tripwire

WHITE PAPER

Five Critical Steps of a Complete Security Risk & Compliance Lifecycle

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

The Security and Compliance Lifecycle

Security and compliance remain at the forefront of concerns facing security leaders today. Tackling the challenge of finding and addressing risks in the enterprise while demonstrating compliance with increasingly demanding regulations requires the maturity and discipline to adopt and follow a complete security risk and compliance lifecycle.

Tripwire worked with clients to capture and distill the five critical steps that successful organizations take to reduce risk, demonstrate compliance and answer the most important questions in today's compliance-driven enterprise:

» How secure and compliant is our network?

» Which top issues must we address today to improve security and achieve compliance?

» Who is accountable and how are they doing?

The five critical steps of a complete security risk and compliance lifecycle include:

1. Inventory Assets to get a complete picture of all assets—known and unknown—and their key characteristics
2. Triage and assess alerts and reports to determine issues and appropriate remediation steps
3. Prioritize and assign actions required to reduce risk by ensuring the right people have accurate information about affected systems, remediation steps and deadlines
4. Remediate the risk or create exceptions with proper testing, tracking and verification
5. Audit and Report on the success of the remediation by presenting the right information to the right teams in the time and manner they need leading to the ability to shift the culture and continually improve security and compliance

Adopting these steps as a lifecycle process improves security and compliance while saving costs and using resources more efficiently. Over time, this leads to process maturity and the opportunity to shape the culture through the use of empirical data from each step of the lifecycle.

Step 1: Inventory Assets

Security and compliance remain at the forefront of concerns facing security leaders today. Tackling the challenge of finding and addressing risks in the enterprise while demonstrating compliance with increasingly demanding regulations requires the maturity and discipline to adopt and follow a complete security risk and compliance lifecycle.

Surprisingly, many organizations don't have an accurate asset inventory due to the constantly changing network and lack of proper inventory tools. Mature organizations maintain comprehensive, accurate inventories that are created through the use of an automated, lightweight discovery process. Frequent or continuous monitoring is made possible by lightweight background scans that adapts to specific bandwidth and resource constraints, ensuring actionable insights are gained without straining resources essential for operations. When selecting a discovery process to build a complete inventory, consider:

» **Thorough discovery scans:** The discovery solution must be able to find, assess and report on a wide variety of systems—actively and passively, known and unknown. Key elements include the ability to identify: assets (approved and unapproved), open ports, services, applications (approved and unapproved), vulnerabilities, system and application configuration.

1. **Tracking assets within the changing network:** Enterprise networks change constantly as systems come on and off the network. Traditionally, keeping track of a particular host is a difficult task in these dynamic environments. Often overlooked, it's important to know if the systems being scanned in the discovery process are the same systems in the inventory to reliably identify, track, and audit hosts.

» **Complete discovery:** The discovery process must be nimble and adaptable to provide timely insights as the network landscape changes and new devices are introduced. An approach that includes the ability to scan, identify and present information on non-standard systems or systems of all kinds—servers, desktops, network devices, etc.

This step results in a complete asset inventory that includes and presents information about new hosts, vulnerabilities and configuration changes. It also incorporates information about "rogue" assets and applications—devices and programs not approved for the network—as well as changes from the established baselines. As the first step in the security risk and compliance lifecycle, getting this right with accurate and complete information ensures continued efficiency and demonstrable success.

The Tripwire Advantage

» Comprehensive, automated asset scanning to develop a complete picture of what's actually on the network

» Designed for lightweight background discovery with Dynamic Host Tracking to identify systems as they leave and rejoin the network

» Complete agent and agentless design enables discovery and identification of the entire network

Step 2: Triage and Assess

After completing the asset inventory, the focus moves to identifying and understanding the top areas to focus on that improve security while achieving compliance. Mature programs successfully address this challenge by incorporating triage and assessment into their normal processes. More than a concept for emergencies, successful organizations start by developing a comprehensive baseline and then apply a routine discipline of triage and assessment against the ongoing findings to drive appropriate action.

Formed through an automated discovery process, the baseline includes information about what is on the network (devices and applications). For triage and assessment to be effective, the baseline must also incorporate relevant policies, regulations and industry-standard guidance for hardening and configuring applications and operating systems. The result is a clear definition of what is "normal" and expected on the network.

Having a baseline provides an additional benefit: something to compare against objectively. By incorporating objective results and measuring against a common baseline, it provides the evidence necessary to explain required actions to improve security and achieve compliance in a way that eases the process of gaining executive support.

Once the baseline is established, a regular, automated scanning process assesses the environment for changes and risks to the environment. It is important to use both vulnerability and configuration assessment to ensure a complete picture of the environment. Regular configuration auditing based on policies can highlight misconfigurations proactively and help prevent breaches.

Once alerted to changes, the triage process is a quick, lightweight review that leads to an initial priority to determine who, when and how to assess further. Assessment delves into the details enough to assign potential fixes, including what is wrong, what needs to be done and potential prioritization based on risk or compliance needs (though this is generally handled in the next step).

The result of this step includes three key elements:

» Baseline of normal and expected operations on the network including guidance on applications and configurations to compare against policy, regulations and industry practices;

» Triage/incident report that provides an initial priority and insight into who, when and how to assess deviations from the baseline, detected during routine vulnerability and configuration assessment;

» Incident assessment that details the problem, what needs to be done and suggests a potential priority to help guide the next step (prioritize and assign).

The Tripwire Advantage

» Comprehensive view of the security and compliance posture of the network

» Detailed reports highlighting vulnerabilities and network changes

» Ability to set a baseline on a host by host and network basis

Step 3: Prioritize and Assign

Once triage and assessment provide information about changes that introduce risk, corrective action needs to be taken. However, since it is not possible to fix everything immediately, each action must be prioritized properly to ensure the bigger risks to security and compliance are dealt with efficiently. Once the right priority is established, the remediation needs to be assigned to the right person, along with guidance on the potential fix and a timeline for action.

The first step in setting the right priority is determining asset value—with a higher emphasis on protecting more valuable targets based on the risk to the business. Once asset value is set, the approach to scoring combines a variety of factors to develop a risk score. Advanced systems also incorporate a robust methodology that incorporates detailed information about the attack, including complexity, age and potential for damage. This results in a more granular score and a more accurate measure of priority.

The final result needs to be easy to understand and take action on. Ideally, this means control over how priority is presented—with different ways to meet different needs—ranging from an extremely granular five-digit score to rankings based on high/medium/low, the numbers 1–5 or the letters A–F.

The result of prioritization is a list what needs to be done, in order, with the appropriate urgency. The key to efficiency is ensuring these actions are assigned to the right people with the appropriate deadline. Often overlooked, the deadline is a critical component of the prioritization that sets the stage to incorporate accountability into the process. Assignment should include sufficient detail about how to remediate or mitigate the risk to an acceptable level.

An automated solution eases the task of prioritization and assignment with the capability to automatically generate support tickets by connecting systems and networks to people, based on custodianship. Automation ensures speed and accuracy while incorporating relevant information into the assignment, easing the process of measuring response, including the ability to meet the deadline.

The outcome of step three includes:

» Prioritization based on empirical and objective evidence, matched to the needs and unique elements of the organization;

» Assignment to the right person with the appropriate details to fix the problem and a clear deadline used to measure performance and accountability.

The Tripwire Advantage

» Tripwire Risk Score—a unique, flexible and objective risk metric that enables organizations to prioritize vulnerabilities and changes, even in the largest networks

» Support for complete workflow with a built-in ticketing system and a ticketing API to connect to an organization's existing ticketing system

» Enterprise-class role-based access controls enable security and IT operations to administer their—and only their—networks

Step 4: Remediate and Verify

Once steps to improve security and achieve compliance have been identified, prioritized and assigned, the risk needs to be remediated. Remediation is more than a step, it's a process that includes multiple sub-steps, including assessment/pre-testing, fixing (or excepting), post-testing, verifying and reporting the results.

This is where the efforts of multiple teams, notably security and operations, intersect. Automating as much of the process as possible helps to smooth the hand-off between groups while improving overall results. The common challenge of remediation is the realization that not everything can be fixed. When the determination is made that the assigned remediation will not work, an exception needs to be requested and processed.

Identifying exceptions creates unique challenges and tends to increase friction between groups. Proper handling of the exception process requires an evaluation, decision and possibly some additional actions to mitigate potential risk. Effective resolution requires objective information and constructive conversation between IT security, operations and business stakeholders. This is why an automated system that provides objective evidence in a variety of formats—what each team needs presented in the way that makes sense to them—is essential.

The entire process needs to be tracked in a way that can be audited (for compliance) until the risk can be permanently addressed. This means the system must provide useful and accurate findings while recording key decisions that can be shared with multiple teams and maintained as part of the lifecycle to demonstrate compliance.

For successful remediation actions, verifying the effort was successful, lasting and did not cause new and additional risks should be automatic. This verification often takes the form of a scan to validate the fix and record the results, along with when the fix was completed. This helps ensure the risk was remediated by the deadline set when assigned.

At the completion of this step, there are three deliverables:

» Systems remediated (or excepted) based on priority and in a way that is verifiable without introducing new risk; in the event of exceptions, the entire process must be recorded in a way that is justified;

» Verification scan completed to ensure the fix was successful, no new risks were introduced as a result of the fix and a log of the effort including time to completion is recorded.

Remediation status report detailing the steps, decisions and timelines useful for process improvement, audit and accountability

The Tripwire Advantage

» Complete remediation instructions for each issue and mitigation alternatives if remediation is not possible

» Automated verification scans can be triggered programmatically when tickets are closed

» Complete remediation report for improved accountability

Step 5: Audit and Report

While taking the steps to remediate risks is necessary to improve security, the final step of the life cycle is to ensure reporting that improves audit readiness, demonstrates compliance and supports continued improvement. Successful organizations use this step to develop specialized reporting designed for several audiences to improve operational efficiency, show progress over time and promote accountability.

When developing comprehensive reporting, mature organizations collect information across all five steps of this lifecycle; this allows the right level of information to be presented at the right time, in the right way. Building reports based on empirical evidence with the appropriate mix of context, actions, consequences and objectivity enables all areas of the organization to be more effective:

- **Executives** need trends to increase visibility and insight into areas to ensure resource investments are allocated appropriately;
- **Audit and compliance teams** are provided with audit results and guidance to proactively achieve continuous compliance with all applicable regulations;
- **Security analysts** are provided with instant visibility into new and existing security risks across the enterprise.

Using an automated solution throughout the lifecycle enhances reporting by making sure all relevant information, notes and actions are recorded and presented in audience-specific reports. By presenting reports on teams, lines of business and even the full enterprise, it is possible to measure and assess accountability. This enables the insight—and suggested actions—to ensure operational effectiveness is maximized.

A robust reporting engine provides objective measurement with the ability to trend over time. This is the difference between a report that is simply a snapshot in time and one that is more like a movie with the powerful insights of understanding how the organization is changing—and whether the change is reducing or increasing risk.

Deliverables for this final step include:

- Reporting based on expected actions, accountability and outcomes, presented in a variety of ways to ensure operational efficiency (or highlight opportunities for improvement);
- Historical trend analysis to show how the organization is handling the challenge of security and compliance over time;
- Information and insights to successfully address the current state of security and compliance, remaining actions to be taken and overall accountability.

Remediation status report detailing the steps, decisions and timelines useful for process improvement, audit and accountability

The Tripwire Advantage

- Trend reporting to track security and compliance status over time
- Compliance reports for PCI, NERC, HIPAA, SOX, UCGSB and more
- Reports designed for specific audiences—executives, audit team, security team and IT operations

Summary

While the challenges of security and compliance continue to drive the needs of organizations, the adoption of the five-step lifecycle enables organizations to develop the maturity and insight necessary to cultivate accountability, streamline operations and improve efficiency. As companies consider and improve on the ability to execute each of these steps, they are often able to do more with less.

A critical factor in adopting this lifecycle is the ability to select and choose a partner with solutions designed to automate each of these steps with an understanding of the entire lifecycle. Successful implementations take into account the unique aspects of the environment, including the role people and politics play on the implementation and operation of these steps.

The combination of the right solutions and the adoption of this life cycle drives risk reduction and automates compliance by:

» Promoting accountability with objective, consistent data that aggregates asset, security, and policy data across the enterprise through executive dashboards that include baseline and trend analysis;

» Integrating security and configuration audit data into security portals, applications, and business processes to support remediation and improve security operations;

» Storing data for extended periods of time to perform long-term trending of hosts, applications, and vulnerabilities, as well as to meet regulatory requirements.

Tripwire's solutions enhance each step of this lifecycle with actionable information, presented to all teams in the way that best supports their needs. This helps to reduce friction and while improving results across the entire sequence. With over 9,000 customers around the world, Tripwire has delivered proven solutions that answer the most important questions in today's compliance-driven enterprise:

» How secure and compliant is our network?

» Which top issues must we address today to improve security and achieve compliance?

» Who is accountable and how are they doing?

By distilling the essence of success into this lifecycle, Tripwire strives to improve the operations of all organizations. Supporting this approach with innovative solutions ensures consolidated, actionable, risk-based reporting for all enterprise audiences—from technical users to the board of directors.

Tripwire is a leading provider of security, compliance and IT operations solutions for enterprises, industrial organizations, service providers and government agencies. Tripwire solutions are based on high-fidelity asset visibility and deep endpoint intelligence combined with business context; together these solutions integrate and automate security and IT operations. Tripwire's portfolio of enterprise-class solutions includes configuration and policy management, file integrity monitoring, vulnerability management, log management, and reporting and analytics. **Learn more at tripwire.com**

***The State of Security*: Security News, Trends and Insights at tripwire.com/blog**
Follow us on Twitter @TripwireInc » Watch us at youtube.com/TripwireInc

WPFCSSL2j 1712