Continuous Cyber Situational Awareness

Continuous monitoring of security controls and comprehensive cyber situational awareness represent the building blocks of proactive network security.

A publication of Lumeta Corporation
www.lumeta.com

Table of Contents

Executive Summary

In today's environment, the ability to manage technology and ensure confidentiality, integrity, and the availability of information is mission-critical. Information security is a dynamic process that requires proactive management. Organizations need to identify and respond to new vulnerabilities, evolving cyber threats, and an enterprise that is in a constant state of change.

Cyber situational awareness answers the "who, what, when and how" of a cyber attack and is the foundation to any successful cyber security program. Organizations have the potential to predict and defeat a cyber attack only when a firm understanding of enterprise activity is in place. Cyber situational awareness includes recognizing emerging threats originating from within the organization and external to the enterprise, and requires a continuous monitoring approach to produce real-time visibility of an enterprise network and all of its connections and devices.

A comprehensive continuous monitoring program provides essential, near real-time security status-related information. It allows an organization to track the security state of a system on an ongoing basis and maintain the security authorization for the system over time. Understanding the security state of information systems is essential in highly dynamic environments with constantly changing technologies and with the proliferation of BYOD programs, cloud-based applications, virtualization and more.

Continuous monitoring of threats and the effectiveness of security controls is critical for managing risks to systems and data for government agencies and commercial enterprises. Many of today's organizations use a variety of threat and vulnerability monitoring "point products" that cannot provide complete visibility into the threat landscape. **The challenge is to develop a continuous cyber situational awareness program that combines relevant aspects of existing product investments, with new approaches to network visibility and data analytics, to achieve real-time, accurate, advanced threat detection and incident response.**

This paper provides an overview of the concept of continuous monitoring, describes how the technology can be effectively deployed, how automation is a critical aspect of both continuous monitoring and reporting, and summarizes the impact of the proliferation of BYOD programs, cloud-based applications and virtualization on an organization's security and risk postures. It also introduces Lumeta ESI (Enterprise Situational Intelligence), an industry-pioneering hybrid approach to continuous monitoring for cyber situational awareness of the network. ESI performs real-time network discovery, topology mapping, and leak discovery to give IT professionals comprehensive network visibility.

Introduction

Securing a large network requires an agile approach. Organizations have to contend with an ever-expanding infrastructure, an exponential increase in the number of connected devices, a distributed management environment and a changing threat landscape. Continuous monitoring of security controls and comprehensive cyber situational awareness represent the building blocks of proactive network security.

Cyber situational awareness involves the collection, correlation and normalization of information to produce a common operational picture of the network infrastructure, including:

- A comprehensive, broad visualization of the current IT infrastructure
- The ability to test the security controls protecting the IT environment
- Identification of critical and/or sensitive infrastructure components
- Detection of events or configurations linked to adversarial or anomalous conditions

Without a means to obtain comprehensive cyber situational awareness, security analysts largely rely on locally focused specialty products, such as intrusion detection systems (IDS), and manual data analysis from complex systems, such as network management suites, to gain a level of insight into the network infrastructure. Continuous network monitoring without visibility into the state of the network as a whole leaves inherent gaps in defenses.

Many organizations, especially within the U.S. federal government, have discovered that while traditional security monitoring systems can help information assurance efforts, they are rarely enough to react to today's external, targeted, persistent attacks. As a result, leading U.S. federal agencies and many private sector organizations are beginning to **replace point-in-time audits and compliance checks with a continuous monitoring program to help them prioritize controls and provide visibility into current threats**.

What is Continuous Monitoring?

The concept of monitoring information system security has long been recognized as a sound management practice. Organizations review their information systems' security controls to ensure that system changes do not have a significant negative impact on security, security plans remain effective after a change, and security controls continue to perform as intended.

Continuous monitoring goes further than a traditional periodic assessment or “snapshot” audit by continuously monitoring transactions and controls, so that weak, poorly designed, or poorly implemented controls can be corrected or replaced sooner rather than later, thus enhancing an organization’s risk profile.

The National Institute of Standards and Technology (NIST) has been the thought leader in the development of information security standards. The NIST Special Publication 800 series[1] of standards for cyber security have become **the de facto standard for securing network data systems in the United States and many other countries**. NIST first defined the concept of continuous monitoring of IT security in May 2004. For almost a decade, leading IT security regulators have been working with this key concept of managing and tracking the security state of information systems – moving away from point-in-time snapshot testing of security infrastructure effectiveness to continual analysis of the ability of security systems to protect critical assets and data.

NIST defines information security continuous monitoring as “maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions[2].”

Continuous monitoring of security controls allows organizations to detect threats and vulnerabilities from today’s sophisticated and persistent adversaries. It’s also instrumental in mitigating enterprise-wide risk through system-level network monitoring and detection. An effective continuous monitoring program should detect and alert information security professionals regarding network changes that require attention.

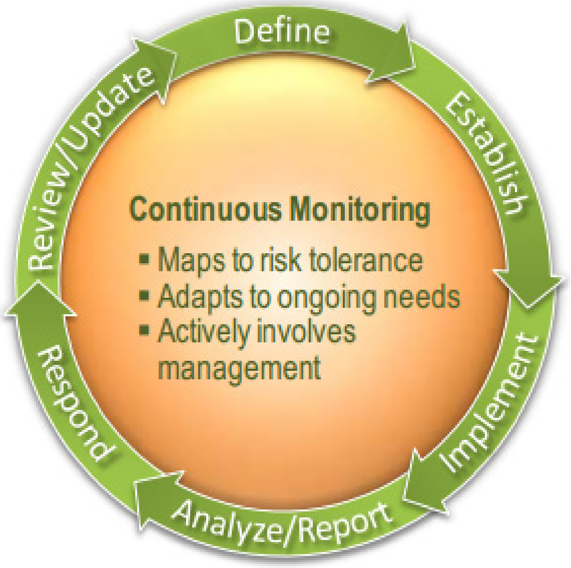


Figure 1: Information Security Continuous Monitoring Process – NIST Special Publication 800-137[3]

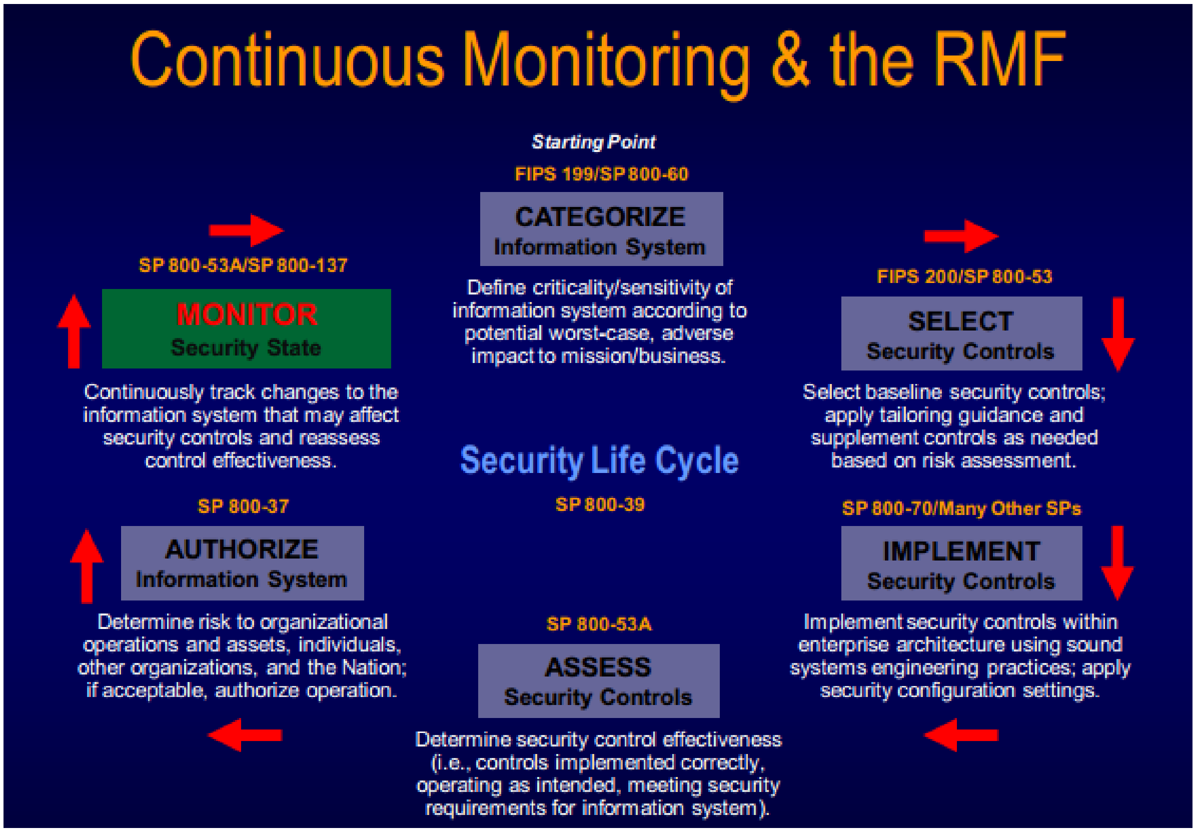
[1] http://csrc.nist.gov/publications/PubsSPs.html

[2] *NIST Special Publication 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, published September 2011*

[3] http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909726

Continuous monitoring enables information security professionals and others to quickly analyze a stream of real-time data regarding the state of risk to their security, the network, end points, and even cloud devices and applications. This allows IT security teams to plug obvious security gaps, eliminate known threats and vulnerabilities, deny unnecessary connections, keep security policies up to date, and more effectively enforce security policies.

NIST defines six components – the Risk Management Framework (RMF) – that work together to provide comprehensive guidance on how to implement continuous monitoring into the security lifecycle (illustrated in Figure 2). The RMF emphasizes the importance of near real-time risk management through strong and effective continuous monitoring processes. It also encourages the use of automation to give top-level management the critical information needed to make cost-effective, risk-based decisions that support their primary missions and business processes.



Continuous Monitoring & the RMF

Starting Point

FIPS 199/SP 800-60

CATEGORIZE
Information System

Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.

FIPS 200/SP 800-53

SELECT
Security Controls

Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.

SP 800-70/Many Other SPs

IMPLEMENT
Security Controls

Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.

SP 800-53A

ASSESS
Security Controls

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

SP 800-37

AUTHORIZE
Information System

Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

SP 800-53A/SP 800-137

MONITOR
Security State

Continuously track changes to the information system that may affect security controls and reassess control effectiveness.

Security Life Cycle

SP 800-39

Figure 2: Continuous Monitoring and the Risk Management Framework proposed at NIST[4]

The purpose of a continuous monitoring program is to provide awareness of threats and vulnerabilities, visibility into organizational assets, detection of anomalies or changes in the organization’s operation and information systems, and the effectiveness of deployed security controls. An effective continuous monitoring program provides ongoing assurance that planned or implemented security controls align with organizational risk tolerance and supplies the information needed to respond to risk in a timely manner.

[4] *http://csrc.nist.gov/groups/SMA/forum/documents/Forum-121410-Continuous-Monitoring-AJohnson.pdf*

While each organization's requirements are different, continuous monitoring should include the following types of monitoring and correlation capabilities:

- Vulnerability, configuration and asset management
- System and network log collection, correlation and reporting
- Advanced network monitoring using real-time network forensics
- Threat intelligence and business analytics that fuse data from all monitoring feeds for correlation and analysis

> *"Continuous monitoring is a proven technique to address the security impacts on an information system resulting from changes to the hardware, software, firmware, or operational environment. A well designed and well-managed continuous monitoring program can effectively transform an otherwise static security control assessment and risk determination process into a dynamic process that provides essential, near real-time security status-related information to organizational officials in order to take appropriate risk mitigation actions and make cost-effective, risk-based decisions regarding the operation of the information system."*
>
> - NIST Special Publication 800-37, Rev 1, Guide for Applying the Risk Management Framework to Federal Information Systems, published February 22, 2010

A key component of continuous monitoring is real-time notification of events outside of security policies that trigger the immediate need to assess security controls or verify security status. Security-related data resulting from continuous monitoring is analyzed in the context of stated risk tolerances, the potential impact that vulnerabilities may have on information systems, business processes, and the organization as a whole, and the potential impact of mitigation options. The end result is improved organization-wide risk management and continual improvement from collecting information and responding to findings.

Protective Monitoring, also known as Good Practice Guide 13 (GPG13), is a UK government[5] recommended set of processes and technology to improve risk profiles – essentially, providing visibility and an understanding of who is accessing a company's or public sector organization's sensitive data. The GPG13 was developed in an effort to better protect systems from internal and external threats through monitoring practically every component within an organization's IT infrastructure. Many of the concepts regarding Continuous Monitoring can also be applied to the Protective Monitoring guidelines, and will help organizations gain situational awareness of risk events.

[5] *CESG (Communications-Electronics Security Group), the United Kingdom's National Technical Authority for Information Assurance (IA).*

The need, the benefits, and who should adopt Continuous Monitoring

In the public sector, OMB and NIST mandates and standards require continuous monitoring. In the commercial sector, Payment Card Industry (PCI) standards, data breach laws, and regulations like Sarbanes-Oxley have requirements for continuous or regular monitoring of security controls. Although details of the mandates and regulations differ, they share common policy requirements pertaining to the need to continuously monitor that security controls are operating as expected and that boundaries around sensitive network data are secured.

Industry and government compliance mandates go a long way to address the issues of maintaining a secure IT infrastructure, as well as policies and procedures to guard against security breaches and access to sensitive data. To be compliant, an organization needs to undergo an audit to ensure that its IT security controls are functioning appropriately and that proper policies and procedures are in place. Historically, IT audits have been snapshots that rarely reflect the true operational security posture of the network.

Change is constant in a large complex network. And companies and agencies can quickly fall out of compliance, becoming more open to the risk of having their network and data assets compromised. A continuous program is needed to monitor transactions and controls ensuring that compliance is effective on an on-going basis.

There is an overall need for proactive, comprehensive security practices amongst organizations of all types. Every organization can benefit from monitoring its security controls on an on-going basis, resulting in up-to-date security and compliance status on IT infrastructure and critical assets in the form of real-time reporting that can be used to make immediate, cost-effective decisions that mitigate IT risk in information systems.

- Government Agencies: The information and systems agencies need to protect are critical to the nation and national security. FISMA regulations now mandate continuous monitoring of security controls.
- Critical Infrastructure Providers: The protection of electric grids, mass transportation, and facilities that manage the nation’s water supply and other industrial systems deserves serious attention on a continuous basis.
- Financial Services: Ensuring the integrity of financial transactions to guard against fraud, error and misuse is a daily essential.

- Other Commercial Enterprises: Vertical industry compliance mandates more frequent ongoing testing of security systems and policies to replace traditional once a year "snapshot" assessments. FISMA standards are expected to become mandatory for any commercial enterprise that works directly with the government.

Depending on the value of the data an organization is trying to protect and the mandates associated with the protection of that data, companies may not be required to implement a continuous monitoring program. However, the savings in expenditures, resources, and continued compliance may outweigh the costs of a once a year audit and the consequences associated with a security breach.

Business is continuous. Security should be as well.

The benefits of continuous monitoring are not simply to comply with monitoring mandates. By using a continuous monitoring program, organizations can improve the quality and timeliness of decision-making as network security is aligned to key business objectives and managed holistically. Continuous monitoring allows organizations to manage IT assets in a proactive manner, and identify risks and gaps in security posture, so that IT professionals can react, recover and maintain key business operations. Overall, organizations will gain:

- Tighter risk control
- Better network assurance
- An effective security posture
- Reduced operations and compliance costs

Virtualization / Cloud

Virtualization and continuous monitoring

Virtualization introduces an additional level of complexity in managing system risk. Virtualization technologies connect to network infrastructure and storage networks and require careful planning with regard to access controls, user permissions, and traditional management and security controls. Organizations should consider the gaps in network visibility that virtualization introduces. IT professionals should review their security architecture, policies and processes in order to implement strategies that bridge these gaps.

Moving to the cloud and a continuous monitoring strategy

Moving to the cloud transfers responsibility for a system, however organizations cannot transfer accountability. When moving to the cloud, an organization must understand the security posture of this new environment. The organization has to understand how the cloud service provider (CSP) performs continuous monitoring, what the monitoring looks at and who has access to the data the monitoring produces. Organizations also have to make sure that the contract with the CSP adequately addresses the level of assurance the organization requires and that it understands the risk to the organization's data.

If an organization puts a system in the cloud, the security requirements of that system have not changed. However, the organization no longer has complete control over the system once it's in the cloud. Organizations have to reassess their security controls with respect to the Service Level Agreement (SLA) with the cloud provider.

Guidance from the Cloud Security Alliance (CSA) calls for a concerted continuous monitoring effort of a CSP's environment, operations, and governance-related activities, such as updating information security. The CSA advises implementing a systematic vulnerability scanning and mitigation program for CSP systems and networks, and continuously monitoring for data protection and unauthorized activities in the cloud. For organizations using a public CSP, it is the CSP's responsibility to monitor its own log data (e.g., host audit logs, firewall logs). Understanding the CSP's policies and establish alerting criteria and procedures is critical.

With the predicted growth in cloud adoptions over the next few years, it is important to develop a continuous monitoring program with the cloud in mind. In the U.S. federal government, continuous monitoring requirements are the same for federal agencies and any external service providers (e.g., cloud service providers) used by the agencies. To receive reauthorization of a Federal Risk and Authorization Management Program (FedRAMP) security authorization from year to year, CSPs must monitor their security controls, assess them on a regular basis, and demonstrate that the security posture of their service offering is continuously acceptable.

Implementation Guidelines

Continuous monitoring is a critical activity and is most effective when implemented as part of a comprehensive enterprise-wide risk management approach. It is one of many approaches in an organization's arsenal that can be employed to strengthen the defenses of the information systems supporting core missions and business processes.

Step 1 – Understand the Enterprise

The weakest security control is a clear understanding of the enterprise. Consequently, the first step of continuous monitoring is to gain a thorough understanding of what makes up the enterprise. This includes connected devices, network infrastructure, virtualized assets, cloud connectivity, partner and gateway connectivity, and network perimeter boundaries. Without a clear understanding of the components that make up the enterprise, a continuous monitoring program will struggle to be successful.

The SANS Institute defines practical suggestions for implementing a process of continuous monitoring and other top defenses for protecting technology systems. These recommendations have been released in the form of the Consensus Audit Guidelines (CAG), published under the title: Twenty Critical Security Controls for Effective Cyber Defense.[6] *Control 1, for example, defines the need for an inventory of authorized and unauthorized devices as a first step in preventing attackers from exploiting new and unprotected systems attached to the network.*

Step 2 – Design for Automation in Continuous Monitoring

A continuous monitoring program applies automation to the assessment of defenses, with a clear focus on proactive risk management, ahead of any attacks. Through the use of automation, IT professionals can:

- Monitor a greater number of security controls on an ongoing basis and with increased frequency
- Ensure that they have not been negatively impacted by changes to the infrastructure
- Provide senior management with an essential, up-to-date security status
- Allow for immediate, cost-effective, risk-based decisions about their information systems

Automated processes, including the use of automated support products (e.g., vulnerability scanners, network scanning devices), can make the process of continuous monitoring more cost-effective, consistent, and efficient. Real-time monitoring of controls using automation can provide an organization with a much more dynamic view of its security state.

Automated products recognize patterns and relationships, such as:

- Verifying technical settings on individual network endpoints
- Ensuring that the software on a machine conforms to organizational policy
- Addressing advanced persistent threat (APT)

[6] www.sans.org/critical-security-controls

Automation serves to augment the security processes conducted by security professionals within an organization and reduces the amount of time a security professional spends on redundant tasks. In addition, automation supports collecting more data, more quickly and can therefore make comprehensive, ongoing control of information security practical and affordable.

Step 3 – Identify Technologies for Enabling Continuous Monitoring

There are a variety of technologies available that an organization can use to efficiently and effectively gather, aggregate, analyze and report data. These range from the security status of its enterprise architecture and operating environment down to components of individual information systems. These technologies (e.g., asset discovery and management, network discovery, vulnerability management, security information event management (SIEM), IDS/IPS) collect, analyze, and meaningfully represent data in support of continuous monitoring of an organization's security posture. They provide visibility into the information assets, awareness of threats and vulnerabilities, and status of security control effectiveness. Continuous monitoring supports a variety of organizational processes, including but not limited to:

- Ongoing assessments of security control effectiveness
- Reporting of security status at the appropriate level of granularity to personnel with security responsibilities
- Management of risk and verification and assessment of mitigation activities
- Assurance of compliance with high-level internal and external requirements
- Analysis of the security impact of changes to the operational environment

Technical Considerations for Continuous Monitoring

There are three approaches to continuous network monitoring techniques: active, passive, and hybrid active/passive.

Active continuous network monitoring techniques function independently of other network management and security assessment products. They probe for information about the network topology, connected hosts, devices and services. Active monitoring techniques are generally accepted as more comprehensive (a greater reach to the endpoints), while generally lacking in detail.

Passive continuous network monitoring techniques are highly effective at real-time detection and at gathering deep levels of host information. The majority of passive monitoring techniques rely on devices to participate within traffic flow on the network, which allows them to sense the traffic a device emits before they can begin to gather data about those devices. While these techniques have the real-time and deep-dive advantages, it is generally accepted that passive monitoring techniques provide less visibility.

Cyber situational awareness requires a hybrid active/passive continuous monitoring approach to produce real-time visibility. Hybrid active/passive continuous monitoring methodologies allow for a real-time discovery of the infrastructure across the entire network. This real-time network visibility offered through passive techniques is continuously tuned by what the active component probes on the network, ensuring that the deep dark corners of the network do not go unexplored.

Lumeta ESI and Continuous Monitoring

Lumeta ESI (Enterprise Situational Intelligence) builds on the widely adopted active network discovery foundation pioneered by Lumeta with its IPsonar product, taking the bounds of network visibility and monitoring into an entirely new stage of advancement. Lumeta ESI is a hybrid active/passive, deeply entrenched operational system, which takes situational awareness of the network to a new level. ESI offers an industry pioneering hybrid approach to active/passive continuous, always-on monitoring. This hybrid active/passive discovery offers comprehensive network visibility coupled with real-time, instant discovery of the dynamic enterprise.

Hybrid Active/Passive

ESI includes a passive monitoring, sensing and analysis technology that participates in the network. It utilizes non-disruptive network discovery to obtain real-time information on routing changes across large-scale networks. Continuous monitoring provides a clear picture of the network security state at any given time, while providing a mirror of control effectiveness over time. ESI maintains historical, passively collected network intelligence, and uniquely analyzes this information against network norms and policies. Components requiring additional analysis are probed through a hybrid active network discovery engine for further assessment of devices participating in routing changes.

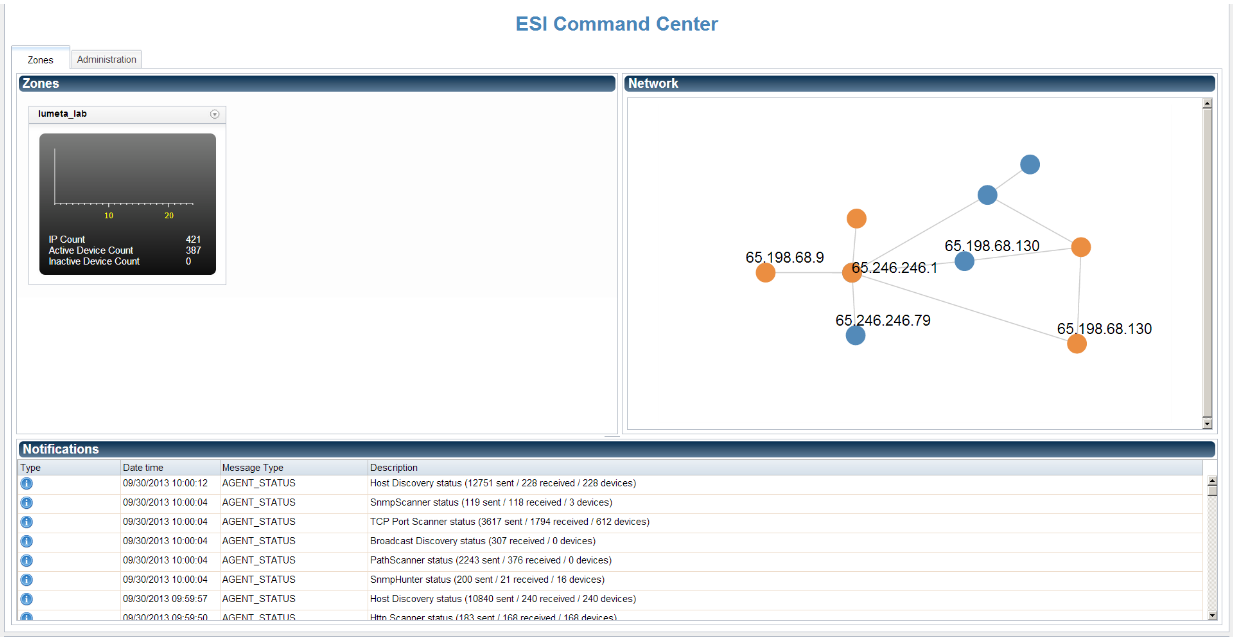
Effective cyber situational awareness requires broad coverage to gather and correlate the high volume of data about the network itself, its routers and routes, as well as device profiles. ESI’s Scouts facilitate accurate and complete depth-of scanning on complex, distributed global networks. ESI provides the flexibility to address network discovery, topology mapping, and network leak discovery in real-time even as networks change and new connections or devices are added. Particularly in this age of BYOD, detecting new devices on the network and changes to the network topology as they happen allows for proactive defense and intrusion detection.

Zones

ESI allows for the creation of zones to allow an organization to segment continuous compliance monitoring of network access controls for compliance with regulatory and internal information security policies. Zones can be as simple or as complex as defined by an organization and can be comprised of logical networks and subnets, regardless of where they are physically deployed around the world.

Analytics & Visualization

A security management dashboard consolidates and communicates relevant security status in real-time, translating raw technology feeds into actionable information and alerts for events that require immediate action. The dashboard presents information in a meaningful and easily understandable format that can be customized to provide the appropriate information to users with specific roles and responsibilities within the organization.



IP Count	421
Active Device Count	387
Inactive Device Count	0

Type	Date time	Message Type	Description
ⓘ	09/30/2013 10:00:12	AGENT_STATUS	Host Discovery status (12751 sent / 228 received / 228 devices)
ⓘ	09/30/2013 10:00:04	AGENT_STATUS	SnmpScanner status (119 sent / 118 received / 3 devices)
ⓘ	09/30/2013 10:00:04	AGENT_STATUS	TCP Port Scanner status (3617 sent / 1794 received / 612 devices)
ⓘ	09/30/2013 10:00:04	AGENT_STATUS	Broadcast Discovery status (307 received / 0 devices)
ⓘ	09/30/2013 10:00:04	AGENT_STATUS	PathScanner status (2243 sent / 376 received / 0 devices)
ⓘ	09/30/2013 10:00:04	AGENT_STATUS	SnmpHunter status (200 sent / 21 received / 16 devices)
ⓘ	09/30/2013 09:59:57	AGENT_STATUS	Host Discovery status (10840 sent / 240 received / 240 devices)
ⓘ	09/30/2013 09:59:50	AGENT_STATUS	Http Scanner status (183 sent / 168 received / 168 devices)

Figure 3: ESI continuously monitors network connections and devices. Data is displayed on a single executive dashboard. ESI provides the real-time visibility and flow analysis required to fully understand and respond to changes taking place in the network.

Situational Awareness through Integration

There is no one “magic bullet” to stop cyber threats. The need to continually understand the complete enterprise is critical. Otherwise, situational awareness is limited. It is crucial to understand the comprehensive dynamic state of the network. This information is foundational intelligence for an effective continuous monitoring program.

Through integration, this foundational intelligence can be provided to technologies including:

- Security Incident and Event Management (SIEM)
- Vulnerability Management
- IDS/IPS
- NAC
- Flow data analysis tools
- Network metadata, packet capture and analysis tools
- Network forensics

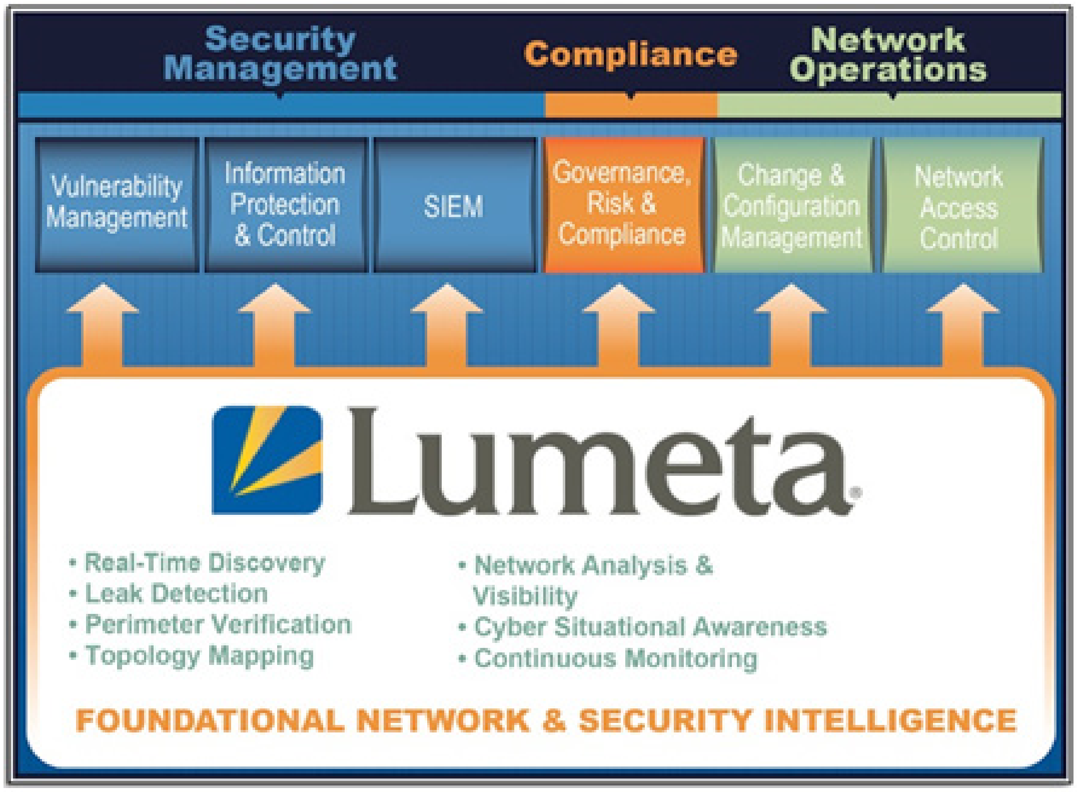


Figure 4: ESI is a necessary foundation for continuous monitoring and comprehensive cyber situational awareness. It integrates with an organization's existing products, such as VM, SIEM and NAC. Network, security and compliance products can only be fully effective when operating with 100% network visibility.

Continuous monitoring using ESI provides a complete view of network assets and connections to monitor network availability and assess business impact due to network changes. ESI is an effective means for both data capture and data analysis to support real-time, risk-based decision making.

Conclusion

In today's environment of widespread cyber-intrusions, advanced persistent threats and insider threats, it is essential for government agencies and commercial enterprises to have real-time accurate intelligence of their enterprise security posture. This allows for a swift response to external and internal threats. **Sophisticated attackers continue to exploit the weakest controls**. Enterprises need to conduct continuous monitoring and be able to determine the security posture of systems and the organization at any given moment.

The ongoing support of business functions requires organizations to constantly alter their network security environments and device settings, creating the potential for new points of risk. As a result, it's crucial for organizations to maintain constant visibility into their security standing to verify that they haven't opened a back door, which could allow attackers to access protected mission-critical information or systems.

Continuous monitoring is a risk management approach to cyber situational awareness that maintains a picture of an organization's security risk posture and provides visibility into assets, which is critical for organizations with a BYOD policy. Automated data feeds allow IT professionals to quickly quantify risk, ensure effectiveness of security controls and implement prioritized remedies.

Organizations of all sizes should consider a comprehensive continuous monitoring strategy to decrease risk. A continuous monitoring program helps to ensure that deployed security controls continue to be effective and operations remain within stated organizational risk tolerances, in light of the inevitable changes that occur over time. In cases where security controls are determined to be inadequate, continuous monitoring programs facilitate security response actions based on risk.

Continuous monitoring supports compliance audits by providing deeper information that can be analyzed over time. The trending information becomes more important for compliance and for overall improvements in operations, security and risk posture. Automation of these tasks decreases the time spent on reporting and reduces the number of errors.

Continuous monitoring is most effective when automation techniques are employed for data collection and reporting. By implementing technologies that automate many of the continuous monitoring activities, organizations can make more effective use of their security budgets. Effectiveness is greatly enhanced when these technologies are working with complete network visibility.

Lumeta ESI provides a clear foundational intelligence of the enterprise to power continuous cyber situational awareness.