PRESCRIPTIVE GUIDE SERIES

Security Reference Architecture:

A Practical Guide to Implementing Foundational Controls

By Dave Meltzer
CTO, Tripwire, Inc.

tripwire®

TABLE OF CONTENTS

PART ONE: INTRODUCTION

For today's chief information security officer (CISO), securing the organization has never been more challenging. Unfortunately, the CISO's job is unlikely to get easier in our lifetime for a dizzying number of reasons. Among these reasons, the rapidly expanding set of devices to protect, driven by growth in virtualization, the cloud, bring your own device (BYOD), and the Internet of Things (IoT). Add to that a continued shortage of qualified and skilled people to tackle the work, an ever-increasing sophistication of threat actors, and stringent industry regulations and compliance demands. Then top it off with a jumble of security solutions meant to address these issues that the CISO and security team must evaluate against security and compliance requirements and operational demands.

Today's organization needs to build a resilient architecture—a dynamic system that can provide effective security today, but that's flexible enough to protect against the unknown threats and new technology of tomorrow. While the dream of the silver bullet solution with the power to stop all attacks on all systems is just that—a dream—you can establish and follow a sensible path forward to arrive at that system. Like any complex project, you can transform the overwhelming into something manageable by stepping back, taking a deep breath, and breaking down the larger project into smaller, doable pieces. That's the intent of this Prescriptive Guide.

WHAT YOU'LL LEARN

This guide describes an overall, holistic strategy and approach to developing a system that protects against today's threats in today's technology environment.

It explains how to develop an overall strategy for security and compliance, including selecting the security framework that will guide you in building your system, and the maturity model that will help you advance your security program. It also discusses the need to adopt or develop a reference architecture at the higher security system level. It then introduces a reference architecture built on the various foundational controls available through Tripwire's solutions. Finally, it discusses how to select the security solution vendors, and prioritize investments for the best results.

The subsequent chapters in this Prescriptive Guide discuss in much greater depth the three foundational controls of the reference architecture offered by Tripwire solutions—file integrity monitoring, security configuration management and vulnerability management. They describe each control, explain where each fits in common security frameworks, how it gets used, key integration points with other controls and business systems, deployment architecture diagrams, and many other important details and considerations related to the control.

Although the reference architecture at the security control level is based on Tripwire solutions, your overall strategy must address the other controls outlined by your security framework. As a result, a complete IT security system will encompass a broader set of solutions from multiple vendors. Ideally, these vendors and their solutions will work together to help your organization build a cohesive, inter-connected system.

SELECTING A FRAMEWORK

Your first step in developing an architecture involves selecting a security framework. The security framework formally describes the many processes, procedures and associated security controls that you can use to reduce risk across your organization and out to its many and diverse endpoints. Security frameworks vary in their level of specificity. Some frameworks have very specific prescriptive guidance on what should be done and the relative priority of each action, while others just paint a broad picture of everything that *could* be done.

COMMON SECURITY FRAMEWORKS

Commonly used security frameworks include the NIST Cybersecurity Framework, CIS Critical Security Controls, ISO 27000-series, ISA 99/IEC 62443, FFIEC Information Security, COBIT, COSO, and HITRUST CSF. The PCI DSS, though mostly perceived as a compliance mandate, provides highly prescriptive security guidance that smaller and mid-size organizations in particular can leverage as a framework.

Each framework consists of high-level functions and detailed guidance on security controls. For example, the NIST Cybersecurity Framework, first published in 2014

and widely adopted in the US, defines five high-level functions of security: identify, protect, detect, respond and recover. It further defines 22 categories and 98 subcategories within those functions. Similarly, the Center for Internet Security Critical Security Controls for Effective Cyber Defense (formerly known as the SANS Top 20 and the 20 Critical Security Controls), identifies 20 high-level critical security controls. Those 20 critical controls are categorized into families of ten System, four Network, and six Application controls, which are then further segmented into 149 total controls.

CONSIDERATIONS FOR SECURITY FRAMEWORK SELECTION

Selecting a primary security framework can help your organization align with a cohesive strategy, but how do you go about choosing one? Making a choice may appear particularly perplexing given that most frameworks actually have more commonalities than differences, especially when it comes to their technical aspects. While no single framework can be definitively called the best, a few considerations will likely lead you to choose one over the other.

Some frameworks have been developed with certain vertical industries in mind—for example, IEC 62443 specifically provides guidance for organizations in industrial markets. Other frameworks are more widely adopted within geographies based on history and evolution. For example, although they are not specific to these areas, the NIST Cybersecurity framework has more adoption in North America, while the ISO 27000-series has more European adoption. Although this should not be a single disqualifying factor, it is worth considering.

Generally, leveraging the same security framework as your industry or regional peers provides significant advantages, including more available expertise to implement it, easier benchmarking of program's maturity against it, and a greater familiarity with it by auditors that leads to easier acceptance and approval of its approaches to security.

USING A FRAMEWORK WITH A SECURITY REFERENCE ARCHITECTURE

This security reference architecture doesn't dictate which security framework you must use. Instead, it simply provides best practices for using the individual security controls of an existing framework, explains how these controls can interoperate most effectively, and outlines how they can do so in the context of Tripwire's solutions and products.

Although the reference architecture can be used with no overall security framework in place, selecting an appropriate security framework is recommended as a foundation for building and evolving your security program. If you've already selected and implemented a framework, this reference architecture speaks to how these controls fit in the frameworks most used by our customers. As a result, you should be able to fairly easily understand how it fits within your choice.

CHOOSING A MATURITY MODEL

The second step involves choosing a maturity model, a valuable companion to your chosen security framework that focuses on your security program's implementation and management of security. A maturity model specifies the types of processes and controls that should be in place as your security program advances through each stage of the model. You'll use your chosen model to assess and establish a baseline of the current state of your security program, and guide it toward achieving higher levels of security based on your chosen framework. You can also use it to evaluate the effectiveness of your program and prioritize new investments.

COMMONLY USED MATURITY MODELS

Just as with security frameworks, you can select from a large number of maturity models. Your choice may be somewhat obvious depending on your selected framework, as many maturity models go hand-in-hand with a given framework. For example, the Cybersecurity Capability Maturity Model (C2M2), produced by the US Department of Homeland Security in conjunction with the Department of Energy, complements the NIST Cybersecurity Framework. The C2M2 model defines four levels of maturity with its maturity indicator levels, which range from 0–3 for each of the security domains covered by the NIST Cybersecurity Framework.

If you are a customer of Gartner, their ITScore for Information Security (www.gartner.com/doc/2507916/itscore-information-security) is another option. This defines five maturity levels that range from **Level 1: Initial** to **Level 5: Optimizing**, along 10 measured dimensions. Forrester also offers its Information Security Maturity Model, with maturity levels that range from **0 – Non-existent** to **5 – Optimized**.

A MATURITY MODEL FOR CRITICAL SYSTEMS AND ENDPOINT SECURITY

Many security programs now recognize the importance of using a maturity model specific to particular areas of security. Systems that are most important to the organization need to receive a heightened level of attention compared to a common end-user laptop. Critical systems are a smaller but more highly sensitive set of systems compared to the broader set of devices—endpoints—which can be broadly defined as every device or system that connects to the organization's technology infrastructure.

Security models for critical systems and endpoints models have been developed and are seeing greater use because many organizations perceive the guidance from traditional security maturity models to be too broad or generic to adequately address endpoint security. Tripwire and SANS recently collaborated to develop the SANS Endpoint Security Maturity Model to help organization's gauge the effectiveness of their security program with endpoint security. The model defines five levels of maturity based on measurements of six different dimensions, called elements.

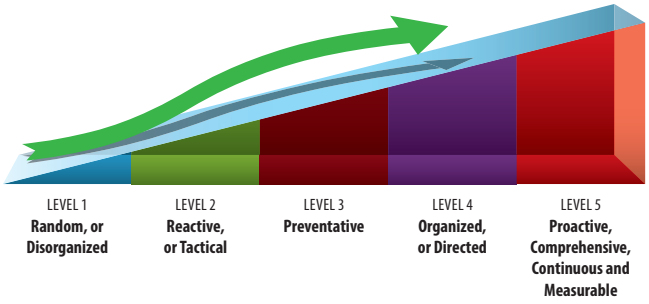

Fig. 1: The SANS Endpoint Security Maturity Model Curve

When selecting a security maturity model, you may need to include a separate model to help you gauge and improve the effectiveness of your security program in securing the organization's endpoints.

TRIPWIRE'S REFERENCE ARCHITECTURE AND THE C2M2 MATURITY MODEL

This reference architecture sets relate back to maturity levels defined in C2M2. The architecture helps place each security control into its appropriate C2M2 domain, defining what levels of maturity you can expect by implementing the reference architecture for a given control, and differentiating between the various levels by what technologies, processes or people are in place. The reference architecture further defines appropriate MILs for the controls provided by Tripwire products, augmenting the general definitions of the MILs with more specific guidance.

DEVELOPING A SECURITY ARCHITECTURE

While a security framework provides a broad view of the many different security controls an organization may need to deploy and manage; you shouldn't view it as a checklist of 149 controls that you can implement one by one until you are finished and secure. In the past, a checklist approach may have been more appropriate, but security has evolved. Organizations used to have a "defense in depth strategy," with numerous independently deployed security controls that provided layers of protection. Today, security is more of an interconnected web of controls that communicate with each other and adapt dynamically based on changing intelligence and needs.

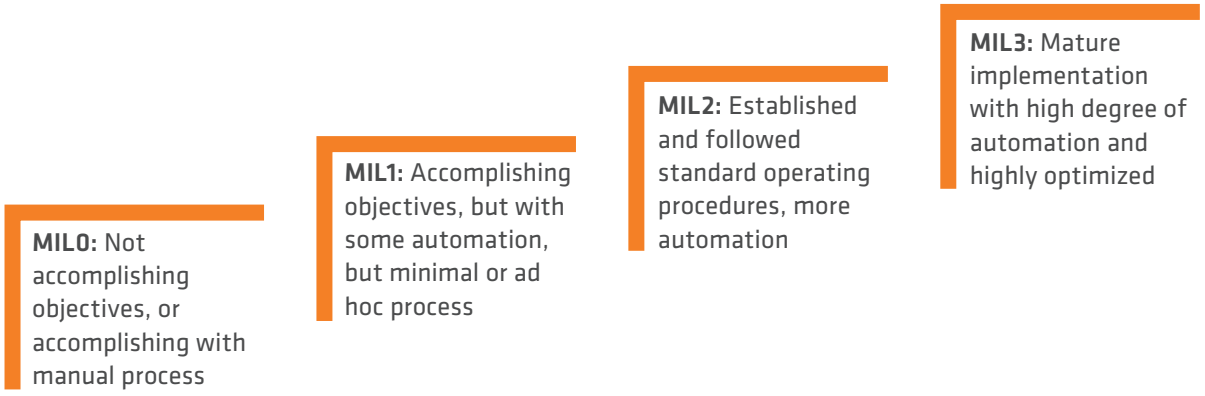

Fig. 2: The Cybersecurity Capability Maturity Model (C2M2) maturity indicator levels (MILs)

Level	Characteristics
MIL0	• Practices are not performed
MIL1	• Initial practices are performed but may be ad hoc
MIL2	*Institutionalization characteristics:* • Practices are documented • Stakeholders are identified and involved • Adequate resources are provided to support the process • Standards or guidelines are used to guide practice implementation *Approach characteristic:* • Practices are more complete or advanced than at MIL1
MIL3	*Institutionalization characteristics:* • Activities are guided by policy (or other directives) and governance • Policies include compliance requirements for specified standards or guidelines • Activities are periodically reviewed for conformance to policy • Responsibility and authority for practices are assigned to personnel • Personnel performing the practice have adequate skills and knowledge *Approach characteristic:* • Practices are more complete or advanced than at MIL2

Fig. 3: Generic characteristics of each Maturity Indicator Level defined in C2M2

To better understand this evolution, consider this example: In the past, a network firewall and a file integrity monitoring system on a server had nothing in common other than they were both providing security to an organization. Network and system security were considered very different practices, and although both were important, they barely overlapped. Because they were so different, building a deployment architecture for a firewall was unlikely to even consider what security controls were in place on servers, other than perhaps what ports and protocols they would need to communicate over for management purposes.

Contrast that to the way these controls are being deployed today. Next-generation firewalls now connect to threat intelligence services that provide updated rules designed to block the command and control of infected endpoint systems. These rules are developed based on dynamic analysis of malicious code that's been delivered to sandbox analysis systems.

With the example above, a security reference architecture can help you coordinate the detection and real-time delivery of a potentially malicious executable for analysis from a critical server to a malware analytics service. That service can then create blocking rules on an organization's external firewall, which may block a successful malicious code insertion from being used to pivot to additional systems or exfiltrate data. That's the connection and coordination of three separate security controls—a network firewall, a malware sandbox analysis service, and an endpoint detection and response system.

The now interconnected nature of security controls requires you to architect security solutions together. A security reference architecture can help you define how to implement your controls so that they form this interconnected and coordinated web of controls.

CONSIDERATIONS WHEN SELECTING SECURITY CONTROL SOLUTIONS

While it would be wonderful if you could simply buy all 149 security controls from a single vendor and have them all work together, that's just not reality. Ironically, the vendors that have accumulated the largest number of controls tend to do the worst job of actually integrating them. In addition, some of the largest security vendors in times past have recently been the most active in end of life-ing and divesting products. That said, you probably don't want to buy your 149 controls from 149 different security vendors, either.

Selecting the right vendors is important in developing a successful architecture. Maintaining a core set of trusted strategic vendors that have articulated a well-defined framework, and demonstrated both commitment and execution on integration and interoperability with other security control vendors is the best approach here.

The ideal architecture for a security control is a complete, well-documented, and open API, with pre-built integrations with many partners. This allows for the connectivity between security controls required by today's approach to security. Unfortunately, these characteristics tend to be present only in controls built on aggregating data from other systems. When choosing a solution for a security control, identify the most important integration points in the architecture for that control and determine if the solution has the capability for those specific integrations.

THE TRIPWIRE REFERENCE ARCHITECTURE SET

You can apply a model for security architecture to multiple layers of security and at different levels of abstraction. Tripwire's reference architecture provides details at two levels:

» **Level 1**: Systems security reference architecture, which describes the inter-related controls of an entire framework as it relates to systems security. This is complementary to other architectures that focus on network security.

» **Level 2**: Specific security controls reference architecture, which describes the architecture for the individual controls offered by Tripwire.

» Our reference architecture set excludes other areas where reference architectures are also important. For example, the set excludes the areas of network and application security and the myriad security controls outside of the scope of Tripwire's offerings.

Note that systems security is a broad area that covers multiple security controls. It includes controls offered by Tripwire, such as file integrity monitoring, security configuration management, vulnerability management and log management. But it also includes additional controls from Tripwire partners and others in the market, such as antivirus/anti-malware, identity and access management, asset management, deployment management, remote management, patch management, email filtering, browser protection, exploit prevention and disaster recovery.

PRIORITIZING SECURITY INVESTMENTS AND EFFORTS

When selecting security controls, you must first take the time to identify which controls to use for all your different types of assets. This takes significant effort and thought. In addition, you must prioritize and balance the following three competing strategies across this complete control set—perhaps an even greater challenge:

» **Depth of coverage**: Make additional use of the controls already in place on the assets already covered

» **Breadth of coverage**: Deploy controls already in use on additional assets not currently covered

» **Broaden control set**: Deploy new controls not currently in use on some assets

Perhaps the most logical way to determine which controls to use and where involves taking a risk-based approach to prioritizing new security projects. This approach makes that determination by forecasting the impact a new project may have on reducing risk and seeking to maximize that impact. In reality, almost any legitimate security control will reduce risk, and the sheer number of defined controls make it impractical to fully evaluate the benefits of each option, so establishing these priorities can present many difficult decisions.

CRITERIA FOR SECURITY CONTROLS DESCRIBED BY THE TRIPWIRE REFERENCE ARCHITECTURE

Tripwire's reference architecture first distills all the possible systems security controls you could deploy into a smaller set that meets the following criteria:

Security is the control's primary function. Some controls like disaster recovery may be critical to security, but serve their primary function in a broader IT operations use case. Such controls would fit into an IT operations reference architecture, and while no less important, are not included here.

Security of the individual system the control interacts with is its primary function. Some controls may combine network-based protections with individual system tools. For example, web filtering may be primarily done with a network proxy, but have a system component available for mobile and remote workers as well. The Tripwire reference architecture excludes such a control because it would typically be found in a network security reference architecture.

The resulting list of system security controls that meet these criteria include antivirus/anti-malware, exploit prevention, file/system integrity monitoring, identity and access management, log management, security configuration management and vulnerability management.

Figure 4 shows the systems to be addressed in the Tripwire reference architecture based on both numbers of the type of asset and importance of the asset to the organization. Not surprisingly, endpoints constitute the most numerous systems, but have the lowest value. Infrastructure sits in the middle, and critical systems, while the least in number, rank highest in importance for an organization. Critical systems include both IT

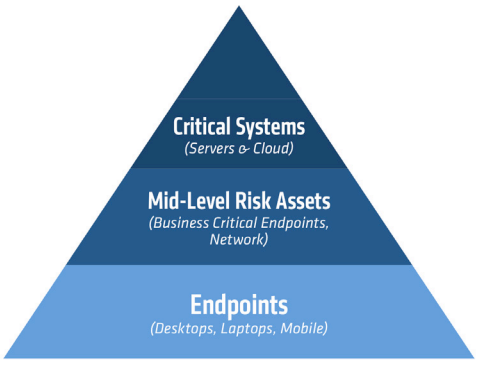

Fig. 4: Pyramid of asset count and value

systems as well as operational technology systems that run the physical operations of a company.

While you can allocate all of your security investment to the top of the pyramid to protect the crown jewels at all costs, that leaves the majority of the organization at the base of the pyramid completely insecure. Finding the right balance of investment is the challenge, but the pyramid figure shows that investment levels should be higher at the top and relatively low at the bottom, on a per asset basis.

This suggests that for the critical systems, all the major security controls are on plan to be implemented, but some controls may be omitted for endpoints, particularly those that require significant human effort to make work operationally. You should construct a more detailed implementation order based on their prioritization with regards to the set of all critical assets—for example, your payment systems may be most critical so you would invest more in securing them sooner than you would in protecting your less, but still critical, assets.

Figure 5 shows how you can allocate systems security controls based on risk. Higher-risk systems inherit the controls from lower risk systems, then add further security controls appropriate for those assets.

Fig. 5: Sample set of system controls allocated by risk

KEY TAKEAWAYS

At this point, you should understand the importance of, and have guidance on, selecting a security framework for creating your reference architecture. You should also recognize the value of selecting a security maturity model and have guidance on making that choice as well.

In addition, you should realize that treating a security framework as a checklist does not work with today's security that relies on an interconnected and coordinated web of security controls. Developing a resilient system for today's security environment benefits greatly from use of a security systems reference architecture that spells out at a high level how each control connects with other controls and systems. Your system also benefits from a security controls reference architecture that takes an in-depth look at each control and its role in the overall systems security architecture.

Finally, you should understand the challenges you'll face when prioritizing your security investments and possible approaches, such as a risk-based approach, that can aid you in meeting this challenge. Prioritization helps you identify the controls you will focus on first when applying your security systems and security controls reference architecture sets.

PART TWO: A REFERENCE ARCHITECTURE FOR FILE & SYSTEM INTEGRITY MONITORING

In Part 1 you learned important background steps to take when developing a system to protect against threats in today's complex and dynamic technology environment and threat landscape. It also introduced three security controls that can help your organization construct a foundation for an effective defense against today's threats. These controls include file integrity monitoring (FIM), security configuration management (SCM), and vulnerability management (VM).

This part of the guide delves into greater detail about the security control FIM, also known as system integrity monitoring or change auditing. FIM is the control that monitors, detects and manages all changes to system state. For simplicity's sake, this guide will use Tripwire's acronym for the capability, FIM, even though identified state changes may be anywhere on a system, and not necessarily in a file.

In this chapter you'll discover:

- Business drivers for FIM from the perspectives of security, compliance and operations
- FIM's relationship to a variety of common security frameworks
- The three main use cases for FIM
- Key integrations of FIM with other controls, systems and workflows
- Descriptions of and diagrams for FIM deployment on both a small and large scale
- Considerations for determining FIM asset coverage and monitoring levels
- Key performance indicators (KPIs) to evaluate your FIM implementation's effectiveness
- C2M2 levels of security maturity your security program can attain using FIM with Tripwire Enterprise
- Standard operating procedures (SOPs) for building, maintaining and operating your FIM solution
- Additional valuable business services you can gain using FIM with Tripwire Enterprise beyond meeting the control objectives for change monitoring

BUSINESS DRIVERS FOR FILE INTEGRITY MONITORING

You may have heard the phrase, "What's good for security is good for compliance." You could modify that phrase to "What's good for security is good for IT operations," and it would still ring true. Security, compliance, and operational requirements tend to be highly interrelated, a fact that's reflected by the demand for FIM across all three programs for these areas.

SECURITY DRIVERS FOR FIM

All security programs monitor for system change. It's a fundamental function, and every security framework includes a control for FIM, often in multiple places. The need for FIM is driven by a requirement to identify unauthorized changes on systems as part of reducing the attack surface of a system to prevent breaches. It's also driven by the need to Identify malicious changes on systems as part of identifying and responding to security incidents.

FIM lets you proactively address security before a breach occurs by identifying possible new risk exposure introduced in an environment, even when done so inadvertently. It also lets you reactively address security after a breach occurs by providing a forensics trail of what happened to a system. This trail may include activity that led to the initial breach activity, along with follow-on actions an attacker may have taken to tamper with the system.

No security program will ever be able to prevent every attack from succeeding, so you need controls in place to quickly identify when malicious events and changes have occurred. And while many controls offer different

ways to detect breaches—network-based, host-based, signatures, behaviors, sandboxes, honeypots, and the like—FIM remains a fundamental and foundational security control because it answers the key question: Are systems still in a secure, trusted state, and if not, what changed? It does not rely on understanding any specific attack signature, vector or exploit to answer that question.

IT OPERATIONS DRIVERS FOR FIM

Undesired change on a system, whether inadvertent or malicious, can not only create security risks, but also availability, reliability and operational failures. FIM's ability to audit change, independent of a deployment process responsible for making the change, provides assurance that a business system is in its desired state, and that undesirable change has not occurred. When an operational incident, such as a system failure, does occur, FIM can provide you historical data to identify what changed on the system, when, and who made that change. This information can help with root-cause analysis and improve operational process going forward. In fact, many organizations use FIM as a detective control for identifying unapproved change as part of their ITIL-based change management process.

COMPLIANCE DRIVERS FOR FIM

As with security configuration management (SCM), FIM is "baked in" to almost every security framework, best practice, compliance mandate and regulation because it is so fundamental to reducing risk in IT environments. The driver for FIM in some organizations may be to comply with a regulatory requirement that the control be in place and auditable. In most cases, the requirement exists because of the security value of the control. However, regulatory requirements often dictate specific implementation details of the control that may go beyond what you may need to address security concerns.

RELATION TO SECURITY FRAMEWORKS

As mentioned earlier, the most commonly used security frameworks include FIM as a required control, many of them mentioning it in multiple places. The table below highlights where several of the common frameworks require or recommend the use of FIM.

Security Framework	Reference
CIS Critical Security Controls	CSC 3.5: Use file integrity checking tools
NIST Cybersecurity Framework	PR.DS-6: Integrity checking mechanisms, PR.IP-1: Baseline configurations, PR.IP-3: Configuration change control processes, DE.CM: Security Continuous Monitoring,
PCI DSS	11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools), 10.5.5 Use file-integrity monitoring or change-detection software on logs,
ISO 27000-series	ISO 27001—10.1.2 Change Management, 10.2.3 Managing changes to third party services, 10.4.1 Controls against malicious code, 12.5.1 Change control procedures, 12.5.2 Technical review of applications after operating system changes, 12.5.3 Restrictions on changes to software packages, 13.2.3 Collection of evidence
COBIT	BAI10 Manage Configuration, F5.1 Adequately secured system services
NERC	CIP-010-1 Cyber Security—Configuration Change Management and Vulnerability Assessments, CIP-007-5 Cyber Security—Systems Security Management, CIP-003-5: Cyber Security—Security Management Controls

FIM USE CASES

In general, FIM tends to be used in three different ways: for change logging, change auditing, and for endpoint detection and response (EDR).

CHANGE LOGGING

In its simplest use case, change logging, FIM lets you produce an audit record of what changed on a system, when, and who made that change. The existence of that audit trail may itself be sufficient to meet a compliance requirement, though you may also find it valuable to

have that audit trail if you need to perform a forensics investigation in the future.

CHANGE AUDITING

Change auditing records the same data as change logging, but adds a heavily automated process that reviews all changes to identify any that are not authorized, approved or desired on the system. Because many changes happen on your production systems, if you fail to thoughtfully implement your change audit solution, it can create the need for a tremendous amount of human interaction. It's important to minimize manual parts of this process and understand any limitations of what can realistically be accomplished. For an effective change auditing process, integrate your FIM solution with your IT operations systems for change management. This enables you to automatically reconcile actual changes with approved and expected changes, leaving relatively few changes for manual review.

ENDPOINT DETECTION AND RESPONSE (EDR)

EDR is a similar use case to change auditing, except it focuses on identifying malicious change rather than unauthorized change. In most cases, an unauthorized change is not malicious; consequently, you don't use the same process, workflow, or review the same characteristics that you would when looking at changes for malicious activity. Filtering out authorized changes from trusted sources, as in change auditing, helps you narrow the scope of change that needs to be assessed for malicious intent.

While EDR is a relatively new term for this use case, the concept of using FIM as a host-based intrusion detection system is well-established. Many organizations have been doing this for years.

FIM KEY INTEGRATION POINTS

As you can see by the change auditing use case, integrating FIM with other systems can extend the value of your FIM solution. But it's not just operational system like change management that provide these benefits—FIM delivers even greater value when integrated with the following security controls, operational system and workflows.

INTEGRATION WITH SECURITY CONFIGURATION MANAGEMENT

Tripwire provides a single product that provides both FIM and security configuration management (SCM) capabilities. This is important because the same configuration items that an SCM monitors for configuration changes with security implications are monitored for change by FIM. When multiple systems continually monitor the same system for the same things, you can impact system performance and experience interaction issues. It just makes sense to consolidate these systems into a single product.

INTEGRATION WITH REPORTING, NOTIFICATION AND REMEDIATION WORKFLOWS

Reporting, notification and remediation workflows are also important integration points for FIM. While your operational reporting may occur at the individual control level, you'll likely use reports, analytics and dashboards that aggregate data across multiple security controls for management reporting purposes.

Similarly, you may wish to send changes that introduce immediate and serious new risks to a security operations center (SOC) for immediate response—such a workflow may involve integrating your FIM solution with a security information event management (SIEM) system. Delivering the change details and suggested remediation action can be as simple as delivering an e-mail to an asset owner, but a more sophisticated integration may create a ticket in your organization's IT ticketing system requesting action to either remediate or justify a waiver for a new risk.

INTEGRATION WITH VULNERABILITY MANAGEMENT

Integrating your FIM solution with a vulnerability management (VM) system provides an effective capability for adaptive monitoring. By feeding the vulnerability state of an asset to the monitoring system, you can dynamically adjust the depth, frequency and response workflow for changes. For example, if you have a system with a new high-risk vulnerability and a high priority risk profile, you may decide that it warrants real-time monitoring across a broad set of system characteristics and immediate SOC notification of a suspicious change. In comparison, if you have the same system with no vulnerabilities, you may just choose to roll up changes for daily review by an analyst before escalating additional action.

INTEGRATION WITH CHANGE MANAGEMENT/ TICKETING AND SOFTWARE RECONCILIATION SYSTEMS

In a change logging use case, FIM can operate in a stand-alone manner with little integration. As noted earlier, integration becomes important for the change auditing use case. Integration with your organization's IT operational change management system can allow you to automatically reconcile a change. If a change is approved, your change management system can simply promote it into the new trusted system state. Filtering out the many regular operational changes from those that need to be reviewed significantly reduces the personnel you require for those manual reviews. Similarly, integrating your FIM solution with your software update systems provides this same filtering and promoting of authorized changes due to regular system updates.

INTEGRATION WITH EDR (THREAT INTELLIGENCE AND MALWARE ANALYTICS SYSTEMS)

For an EDR use case, integrating your FIM solution with security technologies like threat intelligence sources and malware analytics systems becomes particularly important. With a threat intelligence integration, you can compare changes identified in your FIM against previously seen indicators of compromise from commercial, open source or peer threat intelligence sources. This comparison examines your past change history for forensics, but also continuously looks for known threats.

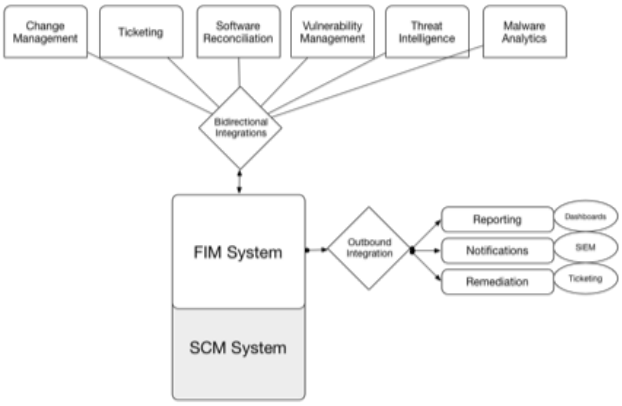

Diagram Architecture for key integration points for file integrity monitoring (FIM)

FIM DEPLOYMENT WITH TRIPWIRE

Tripwire offers Tripwire® Enterprise as its primary FIM product. Although Tripwire Configuration Compliance Manager (CCM) also provides FIM capabilities appropriate for change logging, it's not as well suited for change auditing or EDR. Tripwire Enterprise is covered in this paper. The chapter, which discusses SCM, includes more details on Tripwire CCM deployment architecture.

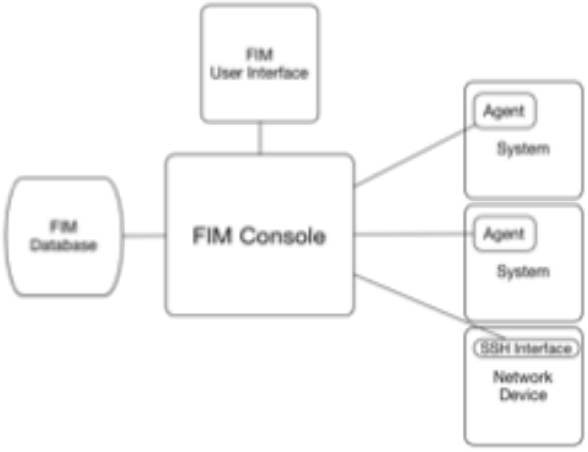

Diagram Tripwire Enterprise model – FIM deployment with agents and agentless (SSH Interface)

At the highest level, you can break FIM deployment into the FIM management layer and the assets it monitors. With Tripwire Enterprise, FIM management consists of a central console, responsible for communicating with monitored assets and central management, a back-end database for storage, and a user interface for configuration and usage. Tripwire Enterprise monitors assets by deploying an agent on the asset when possible, but using an agentless approach through existing network management interfaces (SSH), where appropriate.

For large-scale deployments, you can use multiple FIM consoles or management servers, and then use Tripwire Connect to aggregate data into a higher-tier for consolidated reporting and management.

DETERMINING FIM ASSET COVERAGE AND MONITORING

Figuring out which assets to monitor—and how

intensely—with FIM takes a great deal of time and effort. It's a balance of resource use versus potential security benefit.

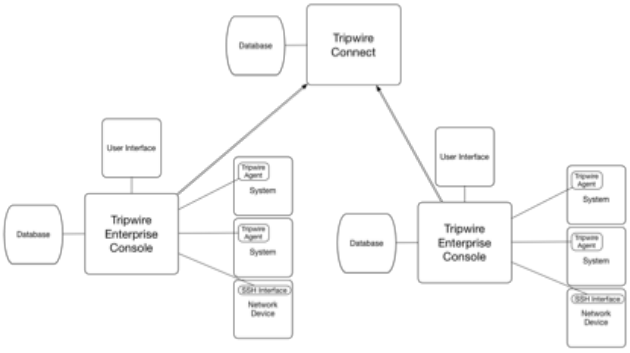

Diagram Aggregated Reporting, Analytics, and Visualization provided by additional component for additional scalability and capabilities

With that in mind, the most people- and process-intense use case for FIM, change auditing, is best limited to the systems that are both most important to the organization and that also have change control processes built around them. As a detective control for change, you'll find it difficult and time-consuming to determine and reconcile unauthorized changes with no way to manage that process operationally.

The less intensive use cases for FIM, change logging and EDR, can be effective without the same level of operational processes; consider a broader deployment of FIM for these use cases. SCM, along with lightweight change logging of the most critical system files and EDR, provides an effective combination.

Effective FIM also requires you to identify the right parts of a system to monitor on a per system level. Monitoring for a system too broadly—for example, trying to monitor every file on a system—creates significant noise from identifying changes to meaningless items such as temporary folders and cache files. Individual applications often place their own temporary files in many different places on a system, so it's important to identify locations of the important areas of a system to monitor, both from a system file and an application level.

If some cases, regulation may be your biggest driver for prioritizing coverage. If you have a particular set of devices in scope for change monitoring for a regulatory requirement, it makes sense to make those a top priority. Other factors to consider when prioritizing coverage include risk levels, business functions and the presence of sensitive data.

EVALUATING EFFECTIVENESS

Identifying and tracking key performance indicators (KPIs) for your FIM implementation can help you evaluate your security program's effectiveness. In reviewing KPIs, don't lose sight of the key objectives of FIM. Although these objectives may vary depending on your organizational goals, they'll typically include breach detection, effective incident response, proactive risk reduction, improved operations and demonstrable compliance. Make sure that the indicators you select do indeed reflect the effectiveness of your FIM process in achieving those goals.

Tripwire has developed a set of commonly used metrics and criteria that may be used for evaluating your FIM implementation. These should thoughtfully considered, and then tailored to meet your organization's specific business needs and structure:

- **Unapproved Changes**—The number of unapproved changes detected
- **Configuration Drift**—The relative difference asset configurations have compared to approved configurations
- **Malicious Changes**—The number of malicious changes detected
- **Incident Response**—The number of incidents that leveraged FIM in response
- **Asset Coverage**—The number of assets of an asset set (or complete organization) with active FIM

For each of these metrics, evaluate the data across several categories or dimensions, including:

- Enterprise-wide
- By System Type
- By Business Function
- By Business Unit
- By Regulatory Scope

RELATIONSHIP OF FIM TO THE C2M2 MATURITY MODEL

As emphasized in the Part 1 of the Tripwire Reference Architecture series, a security maturity model can guide your organization's security program as it advances to higher levels. Maturity models do this by explaining what your security program can achieve by implementing recommendations for a control, but also by describing what additional technologies, processes or people your program must have in place to work its way up through the various maturity levels.

While you can use any maturity model to advance your program, this guide refers to the C2M2 security maturity model, shown below, and relates that to using FIM with Tripwire Enterprise.

C2M2 DOMAINS RELEVANT TO FIM

The C2M2 maturity model categorizes broad areas of security programs into domains. FIM falls within the Asset, Change, and Configuration Management domain, but also contributes to the Situational Awareness and Event and Incident Response domain. When implemented using best practices, FIM with Tripwire Enterprise can help an organization reach up to a MIL3—the highest level of maturity—for the relevant areas of these domains. What determines the maturity level of your organization actually depends not so much on the technology, but on the maturity level of the processes and associated personnel in place.

In reality, the specific activities outlined in these domains for reaching the various maturity levels don't always directly apply to the narrower scope of FIM. However, this guide uses best judgment and experience to provide guidance in assessing your organization's maturity level with FIM for these activities. If you'd like to learn more about the specific activities, refer to the sections 5.2, 5.5, and 5.7 of the C2M2 Security Maturity Model.

ADVANCING THROUGH THE MATURITY LEVELS

During the initial phase of deploying and operationalizing Tripwire Enterprise, most organizations tend to operate at MIL1. If you're operating at this maturity level, you're using Tripwire Enterprise to accomplish essential and necessary activities related to FIM. These activities include deployment of Tripwire Enterprise agents on critical systems and ongoing change monitoring. It also includes having procedures in place for manually reviewing changes that Tripwire Enterprise indicates are unauthorized or associated with suspicious activity.

To move up to MIL2, you must mature your processes and practices around FIM. Processes will be more formally documented and you will be incorporating more best practices used by other organizations in these areas, particularly around the use of automation. Although at MIL1, you may be performing the same practices around integrity monitoring and have some process documentation, as your program evolves to MIL2 and then on to MIL3, processes and practices should become more comprehensive and formalized.

Several organizations with Tripwire Enterprise have evolved their implementation up to MIL3. The next section presents standard operating procedures (SOPs) based on these organizations that you can leverage as best practices to help your organization reach higher maturity levels.

FIM STANDARD OPERATING PROCEDURES

Tripwire offers a variety of documentation for standard operating procedures (SOPs) for FIM based on successful Tripwire Enterprise implementations. These can be extremely useful in helping you build, maintain and operate your Tripwire solution for FIM. Because SOPs are very specific to an organization both in the actual procedures developed, but also in how they're organized and presented, you'd be hard pressed to find a standard set of documentation that fully meets your organization's needs. However, the following documentation developed from Tripwire customers operating at MIL2 and MIL3 can provide a valuable starting point in developing a set of SOPs tailored for your organization.

Alternatively, you can work with Tripwire Professional Services to develop these procedures.

1. Sample Operational Procedures from Tripwire Remote Operations—A sample set of procedures based on the experiences of Tripwire consultants managing Tripwire Enterprise implementations on behalf of customers.

2. Sample Design and Implementation Guide for Tripwire Enterprise—Operational process docu-

mentation collaboratively developed by Tripwire Professional Services with a Tripwire customer that has mature processes in in place.

3. Standard Operating Procedures Outline—An outline of an SOP document from a Tripwire customer with a more mature, process-oriented security program and Tripwire Enterprise implementation. This outline provides a template that you can use to develop your organization's internal process documentation.

ADDITIONAL SERVICES PROVIDED BY TRIPWIRE ENTERPRISE FIM

You can leverage FIM capabilities in Tripwire Enterprise to deliver additional value to the business beyond meeting a security control objective for change monitoring. These unique service offerings, made up of one or more Tripwire Enterprise capabilities, may be of particular interest to specific users within your organization, and are worth investigating. The following table describes each service, along with its associated capabilities and target users:

KEY TAKEAWAYS

From reading this section, you've learned the value that FIM provides the organization—not just from a security perspective, but also from IT operations and compliance perspectives. You've also discovered how FIM relates to some of the most commonly used frameworks, and the three main use cases for FIM—change logging, change auditing, and endpoint detection and response. In addition, you've discovered the value of integrating FIM with other security controls, operational systems and workflows to extend the value of your solution.

The paper then gets more specific, explaining not only how to deploy FIM with Tripwire Enterprise, but also how it can help you advance your security program based on the C2M2 security maturity model. From a practical standpoint, this Prescriptive Guide leaves you with three documents for developing your own set of standard operating procedures for building, operating and maintaining your Tripwire Enterprise implementation for FIM. Finally, it outlines additional valuable business services related to security that Tripwire Enterprise offers your organization beyond simply meeting the control objective of change monitoring.

In short, you have hopefully realized how much security benefit you can derive from a FIM solution, particularly a solution based on Tripwire Enterprise.

PART THREE: A REFERENCE ARCHITECTURE FOR SECURITY CONFIGURATION MANAGEMENT

In Part 1: *A Guide for Building a System for Adaptive Threat Protection Based on a Security Reference Architecture*, you learned important background steps to take when developing a system to protect against threats in today's complex and dynamic technology environment and threat landscape. It also introduced three security controls that can help your organization construct a foundation for an effective defense against today's threats. These controls include file integrity monitoring (FIM), security configuration management (SCM), and vulnerability management (VM).

Part 2: *A Reference Architecture for File & Server Integrity Monitoring* delved into greater detail about the security control FIM. In this part of the guide, you'll learn similar details about SCM. SCM is the control that assures system are set up and maintained in a way that minimizes risk while still providing the essential business function of the system.

In this chapter you'll discover:

- Business drivers for SCM from the perspectives of security and compliance
- The relationship of SCM to a variety of common security frameworks
- The two main use cases for SCM
- Key integrations of SCM with other controls, systems and workflows
- Descriptions of and diagrams for SCM deployment
- Considerations for determining SCM asset coverage and monitoring levels
- Key performance indicators (KPIs) to evaluate your SCM implementation's effectiveness
- C2M2 levels of security maturity your security program can attain using SCM with Tripwire
- Standard operating procedures (SOPs) for building, maintaining and operating your SCM solution
- Additional valuable business services you can gain using SCM with Tripwire beyond meeting the control objectives

BUSINESS DRIVERS FOR SECURITY CONFIGURATION MANAGEMENT

Extensive security research has shown that misconfigurations, many of them easy to correct, have been the underlying reason for many successful breaches. You can use SCM to identify and remediate these issues to provide a proactive defense against attacks.

If you have a smaller technology environment, you can use manual processes or leverage built-in tools provided by business systems to accomplish SCM. However, if you have a larger, more complex technology environment consisting of numerous systems with differing configuration states and business requirements, the operational cost of taking a manual or less sophisticated approach can be significant. In these environments, you need technology that automates the assessment, monitoring, and management of configurations across all your systems to ensure their ongoing security.

DRIVERS FOR SCM FOR SECURITY

Two complementary requirements often drive the need for SCM. The first, to reduce your organization's security risk by assuring you have secure configurations in place. The second, to ensure your compliance with regulations that require you to have this control in place and auditable. As you can see, these two requirements are highly inter-related, with compliance around SCM helping ensure IT and data security, and security for your SCM directly supporting compliance.

From a security standpoint, you'll see that almost every security framework, best-practice, and regulation has SCM baked in. That's because SCM is so fundamental to reducing risk in an environment.

From a compliance perspective, your organization may require SCM to achieve regulatory compliance. In almost all cases, that regulatory requirement exists because of the security value of the control. It's important to note that regulatory requirements may dictate specific implementation details of the control that may go beyond what would you would minimally need to address the security concerns.

RELATION TO SECURITY FRAMEWORKS

As noted earlier, most security frameworks bake in SCM due to its fundamental ability to reduce risk. The table below highlights where several of the most common frameworks require or recommend the use of SCM.

SECURITY FRAMEWORK	REFERENCE
CIS Critical Security Controls	CSC 3: Secure Configurations for Hardware and Software
NIST Cybersecurity Framework	PR.IP-1: Baseline configurations created and maintained PR.IP-3: Configuration change control processes
PCI DSS	1.1, 2.1, 2.2, 2.3, 5.2, 6.1, 6.4, 8.5
ISO 27000-series	ISO 27001 – 10.1.2, Change Management; 11.3, 11.4, 11.5, 12.5, 15.2.2, Technical compliance checking; 15.3.1, Information systems audit controls
COBIT	DS9.1 Configuration repository and baseline; DS9.2, Identification and maintenance of configuration items; DS9.3, Configuration integrity review
NERC	CIP-010-1 Cyber Security—Configuration Change Management and Vulnerability Assessments, CIP-007-5 Cyber Security—Systems Security Management, CIP-003-5: Cyber Security—Security Management Controls

USE CASES FOR SCM

In general, you will use SCM in two distinct ways: for assessment and continuous monitoring.

ASSESSMENT

In the assessment use case, SCM compares the current state of your systems against a set of secure configuration policies. These policies have been built by security experts and represent secure settings you should use when configuring your various types of systems. The comparison results show you which system settings meet those recommendations, but also which system settings create deficiencies.

When your SCM assessment detects deficiencies, it should detail the actual configuration state and the expected configuration state. It should also explain the risk posed by the current deficient state and provide you with recommended remediation actions for bringing the configuration into compliance with the recommended best practice.

In addition, your SCM assessment should include a high-level view of and guidance on your organization's overall state of compliance against best-practices, segmented by the way your organization operates. For example, it should include aggregated reporting by system types, business functions, network segmentation, and geography. While achieving a 100 percent compliant state borders on the impractical, it's important that your SCM help you establish an acceptable risk level based on what's considered typical for specific types of systems and your organization as a whole.

Your SCM should be able to produce an assessment report that contains this type of information, and that also presents and distributes it in a way that's suitable for various stakeholders. For example, a report for individual asset owners should contain enough detail to allow them to take necessary remediation action, while a report for security management should provide the right level of information for them to review to obtain an overall sense of the state of system configurations.

While the act of performing the assessment may fulfill compliance requirements, many regulations require that you maintain evidence of the assessment for audits. Your SCM reports should be able to provide that evidence.

CONTINUOUS MONITORING

Performing an assessment is an important first step in bringing SCM to an organization, but with the assessment alone, you've not reduced your security risk. Only by taking follow-up actions on risks identified by the assessment can you do reduce your risk, and that requires ongoing engagement from your people, processes, and technology involved in SCM to drive that action. To make real security maturity gains and realize the true value offered by SCM, you must quickly progress to using SCM for continuous monitoring.

In the continuous monitoring use case for SCM, your SCM solution monitors the state of systems against secure configuration policies on an ongoing basis. Your organization has a continuous view into the state of each system against its secure configuration policy, but also an aggregate view of system state segmented according to business needs.

Inevitably, a system's state will not align with its secure configuration policy. Occasionally, this misalignment can be introduced by updates to the configuration policy itself, but more often it can be due to changes that occur to the actual state of a system. When your SCM detects differences between actual system settings and the secure configuration policy, it kicks off a workflow for you to address that discrepancy. The workflow may involve notifying your security team, escalating the issue to the asset owner, or providing an aggregate view of all such violations that have occurred for prioritization and follow-on actions.

In some cases, best practices may dictate using one configuration, while business requirements dictate another. By building a complete workflow allowing those deviations from the secure configuration to be evaluated, and if desired accepted, you can determine the right balance between business value and risk.

To build a mature process for SCM, your organization should automate not only the initial assessment of compliance, but the complete lifecycle of addressing configuration drift that impacts security.

SCM KEY INTEGRATION POINTS

SCM delivers even greater value when you integrate it with the following security controls, operational system, and workflows.

INTEGRATION WITH FILE/SERVER INTEGRITY MONITORING

Tripwire provides single products that cover both FIM and SCM. This is important because the same configuration items that an SCM monitors for configuration changes with security implications are monitored for change by FIM. When multiple systems continually monitor the same system for the same things, you can impact system performance and experience interaction issues. It just makes sense to consolidate these systems into a single product.

It's important to understand that integration points for SCM differ from those for FIM, though. For example, FIM identifies if a change is authorized or unauthorized. This suggests, as is detailed in the Reference Architecture for File/System Integrity Monitoring, the importance of integrating change management systems. For SCM, however, an authorized change may still inadvertently create security risk, so you still must evaluate and respond appropriately to both authorized and unauthorized change.

INTEGRATION WITH REPORTING, NOTIFICATION AND REMEDIATION WORKFLOWS

Reporting, notification, and remediation workflows are also important integration points for your SCM solution. While your operational reporting may occur at the individual control level, you'll likely use reports, analytics, and dashboards that aggregate data across multiple security controls for management reporting purposes.

Similarly, you may wish to send changes that introduce immediate and serious new risks to a security operations center (SOC) for immediate response—such a workflow may involve integrating your SCM solution with a security information event management (SIEM) system. Delivering the change details and suggested remediation action can be as simple as delivering an e-mail to an asset owner, but a more sophisticated integration may create a ticket in your organization's IT ticketing system requesting action to either remediate or justify a waiver for a new risk.

INTEGRATION WITH SECURE CONFIGURATION POLICIES

The most critical inputs for your SCM integration are the best-practices policies against which it will assess and monitor the configurations. While you may choose

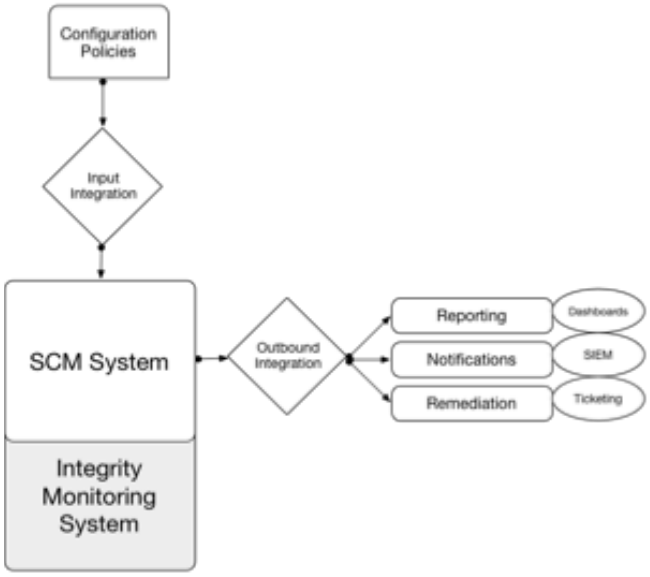

Diagram: Architecture for key integration points for SCM

to use out-of-the-box policies included with your SCM product, larger organizations will often have their own internal processes for developing, evolving, and managing configuration policies, which they will then operationalize into the SCM system. The process by which you select and use policies is a critical aspect of your SCM deployment.

SCM DEPLOYMENT WITH TRIPWIRE

Tripwire offers Tripwire Enterprise and Tripwire Configuration Compliance Manager (CCM) for SCM. The deployment architecture is similar between the two products.

At the highest level, you can break SCM deployment into the SCM management layer and the assets it monitors. SCM management consists of a central console for communicating with monitored assets and central management, a back-end database for storage, and a user interface for configuration and usage. Tripwire SCM products monitor assets through deployed agents, existing network management interfaces (agent-less), or dissolvable agents—software temporarily placed on the device to gather data (which some may consider agent-less).

In an agentless deployment like that used with Tripwire CCM, you may have an additional component, a scan engine. One or more scan engines may be deployed around your network for communicating with the monitored devices to collect data from them, aggregate that data, and delivered the aggregated data to the central management system.

For large-scale deployments of either agent-based or agentless systems, you can use multiple consoles or management servers and aggregate data into a higher tier for consolidated reporting and management. Tripwire Enterprise uses Tripwire Connect as its aggregation layer, while with Tripwire CCM uses Tripwire Security Intelligence Hub.

DETERMINING SCM ASSET COVERAGE AND MONITORING

Although you get the best security by covering every asset in an organization with SCM monitoring, this is not always possible or practical. Even if the ultimate goal is complete coverage, you will always need to prioritize and select the sets of devices that will provide the most value from having SCM.

In many cases, regulation is the biggest driver for coverage prioritization. If a particular set of devices is in scope for a regulatory requirement, it makes sense to

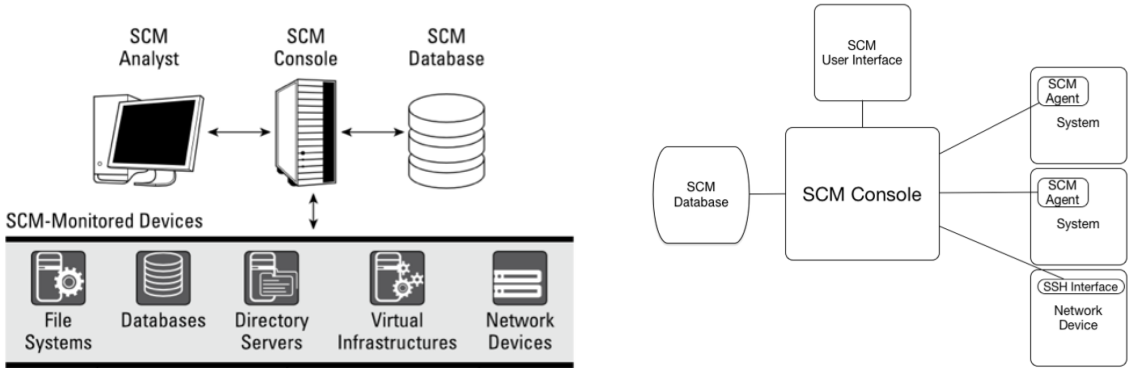

Diagram: Tripwire Enterprise model—SCM Deployment with both agent and agentless approaches used

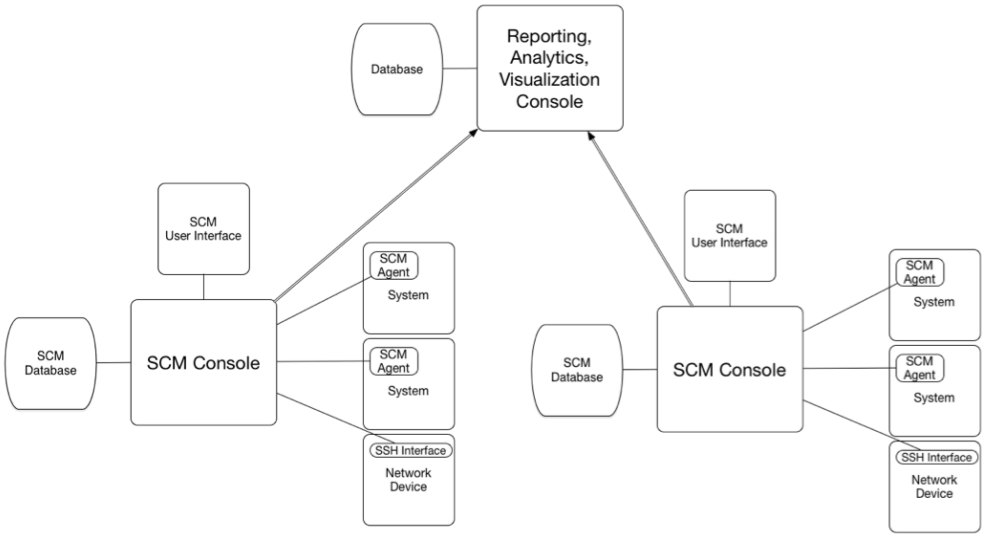

Diagram: Aggregated reporting, analytics, and visualization provided by additional component for additional scalability and capabilities

put those devices at the top of the priority list. You should also consider prioritizing coverage by factors such as risk, business functions, and the presence of sensitive data.

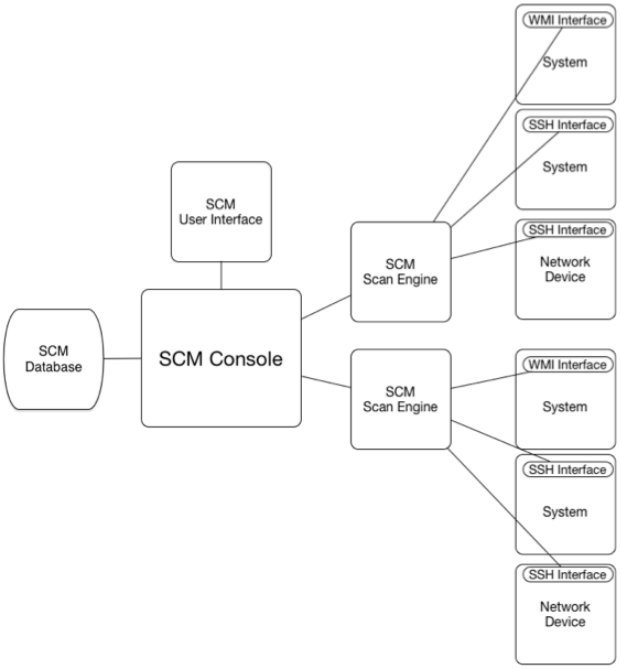

Diagram: Tripwire Configuration Compliance Manager includes a scan engine component to support agentless and dissolvable agent approaches

The readiness of a particular asset, group of assets, or part of an IT organization for SCM is also an important consideration when prioritizing coverage. For example, if you already have a set of best practices security policies defined for your Unix servers, an IT administration team capable of remediating issues on them, and asset owners who have bought into the value of SCM, you're better off deploying SCM on those systems than on a mainframe system that has no clear pre-existing policy and an administrator who would be reticent to make any changes even if security issues were communicated to him or her.

When determining asset coverage, create a practical and realistic roadmap, starting with the most critical systems and working to expand to others over time. The roadmap below, which is similar to roadmaps used by many Tripwire customers, can be a good starting point and guide.

Priority	Assets	Timeline
1	Payment and Personal Information server group	3 months
2	All Unix servers and core network devices	6–9 months
3	All Windows servers	9–12 months
4	Windows desktops	12–24 months
5	OT/Manufacturing systems	24–36 months

EVALUATING EFFECTIVENESS

Identifying and tracking key performance indicators (KPIs) for your SCM implementation can help you evaluate your security program's effectiveness. In reviewing KPIs, don't lose sight of the key objectives of SCM: first, to proactively prevent successful breaches by reducing the attack surface of systems, and second, if applicable, to ensure compliance with regulatory standards. Make sure that the indicators you select do indeed reflect the effectiveness of your SCM process in achieving those goals.

Tripwire has developed a set of commonly used metrics and criteria that may be used for evaluating your SCM implementation. These should be thoughtfully considered and then tailored to meet your organization's specific business needs and structure:

- **Policy Compliance**—The level of compliance of assets against the configured policies
- **Average Risk Score**—The level of risk of assets based on deviations from configured policies
- **Top Policy Failures**—The most common deviations from configured policies across an asset set
- **Asset Coverage**—The number of assets of an asset set (or complete organization) with active SCM

For each of these metrics, evaluate the data across several categories or dimensions, including:

- Enterprise-wide
- By System Type
- By Business Function
- By Business Unit
- By Regulatory Scope

RELATIONSHIP OF SCM TO THE C2M2 MATURITY MODEL

As emphasized in the introductory part of this guide, a security maturity model can guide your organization's security program as it advances to greater levels of security. Maturity models do this by explaining what your security program can achieve by implementing recommendations for a control, but also by describing what additional technologies, processes, or people your program must have in place to work its way up through the various maturity levels.

While you can use any maturity model to advance your program, this guide refers to the C2M2 security maturity model, shown below, and relates that to using SCM with Tripwire Enterprise or Tripwire Configuration Compliance Manager.

C2M2 DOMAINS RELEVANT TO SCM

The C2M2 maturity model categorizes broad areas of security programs into domains. SCM falls within the C2M2 Asset, Change, and Configuration Management domain. In addition to addressing SCM, this This domain encompasses asset inventory, integrity monitoring, and vulnerability management are all relevant to this domain.

Within the scope of the objectives and practices relevant to SCM, implementing the Tripwire Reference Architecture for SCM supports an organization reaching either the MIL2 or MIL3 level of maturity. To reach MIL3, you must have more detailed processes and associated personnel in place for configuration and change management. You must also ensure that you've rolled out SCM comprehensively, including in the preproduction phases of your deployment processes.

If you'd like to learn more, refer to section 5.2 of the C2M2 Security Maturity Model, available at www.energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program/cybersecurity

ADVANCING THROUGH THE MATURITY LEVELS

During the initial phase of deploying and operationalizing Tripwire Enterprise and Tripwire CCM, most organizations tend to operate at MIL1. If you're operating at this maturity level, you're using these solutions to accomplish essential and necessary activities related to SCM. These activities include deployment of Tripwire Enterprise agents or agentless deployment of Tripwire Configuration Compliance Manager on critical systems and ongoing security configuration assessments and monitoring. It also includes having procedures in place for reviewing changes that your Tripwire SCM solutions indicate fail to align with the associated policy.

STANDARD OPERATING PROCEDURES OUTLINE

The outline below provides a sample set of Standard Operating Procedures:

- Define the objectives you want to achieve with the control
- List any applicable regulatory requirements
- Describe the deployment of your Tripwire Enterprise or Tripwire Configuration Compliance Manager solution
- Define roles and responsibilities for:
  - System owners
  - System administrators
  - Information security operators
  - Information security managers
- Describe the review process for out-of-policy configuration settings
  - List any responsible parties for reviewing out-of-policy settings
  - Define escalation procedures
  - Describe the scheme for prioritizing out-of-policy settings for review
  - Define the frequency of reviewing out-of-policy settings
  - Explain the procedure for promoting a setting to the baseline and updating the policy
  - Describe alerts to high-priority out-of-policy settings
- Describe the process for onboarding new assets and applications
- Document the reports you will automatically generate, including details about:
  - Nodes included in the report
  - Responsible parties to whom you will deliver reports
  - Frequency of generating reports

To move up to MIL2, you must mature your processes and practices around SCM. Processes will be more formally documented and you will be incorporating more best practices used by other organizations in these areas, particularly around the use of automation. Although at MIL1, you may be performing the same practices around assessment and continuous monitoring and have some process documentation, as your program evolves to MIL2 and then on to MIL3, processes and practices should become more comprehensive and formalized.

Several organizations with Tripwire Enterprise have evolved their implementation up to MIL3. The next section presents SOPs based on these organizations that you can leverage as best practices to help your organization reach higher maturity levels.

SOPs FOR SCM

Tripwire offers a variety of documentation for SOPs for SCM based on successful Tripwire Enterprise implementations. These can be extremely useful in helping you build, maintain, and operate your Tripwire solution for SCM. Because SOPs are very specific to an organization both in the actual procedures developed, but also in how they're organized and presented, you'd be hard pressed to find a standard set of documentation that fully meets your organization's needs. However, the following documentation developed from Tripwire customers operating at MIL2 and MIL3 can provide a valuable starting point in developing a set of SOPs tailored for your organization. Alternatively, you can work with Tripwire consulting to develop these procedures.

1. Sample Operational Procedures from Tripwire Remote Operations. A sample set of procedures based on the experiences of Tripwire consultants managing Tripwire Enterprise and Tripwire CCM implementations on behalf of customers.

2. Sample Design and Implementation Guide for Tripwire Enterprise and Tripwire CCM. Operational process documentation collaboratively developed by Tripwire Professional Services with a Tripwire customer that has mature processes in in place.

3. Standard Operating Procedures Outline. An outline of an SOP document from a Tripwire customer with a more mature, process-oriented security program and Tripwire Enterprise or Tripwire CCM implementation. This outline, shown below, provides a template that you can use to develop your organization's internal process documentation.

ADDITIONAL SERVICES PROVIDED BY TRIPWIRE SCM

You can leverage SCM from either Tripwire Enterprise or Tripwire CCM to deliver additional valuable services to the business beyond meeting a security control objective for security configuration management. These unique service offerings, made up of one or more capabilities of either Tripwire solution for SCM, may be of particular interest to specific users within your organization, and are worth investigating.

The table below describes each service, along with its associated capabilities and target users.

KEY TAKEAWAYS

From reading this chapter, you've learned the value that SCM provides your organization—not just from a security perspective, but also from a compliance perspective. You've also discovered how it relates to some of the most commonly used frameworks, and the two main use cases for SCM—assessment and continuous monitoring. In addition, you've discovered the value of integrating SCM with other security controls, workflows, and security configuration policies to extend the value of your solution.

The guide then gets more specific, explaining not only how to deploy SCM with Tripwire Enterprise or Tripwire CCM, but also how it can help you advance your security program based on the C2M2 security maturity model. From a practical standpoint, the guide leaves you with three different documents for developing your own set of standard operating procedures for building, operating and maintaining your Tripwire SCM implementation. Finally, it outlines additional valuable business services related to security that Tripwire SCM solutions offer your organization beyond simply meeting the control objective of assessment and continuous monitoring of configurations.

In short, you have hopefully realized how much security benefit you can derive from a SCM solution, particularly a solution based on Tripwire Enterprise or Tripwire Configuration Compliance Manager.

Service	Capabilities	Target Users
Policy Compliance	Compare the current state of a system against specific regulatory or internal compliance requirements and produce compliance reporting on deviations and a process for remediation.	Compliance auditors IT system owners IT application owners IT system administrators
Configuration State Assessment	Compare the current state of a system to a desired state and tell me where it deviates. Allow an administrator to provide policy standards for configuration in an application and have systems assessed against those standards on an ongoing basis.	Compliance auditors IT system owners IT application owners IT system administrators
Whitelist Profiling	Allow an administrator to define the set of ports, services, and applications that are intended to be used on a system and have the system monitored to validate the system does not deviate from that defined configuration, with a mechanism for notification to appropriate stakeholder if a variation occurs.	Compliance auditors IT system owners IT application owners IT system administrators
Reference Node Comparison	Compare the differences between a reference node and any of the other nodes of the same group so variations and non-standard configurations are easily identified.	Compliance auditors IT system owners IT application owners IT system administrators

Table. Additional valuable business services offered by SCM from Tripwire

PART FOUR: A REFERENCE ARCHITECTURE FOR VULNERABILITY MANAGEMENT

In Part 1: *A Guide for Building a System for Adaptive Threat Protection Based on a Tripwire Reference Architecture*, you learned important background steps to take when developing a system to protect against threats in today's complex and dynamic technology environment and threat landscape. It also introduced three security controls that can help your organization construct a foundation for an effective defense against today's threats. These controls include file integrity monitoring (FIM), security configuration management (SCM), and vulnerability management (VM).

Parts 2 and 3 delved into greater detail about the security controls FIM and SCM, respectively. In this part of the guide, you'll learn similar details about vulnerability management (VM). VM is the control that assures that you minimize the risk of systems being successfully exploited by continuously identifying, prioritizing, and mitigating vulnerabilities.

In this part of the guide, you'll discover:

- Business drivers for VM from the perspectives of security and compliance
- The relationship of VM to a variety of common security frameworks
- The two main use cases for VM
- Key integrations of VM with other controls and systems
- Descriptions of and diagrams for VM deployment
- Considerations for determining VM asset coverage and monitoring levels
- Key performance indicators (KPIs) to evaluate your VM implementation's effectiveness
- C2M2 levels of security maturity your security program can attain using VM with Tripwire
- An approach to inventorying systems to protect and categorizing them
- Standard operating procedures (SOPs) for building, maintaining and operating your VM solution

BUSINESS DRIVERS FOR VULNERABILITY MANAGEMENT

Today, tens of thousands of known vulnerabilities exist, with thousands of new vulnerabilities discovered each year by security researchers. Although eliminating all vulnerabilities from your organization it is almost impossible, an effective vulnerability management process can significantly reduce the risk vulnerabilities pose.

Two complementary requirements often drive the need for VM. The first, to reduce your organization's security risk by mitigating the highest risk vulnerabilities in an environment. The second, to ensure your compliance with regulations that require you to have this control in place and auditable. As you can see, these two requirements are highly inter-related, with compliance around VM helping ensure IT and data security, and security for your VM directly supporting compliance.

From a security standpoint, you'll see that almost every security framework, best-practice, and regulation has VM baked in. That's because VM is so fundamental to reducing risk in an environment.

From a compliance perspective, your organization may require VM to achieve regulatory compliance. In almost all cases, that regulatory requirement exists because of the security value of the control. It's important to note that regulatory requirements may dictate specific implementation details of the control that may go beyond what would you would minimally need to address the security concerns.

RELATION TO SECURITY FRAMEWORKS

As noted earlier, most security frameworks bake in VM due to its fundamental ability to reduce risk. The table below highlights where several of the most common frameworks require or recommend the use of VM.

Security Framework	Reference
CIS Critical Security Controls	CSC 1: Inventory of Authorized and Unauthorized Devices, CSC 4: Continuous Vulnerability Assessment and Remediation
NIST Cybersecurity Framework	PR.IP-12: A vulnerability management plan is developed and implemented,
PCI DSS	11.2 Run internal and external vulnerability scans
ISO 27000-series	ISO/IEC 27002 12.6 Technical vulnerability management
COBIT	DSS03.01 Identify and classify problems
NERC	CIP-010 R3 Vulnerability Assessments, CIP-002 R1: BES Cyber System Identification

USE CASES FOR VM

In general, you will use VM in two distinct ways: for assessment and continuous monitoring.

ASSESSMENT

In the assessment use case, you run a one-time scan of your systems to identify the current state of vulnerabilities on those systems. The scan collects details about detected vulnerabilities, including what it is, evidence of its existence on the system, the risk it poses based on a sensible scoring algorithm, and information on you to mitigate and remediate the vulnerability.

In addition to providing details about the vulnerability state of individual systems, the assessment needs to prioritize vulnerabilities across your assets. This allows your organization to make the most effective decision on how to prioritize use of IT resources to reduce risk. Achieving a state of zero vulnerability risk borders on the impossible, so it can be valuable and practical to establish some benchmark level of vulnerability risk that you can tolerate. Risk that exceeds that benchmark is therefore intolerable and requires immediate action.

Your VM should be able to produce an assessment report that contains this type of information, and that also presents and distributes it in a way that's suitable for various stakeholders. For example, a report for individual asset owners should contain enough detail to allow them to take necessary remediation action, while a report for security management should provide the right level of information for them to review to obtain an overall sense of the state of vulnerability risk.

While the act of performing the assessment may fulfill compliance requirements, many regulations require that you maintain evidence of the assessment for audits. Your VM reports should be able to provide that evidence.

CONTINUOUS MONITORING

Performing an assessment is an important first step in bringing VM to an organization, but with the assessment alone, you've not reduced your security risk. Only by taking follow-up actions on risks identified by the assessment can you reduce your risk, and that requires ongoing engagement from your people, processes, and technology involved in VM to drive that action. To make real security maturity gains and realize the true value offered by VM, you must quickly progress to using VM for continuous monitoring.

In the continuous monitoring use case, your VM solution assesses systems for new vulnerabilities on an ongoing basis. The speed at which your organization can act on the information tends to drive the frequency of these assessments more than any technical limitations do.

Your solution can discover new vulnerabilities in your environment as a result of many different events—for example, when you install new software or start a new service on an existing system or bring a new system online. It can also discover new vulnerabilities when your update your VM solution with the latest vulnerabilities for assessments, something that can happen weekly, if not more often.

Your organization will build a workflow process around the new vulnerabilities your VM solution discovers in your environment. This workflow typically includes prioritizing a vulnerability based on the risk to the asset, the value of the asset to the organization, and any mitigating factors that may reduce the likelihood of exploitation.

Because you will tend to manage VM independently from IT operations, you'll usually deliver any remediation actions to another part of the organization and have them carry out these actions. The VM process involves escalating the necessary actions to the appropriate individuals, tracking the remediation efforts, and verifying the vulnerability has been remediated. You'll usually verify remediation at the next scheduled assessment, although you can verify on-demand if you need or want.

To build a mature process for VM, your organization should automate as much of the VM process as possible.

VM KEY INTEGRATION POINTS

VM delivers even greater value when you integrate it with other security controls, operational system, and workflows. Tripwire IP360 is Tripwire's vulnerability management solution.

INTEGRATION WITH MANY SECURITY SYSTEMS AS A DATA SOURCE

You can use your VM as a source to supply security data to many of your other security systems and solutions. For example, your intrusion detection system, risk analytics system, security information and event management (SIEM) tools, and security dashboards may take feeds of data from your VM solution.

INTEGRATION WITH TICKETING SYSTEMS

You may have the option to integrate your VM with your ticketing system. This integration can happen either directly to the VM system or through a higher-level reporting system.

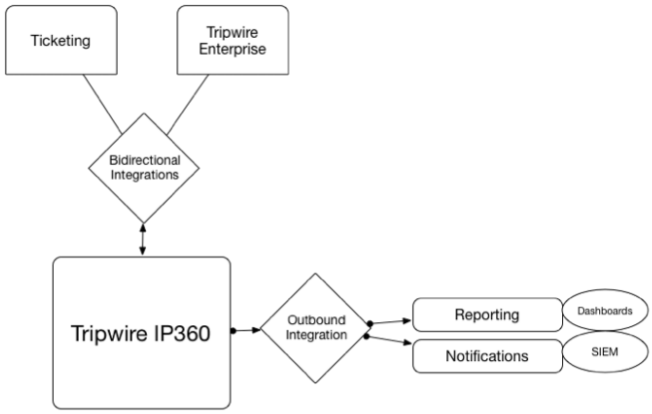

Diagram: Architecture for key integration points for vulnerability management

INTEGRATION WITH FILE/SERVER INTEGRITY MONITORING (FIM)

Integrating your VM solution with your FIM solution can provide enhanced monitoring capabilities at the system level based on the vulnerability state of a system. Tripwire IP360 directly integrates with Tripwire Enterprise to enable that capability.

VM DEPLOYMENT WITH TRIPWIRE

As mentioned earlier Tripwire offers Tripwire IP360 as its VM solution. You can deploy a single or multiple scan engines around a network for communicating with your monitored devices. The data is then aggregated from the devices and delivered back to the central management system.

For large-scale deployments, Tripwire IP360 aggregates data into a higher-tier for consolidated reporting and management. Tripwire Security Intelligence Hub serves as the aggregated reporting system for IP360.

DETERMINING VM ASSET COVERAGE AND MONITORING

You'll typically deploy VM across your entire enterprise. You may have different policies in place as to the frequency, response, and workflow for dealing with vulnerabilities across different parts of the orga-

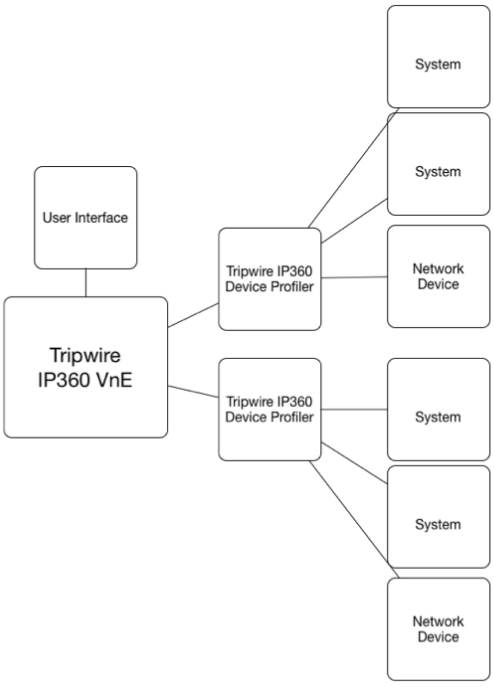

Diagram: Tripwire IP360 includes a VnE Manager and Tripwire IP360 Device Profilers

nization, but coverage of the complete set of assets is important for having a complete view of your risk.

Network topology is often the biggest driver in determining how to cover assets with your VM solution as well as how scanning will reach your target assets. Tripwire IP360 Device Profilers, deployed in physical or virtual instances, provide a flexible way of meeting an organization's infrastructure requirements.

Because scanning can generate significant network traffic, it is recommended that you deploy device profilers as close to the local networks of the devices being assessed as is practical. While some WAN-based scanning is acceptable, a whole architecture of remote scanning is likely to have a negative impact on the network and the performance of scans.

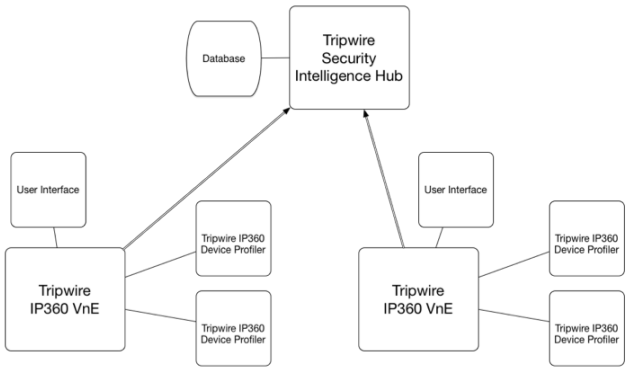

Diagram: Aggregated reporting, analytics, and visualization provided by an additional component allows for scalability and provides additional capabilities

EVALUATING EFFECTIVENESS

Identifying and tracking key performance indicators (KPIs) for your VM solution can help you evaluate your security program's effectiveness. In reviewing KPIs, don't lose sight of the key objectives of VM: first, to proactively prevent successful breaches by reducing the attack surface, and second, if applicable, to ensure compliance with regulatory standards. Make sure that the indicators you select do indeed reflect the effectiveness of your VM process in achieving those goals.

Tripwire has developed a set of commonly used metrics and criteria that may be used for evaluating your VM implementation. These should be thoughtfully considered and then tailored to meet your organization's specific business needs and structure:

- Average Asset Risk Score
- Average Days Since Last Scan
- Vulnerability Distribution by Severity
- Most Common Vulnerabilities
- High Severity Vulnerabilities
- Systems with Vulnerabilities
- Systems with Severe Vulnerabilities
- Scan Schedule Distribution
- Asset Coverage

When evaluating your implementation against these KPIs, also consider:

- Developing a reporting strategy for recurring scanning schedules that describes what items to scan and when
- Generating vulnerability aging reports to track remediation efforts
- Producing granular reports to track risks associated with individual system owners so that you can compare which owners are adhering to established standards and where improvements are needed
- Creating clean, simple trend analysis and executive reports that give senior level management a quick view of your organization's exposures and the risk management program's performance over time
- Automating reports to ensure they address all compliance and audit needs so that your analysts can focus on threat analysis rather than generating reports/metrics
- Producing reports with multiple views, including individual asset and application reports, that can roll up to create an organization risk framework

For each of KPI metric, evaluate the data across several categories or dimensions, including:

- Enterprise-wide
- By System Type
- By Business Function
- By Business Unit
- By Regulatory Scope

RELATIONSHIP OF VM TO THE C2M2 MATURITY MODEL

As emphasized in the introductory part of this guide, a security maturity model can guide your organization's security program as it advances to greater levels of security. Maturity models do this by explaining what your security program can achieve by implementing recommendations for a control, but also by describing what additional technologies, processes, or people your program must have in place to work its way up through the various maturity levels.

While you can use any maturity model to advance your program, this guide refers to the C2M2 security maturity model, shown below, and relates that to using Tripwire's VM solution, Tripwire IP360.

C2M2 DOMAINS RELEVANT TO VM

The C2M2 maturity model categorizes broad areas of security programs into domains. VM falls within the C2M2 Threat and Vulnerability Management domain.

Within the scope of the objectives and practices relevant to VM, implementing the Tripwire Reference Architecture for VM supports an organization at either MIL1, MIL2, or MIL3. To reach MIL3, you must have more detailed processes in place, a broader scope, and greater integration of VM in your organization's overall risk strategy. For more details, refer to section 5.4 of the C2M2 Security Maturity Model.

ADVANCING THROUGH THE MATURITY LEVELS

During the initial phase of deploying and operationalizing Tripwire IP360, most organizations tend to operate at MIL1. If you're operating at this maturity level, you're using these solutions to accomplish essential and necessary activities related to VM. These activities include deployment of Tripwire IP360 and ongoing assessments and monitoring. It also includes having procedures in place for reviewing vulnerabilities that Tripwire IP360 detects.

To move up to MIL2, you must mature your processes and practices around VM. Processes will be more formally documented and you will be incorporating more best practices used by other organizations in these areas, particularly around the use of automation. Although at MIL1, you may be performing the same practices around assessment and continuous monitoring and have some process documentation, as your program evolves to MIL2 and then on to MIL3, processes and practices should become more comprehensive and formalized.

Several organizations with Tripwire IP360 have evolved their implementation up to MIL3. The next section presents standard operating procedures (SOPs) based on these organizations that you can leverage as best practices to help your organization reach higher maturity levels.

SYSTEMS INVENTORY AND CATEGORIZATION

To build an effective risk management program, you must first determine what you are protecting. This applies to not only computing systems and storage networks but also to data types and attached third party systems. To do this, you must:

- Inventory all assets connected to your network because you can't manage what you don't know about
- Identify critical systems as well as at risk systems because these will require increased scan frequencies
- Review and classify all vulnerabilities and associated threats
- Establish a patch management process and Computer Emergency Response Team
- Establish remediation timelines (Normal 90 days, Medium 30 days, High Risk/Zero Day patch immediately)
- Rate risks according to your organization's stated risk categorization and assign a remediation timeline to each risk

STANDARD OPERATING PROCEDURES FOR VULNERABILITY MANAGEMENT

Tripwire offers a variety of documentation for SOPs for VM based on successful Tripwire IP360 implementations. These can be extremely useful in helping you build, maintain, and operate your Tripwire IP360 solution. Because SOPs are very specific to an organization both in the actual procedures developed, but also in how they're organized and presented, you'd be hard pressed to find a standard set of documentation that fully meets your organization's needs. However, the following documentation developed from Tripwire customers operating at MIL2 and MIL3 can provide a valuable starting point in developing a set of SOPs tailored for your organization. Alternatively, you can work with Tripwire consulting to develop these procedures.

1. Sample Operational Procedures from Tripwire Remote Operations. A sample set of procedures based on the experiences of Tripwire consultants managing Tripwire IP360 implementations on behalf of customers.

2. Sample Design and Implementation Guide for Tripwire IP360. Operational process documentation collaboratively developed by Tripwire Professional Services with a Tripwire customer that has mature processes in in place.

3. Standard Operating Procedures Outline. An outline of an SOP document from a Tripwire customer with a more mature, process-oriented security program and Tripwire IP360 implementation. This outline, shown below, provides a template that you can use to develop your organization's internal process documentation.

KEY TAKEAWAYS

From reading this guide, you've learned the value that VM provides your organization. You've also discovered how it relates to some of the most commonly used frameworks, and the two main use cases for VM—assessment and continuous monitoring. In addition, you've discovered the value of integrating VM with other security controls and systems to extend the value of your solution.

The guide then gets more specific, explaining not only how to deploy Tripwire's VM solution, Tripwire IP360, but also how it can help you advance your security program based on the C2M2 security maturity model. From a practical standpoint, the guide leaves you with three different documents for developing your own set of standard operating procedures for building, operating and maintaining your Tripwire VM implementation. Finally, it outlines additional valuable business services related to security that Tripwire IP360 solutions offer your organization beyond simply meeting the control objective of assessment and continuous monitoring for vulnerabilities.

In short, you have hopefully realized how much security benefit you can derive from a VM solution, particularly a solution based on Tripwire IP360.

REFERENCES

The Center For Internet Security. *CIS Controls for Effective Cyber Defense Version 6.0.*
https://www.cisecurity.org/critical-controls.cfm

Department of Energy. *Cybersecurity Capability Maturity Model Version 1.1.*
http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program/cybersecurity

ISACA. *Control Objectives for Information and Related Technology (COBIT).*
http://www.isaca.org/cobit/pages/default.aspx

Federal Financial Institutions Examination Council (FFIEC).
FFIEC Information Technology Examination Handbook (IT Handbook).
http://ithandbook.ffiec.gov/it-booklets/information-security.aspx

International Organization for Standardization. *ISO/IEC 27001 – Information security management.*
http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

Kim, G. (2005). *The Visible Ops Handbook: Implementing ITIL in 4 Practical and Auditable Steps.*
Eugene, OR: Information Technology Process Institute.

North America Electric Reliability Corporation (NERC). *NERC Critical Infrastructure Protection (CIP).*
http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

National Institute of Standards and Technology (NIST). *Framework for Improving Critical Infrastructure Cybersecurity.*
http://www.nist.gov/cyberframework/

National Institute of Standards and Technology (NIST). *Special Publication 800-53 Rev 4: Security and Privacy Controls for Federal Information Systems and Organizations.*
http://dx.doi.org/10.6028/NIST.SP.800-53r4

National Institute of Standards and Technology (NIST). *Special Publication 800-128: Guide for Security-Focused Configuration Management of Information Systems.*
http://csrc.nist.gov/publications/nistpubs/800-128/sp800-128.pdf

PCI Security Standards Council. *PCI DSS 3.2.*
https://www.pcisecuritystandards.org/security_standards/documents.php

Piper, S. (2013). *Security Configuration Management For Dummies, Tripwire Special Edition.* Hoboken, NJ:
John Wiley & Sons.

Tripwire. *Effective Security with a Continuous Approach to ISO 27001 Compliance.*
http://www.tripwire.com/register/effective-security-with-a-continuous-approach-to-iso-27001-compliance/

Tripwire. *Tripwire's Solutions for Automated, Continuous Compliance.*
http://www.tripwire.com/register/automated-continuous-pci-compliance-for-secure-cardholder-data/

Tripwire. *Meeting the True Intent of File Integrity Monitoring.*
http://www.tripwire.com/register/meeting-the-true-intent-of-file-integrity-monitoring/

Tripwire is a leading provider of security, compliance and IT operation solutions for enterprises, 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.

SECURITY NEWS, TRENDS AND INSIGHTS AT TRIPWIRE.COM/BLOG FOLLOW US @TRIPWIREINC ON TWITTER

BRRXTRA1a 201701