication	x	x	x	**Meets**
• Command-Line Interface (CLI)	x	x	x	**Meets**
• Basic Input Output System (BIOS), Unified Extensble Firmware Interface (UEFI), and Other Firmware	x	x	x	**Meets**
Operating System – BSD (Linux)				
• User and Administrator Access to OS Components and Applications	x	x	x	**Meets**
• System Performance and Operational Characteristics	x	x	x	**Meets**
• System Configuration	x	x	x	**Meets**

• File Access	x	x	x	**Meets**
• Host Network Communication	x	x	x	**Meets**
• Command-Line Interface (CLI)	x	x	x	**Meets**
• Security Enhanced Linux (SELinux) AppArmor or Equivalent	x	x	x	**Meets**
• System	x	x	x	**Meets**
• Access and Authentication	x	x	x	**Meets**
• Applications	x	x	x	**Meets**
• Package Install/Uninstall	x	x	x	**Meets**
• Basic Input Output System (BIOS), Unified Extensible Firmware Interface (UEFI), and Other Firmware	x	x	x	**Meets**
Cloud Environments				
• General Events	x	x	x	**Meets**
• General Logging	x	x	x	**Meets**
Cloud AWS	x	x	x	**Meets**
Cloud Azure	x	x	x	**Meets**
Cloud GCP	x	x	x	**Meets**
System Configuration and Performance				
• Configuration		x	x	**Supports**[2]
• Endpoint Detection & Response		x	x	**Meets**
• Configuration Changes		x	x	**Meets**
• System Status		x	x	**Supports**[2]
• Software Updates			x	**Meets**
Authentication and Authorization				
• Administrative		x	x	**Meets**
• Authorization		x	x	**Meets**
Email Filtering, Spam and Phishing				
• Content Filtering Policy Updates		x	x	**Meets**
• Raw and Metadata – Filtering Events		x	x	**Meets**
• Spam Dictionary Modifications			x	**Meets**

Antivirus and Behavior-Based Malware Protection				
• General		x	x	**Meets**[1]
• Indication of the Host that Connected to a Specific URL		x	x	**Meets**
Network Device Infrastructure				
• Firewalls		x	x	**Meets**
• All Devices: IDs/IPs Alerts and Events		x	x	**Meets**
• VPN Gateway – All Events		x	x	**Meets**
PKI Infrastructure		x	x	**Meets**
Vulnerability Assessments		x	x	**Meets**
Database Level		x	x	**Meets**[2]
Application Level				
• Web Applications		x	x	**Meets**
• Web Application Crashes		x	x	**Meets**
• Web Applications & Middleware		x	x	**Meets**
• Commercial Off-the-Shelf (COTS) and Custom Applications		x	x	**Meets**
• General – Non-COTS		x	x	**Meets**
Virtualization System		x	x	**Meets**
Mobile				
• EMM (UEM)/MTD Alerts		x	x	**Meets**
• General		x	x	**Meets**
• Device Data		x	x	**Meets**
• Application Data		x	x	**Meets**
• Device Policy Settings		x	x	**Meets**
• Device Configuration		x	x	**Meets**
• Network Configuration		x	x	**Meets**
• Event / Audit / Crash Logs		x	x	**Meets**
• MTD Agent Info		x	x	**Meets**

Container				
• Supply Chain		x	x	**Supports**[2]
• Image		x	x	**Meets**
• Engine		x	x	**Supports**[2]
• OS		x	x	**Meets**
• Cluster/Pod Events			x	**Meets**
Data Loss Prevention		x	x	**Meets**[1]
Network Traffic: Full Packet Capture Data		x	x	**Meets**
Mainframes			x	**Meets**

[1] Devo is unable to store email attachments. It is unclear from the requirement if storing attachments in the logging platform is an actual requirement.

[2] Devo may require a third-party solution to collect the data and send it to Devo.

SUMMARY

The Devo Platform meets all of the OMB requirements that apply to the event logging platform. Beyond log management, the Devo Security Operations and Service Operations applications provide federal organizations with capabilities that are critical to federal security operations centers (SOC) and IT operations, without additional effort.

The Devo Security Operations and Service Operations applications are included in the standard Devo Platform license at no additional cost. Reach out to your Devo representative today to learn more.

Devo
255 Main Street
Suite 702
Cambridge, MA 02142

Devo is the only cloud-native logging and security analytics platform that releases the full potential of your data to empower bold, confident action. With unrivaled scale to collect all of your data without compromise, speed to give you immediate access and answers, and clarity to focus on the signals that matter most, Devo is your ally in protecting your organization today and tomorrow. Devo is headquartered in Cambridge, Mass. Learn more at **www.devo.com**.