A Real-Time Approach to Continuous Monitoring

Copyright SANS Institute
Author Retains Full Rights
Continuous Monitoring Defined

The Phases of Monitoring

Components of Continuous Monitoring

Real-Time Information Fusion: A Case Study

Advisor: David Rice, Director of the Monterey Group
Introduction

Many organizations, especially within the U.S. federal government and defense industry base, 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, zero-day attacks. As a result, leading U.S. federal agencies and some 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.

There is much debate over the definition of continuous monitoring. In December 2010, the National Institute for Standards in Technology (NIST) produced a draft publication to help the IT security community understand what is involved in a continuous monitoring effort. While many believe it to mean continuous monitoring for system vulnerabilities, others consider it to mean much more. For example, NIST, in its latest documentation, defines continuous monitoring as including vulnerability monitoring, application monitoring and threat monitoring.¹

As an extension of the documentation produced by NIST, the Center for Strategic and International Studies (CSIS)² and the SANS Institute have collaborated with more than 200 U.S. government agencies and information assurance professionals to define 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.³ Control 6, for example, defines the need for continuous monitoring of audit logs and improved analysis of log data for better response and network improvement. Other controls call not only for assessment, inventory and monitoring for secure configuration, but also real-time monitoring of account activity, sensitive data movement, malware and threats.

Today’s enterprises use a variety of legacy threat and vulnerability monitoring tools that are not providing adequate visibility into the current threat landscape. The challenge is to develop a comprehensive network-wide monitoring program that incorporates the best aspects of existing systems investments with new approaches to network visibility and data analysis to achieve real-time, accurate, advanced threat detection and incident response. This paper identifies the components of a comprehensive continuous monitoring program and how organizations can use this approach to decrease risk and improve efficiency.

² http://csis.org
³ www.sans.org/critical-security-controls
Continuous Monitoring Defined

One of the first major challenges in developing a strategy for implementing a continuous monitoring effort is defining the term. To date, NIST has produced two documents that seek to define and provide guidance on the subject of continuous monitoring. The first of these documents is a Frequently Asked Questions (FAQ) guide on continuous monitoring that was published in June 2010.4 The second of these guides is the draft publication for Special Publication 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organization, released in December 2010. This second document expands the role of continuous monitoring to include threat analysis and risk management support as well as vulnerability monitoring. In this latter document, NIST defines continuous monitoring:

“Information security continuous monitoring is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. The objective is to conduct ongoing monitoring of the security of an organization’s networks, information, and systems, and respond by accepting, avoiding/rejecting, transferring/sharing, or mitigating risk as situations change.” (NIST Special Publication 800-137 Draft December 2010)

While these monitoring recommendations may seem to call for a confusing array of monitoring components to merge and manage, the recommendations are easier to understand when we break continuous monitoring into two primary categories:

- **Proactive**: Vulnerability monitoring and asset/device awareness
- **Detective**: Full-view, context-aware threat monitoring, analysis and alerting

Proactive technologies are aware of device and security state (through configuration and patch management, application monitoring, endpoint security monitoring, and so on). Such technologies are available to help organizations know everything happening across the network—not just traffic pattern and type, but complete, port-agnostic awareness of content and context of all network data.

To create situational awareness and achieve successful continuous monitoring of networks, proactive and detective monitoring actions must work together and be visible to top-level analytics. For example, an organization using proactive monitoring for devices, system state, and vulnerabilities may provide a level of foreknowledge of whether a known or emerging threat applies to its IT assets. The detective threat-monitoring system should be able to reference these data when analyzing threat information. To combat advanced problems, such as zero-day malware, command and control traffic, and sensitive data exfiltration, continuous monitoring systems must accurately analyze all network traffic, fuse external threat intelligence, and gather log data from applications, network data and security systems in real-time. This capability includes the requirement for visibility into threats and encrypted malicious traffic hiding in approved traffic types and using approved ports and services.

---

Continuous monitoring and real-time analysis are not new concepts. However, they are both still evolving, and so organizations today find themselves at varying levels of understanding and deployment. Essentially, however, continuous monitoring breaks down into three phases, described in more detail in the following sections.

**Phase I: Limited Real-Time Data**

In most organizations, Phase I monitoring is already in place. This includes firewalls, intrusion detection/prevention (IDS/IPS) and log collection systems—the latter of which are used among 89 percent of respondents to the SANS Sixth Annual Log Management Survey.\(^5\) By continuously analyzing the data feeds produced by these systems, information assurance professionals can gather actionable information to respond to threats. However, experience suggests that without proper automation, organizations only monitor their logs on an ad hoc basis, which limits the ability to respond to attacks in real time. And, because they rely on known signatures and behaviors for their detection, IDS/IPS tools, while continuously monitoring for threats, miss many of today’s zero-day attacks. Furthermore, first-phase IDS/IPS and firewall monitoring does not capture exfiltration of sensitive data and commands in outbound traffic.

For example, applications and devices can be continuously monitored for access violations, for variances from secure state, and for signs of misuse using any number of commercial monitoring tools available today. Some of these tools monitor database applications, whereas others monitor desktop and e-mail applications. Still others monitor operating systems and the security state of servers, network devices and end points. Typically, in Phase I organizations, the deployment of these technologies is incomplete, and aggregation of monitoring data is not performed.

**Phase II: More Real-Time Data**

Finding evidence of threats not seen before requires a complete, real-time picture of what’s happening on the network while an incident is occurring—beyond just alert data appearing after the fact. Phase II of real-time monitoring includes more advanced forms of threat monitoring, including pervasive network recording, better visibility into network traffic, and deeper understanding of application state to monitor and report on deviant application and network behavior.

Threat analytics are available today that go beyond behavior- and signature-based monitoring. To be most useful, these analytics need to enable standard business processes using HTTP, social networking and other types of traffic that are allowed by policy. At the same time, these tools need to constantly analyze for malicious code and suspicious activity within those approved pathways and services that Phase I monitoring systems can’t detect.

\(^5\) [www.sans.org/reading_room/analysts_program/logmgtsurvey-2010.pdf](www.sans.org/reading_room/analysts_program/logmgtsurvey-2010.pdf)
For example, recording all network traffic would help organizations determine more than the time and location of an event, which are available with traditional packet header reading technology in Phase I network monitoring. Pervasive real-time network forensics-based approaches permit organizations to see the precise details of an event all the way down to complete session information, when required. With this complete content and context data available to them, organizations can analyze malicious attacks in detail, and incident handlers can obtain clear details on attack methodologies. Having this complete level of network visibility, including full knowledge of unknown executables and binaries crossing a network, provides even more actionable threat intelligence that can be used to stop attacks and protect against them happening again in the future.

Next generation continuous monitoring also needs to have broad visibility into the behavior of traffic that is allowed on the network: Is it making calls to another server it shouldn’t be? Is it opening connections with an internal IP address it normally doesn’t connect to? Is it sending communications, commands and data outside the company? Is it connecting to unauthorized services? What systems are compromised? To answer these questions requires deep threat analysis combined with situational awareness gathered from applications, end points, and vulnerability monitoring.

Phase III: Real-Time Analysis

Organizations in this most advanced level of maturity and deployment have a wide variety of custom and commercial monitoring tools at their disposal to handle the individual components of continuous monitoring. The question is: How are they putting all these components together for enterprise-wide visibility of the network and activity across the network?

Phase III organizations are purchasing advanced intrusion prevention, next generation firewalls, advanced log management systems with correlation capabilities, real-time enterprise network forensics, SIEM (Security Information Event Management), and other tools to consolidate feeds into their monitoring dashboards and alerting systems. In some cases, the SIEM or log management program is able to provide high-level threat context by pulling data from asset databases, document classification systems or financial systems. Organizations are also combining monitoring capabilities on their own, through use of commercial, open source and home-developed programs.
One of the more promising examples of an organization producing its own consolidation and analytics system is the U.S. Department of State and its iPost system. In the iPost system, the Department of State measures risk levels in real time by consolidating feeds from multiple sources, such as Microsoft Active Directory and SMS, along with data from a commercial vulnerability analysis tool. By consolidating information in a continuous monitoring dashboard (Figure 1), engineers and managers are able to identify portions of the organization that have higher levels of risk and respond to threats against these areas appropriately.

![Sample iPost Consolidated Risk Dashboard](image)

All of these continuous monitoring efforts result in better situational awareness of systems, users and activity—as well as awareness of the attacks being attempted on the networks despite their best proactive efforts.
Components of Continuous Monitoring

While each organization's requirements are different, continuous monitoring should include the following types of both legacy and leading-edge 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

These monitoring categories are discussed in more detail in the following sections.

Vulnerability, Configuration and Asset Management

Organizations need clear visibility into data regarding vulnerabilities, device behavior, system configuration and patch levels, and overall security state. Vulnerability and security state information for these systems must also be monitored and correlated to demonstrate security compliance when required.

In addition to providing definitions, NIST has also provided the Security Content Automation Protocol (SCAP), which can assist organizations in correlating the vulnerability and configuration information collected from monitored systems. In this document, NIST defines six components that work together to provide comprehensive guidance on how to implement continuous monitoring into the security lifecycle. Those steps include:

1. Categorize information systems.
2. Select security controls.
3. Implement security controls.
4. Assess security controls.
5. Authorize information systems.

These steps are illustrated in Figure 2.
Logging

Log capture is the typical starting point for many legacy continuous monitoring efforts. Almost all systems today produce logs in some format or another. An effective approach to continuous monitoring must include the ability to collect, consolidate and index logs from diverse systems and applications, and then correlate those logs into a central database so the data can be analyzed in real-time for analysis and alerting.

Effective continuous monitoring requires the ability to collect system events as well. If a system reboots, a new process is spawned, a new user account is created or added to a group, or files on a file system are changed—these and other anomalous events need to be reported to an analytics engine that can correlate this network event data. Traditional syslog engines, Windows event logs, file integrity assessment tools, anti-malware systems, and similar technologies fit into this category. According to the SANS Annual Log Management Survey, log systems are adapting to these and other security and business challenges.

On the proactive side, data should also be correlated over time in support of organizational metrics and risk tolerance. Continuous monitoring data can be correlated to provide root cause analysis, which can be used to identify new risks and enable ongoing improvements to organizational risk management.

Advanced Network Monitoring

Today, most organizations rely upon legacy security tools that are perimeter-oriented and signature-based. Unfortunately, these tools fail to identify critical threats from insiders, cyber criminals, and nation-state adversaries who utilize targeted and zero-day malware, advanced persistent threats (APTs), application layer attacks, and sophisticated data leakage techniques.

Knowing everything about what is happening on the network allows an analytics engine or incident responder to react to unknown, zero-day threats potentially hidden in network traffic. For example, it is useful to track port 443 traffic on the network, but it would be much more useful to understand how much of this traffic is not SSL, or is not encrypted, or has other layer 2 through 7 threat characteristics that could be signs of malware, sensitive data leakage, or command and control data. The more information incident responders have, the better they are able to efficiently respond to the events as they are discovered.

Analysis and Reports

Once the different forms of real-time data have been collected, the process of analysis begins. For continuous monitoring to be successful, the correlation engine must have the ability to translate raw technology feeds into actionable information used to make business decisions about risks to revenue, services and reputation. For example, let’s say an exploit is discovered on two network segments and that the exploit takes advantage of a flaw in Oracle’s Java Virtual Machine. If one of those network segments has multiple systems in it that are vulnerable to the exploit and the other network segment has no systems vulnerable to the exploit, then clearly the organization’s response must be to defend the network segment most vulnerable to this assault.

In addition, the analytics engine must be able to fuse threat intelligence into its analysis. Analytics engines for continuous monitoring must be extensible enough to allow organizations to teach the system what to look out for and where to look. The end goal is that business analytics, including correlation, visualization and reporting, are capabilities of the continuous monitoring analytics engine.
As reports come in from different monitoring devices, how are these data used for real-time analysis and decision-making? Most organizations, currently between Phase I and II, will need to integrate their multiple monitoring operations and graduate to Phase III. The technology exists today that will allow this functionality. It's a matter of implementing and coordinating the information from all relevant feeds that will produce accurate analytical information on advanced threats, malware, insider threats and data leakage in an ever-advancing threat landscape.

The following case study, although hypothetical, outlines how applicable monitoring data could be extracted and correlated from multiple monitoring systems for use in real-time analysis by using tools available today.

ACME Corp. is a Phase III organization that has integrated its security systems for continuous monitoring. The security and operations teams have identified each of the proactive and detective security data sets that are of value to their monitoring efforts.

The most time-consuming piece in developing this integrated network-monitoring architecture was the business logic. The vendor they chose for their data modeling, analytics and visualization platform assisted in the integration and business logic development. However, ACME IT staff still needed to customize these standard alerts and risk priorities based on their unique business needs. To do this, system engineers worked with business units in identifying systems, understanding their specific use purpose, and baselining their traffic to understand a definition of “known good.”

Rather than have each of their reporting systems work as individual silos, they integrated all systems, including reporting systems, through their log management platform for normalization and correlation. They then integrated the result into their situational awareness dashboard for full analysis and reporting. Using some self-developed policies and heavily leveraging policies available within their commercial monitoring and management systems, they integrated real-time alerts from the individual monitoring system consoles and platforms. The system's business logic was also developed to allow for upgrades in policy when required. The organization chose to implement pervasive network recording and real-time network forensics.
Before this integration, ACME’s helpdesk was responsible for escalating alerts originating from each individual security appliance. Now most of that is automated. After the integration, instead of coming into work each day and analyzing dozens of consoles (which they never really had time to do), ACME’s administration and security team members log in to perform their specified tasks through one integrated console.

A most pressing concern for the day appears to be an intelligence report about a new vulnerability that was recently discovered in Adobe's PDF Reader software in which obfuscated executables could be hidden in PDFs, leading to second and third stage malware infections.

An alert surfaced from their next-generation network monitoring tool that several PDFs had indeed crossed the wire with the following characteristics: embedded JavaScript, downloaded via HTTP over port 80 from a site in a country on the watch list, originating from a site with a known ZeuS association. Clearly there are numerous issues, but how can ACME’s team be sure of the company’s security status?

A quick search using the data visualization tool validated that other data sources in the enterprise had visibility into various components of this potential incident, including the source and target IP, actual filename, and the external source domain of the attack. The security team then used both the interactive forensics capability of the tools and the all-data search capability to drill down into the details about the host to learn more about the system. The analyst opened the asset inventory menu of his security operations dashboard to discover that, indeed, Adobe software is installed on the system, but that it is a later version of the software that is not vulnerable to this particular attack.

No need to wake up the Chief Information Security Officer (CISO) for this event. However, ACME does need to block the IP address of the originating mail host and the dynamic DNS of the ZeuS host. Security team members also need to investigate for secondary damages, data losses and infection using the proactive and protective data available to them to determine where to improve their security policies and monitoring efforts.

This is the vision of continuous monitoring—and it is already being implemented by leading enterprises in the government and commercial sectors where CISOs and their teams are reducing risk and the cost of their security operations while giving full visibility into their networks and systems.
The process of using IT security expertise to manually analyze unstructured data sets from different security systems, applications and network traffic sets is costly, inefficient and error-prone. Network monitoring must evolve in many organizations if the organizations are to be successful in combating today’s threats.

To achieve continuous monitoring, organizations should:

1. **Collect and analyze all network traffic in real time.** Log files and signature-based analysis are ineffective against advanced and zero-day malware, data leakage, insider threats and APTs. Organizations must implement pervasive network monitoring based upon knowing everything about the network and being able to answer any question about network activity and data flow to the most precise detail. This capability requires more than simple packet capture; it requires an architecture that supports real-time network forensics, data fusion and agility.

2. **Centralize legacy log and statistics-based data sets.** Determine all of the data feeds that will eventually be consolidated and start collecting the data. Whether these are individual stand-alone systems, logs in an application, or something different, data must be available. Only after data feeds are available can they be consolidated and analyzed for real-time proactive and detective security information. Centralize this information into a consolidated engine for use in analytics. Log management vendors today seem best positioned to provide this service. The priority is to gather all relevant data in one place so that it can later be used to analyze the information.

3. **Create actionable business analytics.** Once the data has been centralized, the final step of maturity is to create business analytics, which can be acted on by information security teams. This reporting will provide metrics as to the capabilities of the organization and will alert the organization to potential risks that may otherwise have been neglected. Actionable remediation, prioritized according to business value, is ultimate maturity in this area—particularly when it can be used to improve the security and operations of networks and devices.
James Tarala is a principal consultant with Enclave Security and is based out of Venice, Florida. He is a regular speaker and senior instructor with the SANS Institute as well as a courseware author and editor for many SANS auditing and security courses. As a consultant, he has spent a large amount of time assisting organizations in their security management, operational practices and regulatory compliance issues. He often performs independent security audits and assists internal audit groups in developing their internal audit programs. James completed his undergraduate studies at Philadelphia Biblical University and his graduate work at the University of Maryland. He holds numerous professional certifications.
SANS would like to thank this paper’s sponsor

NETWITNESS

splunk®
<table>
<thead>
<tr>
<th>Event Name</th>
<th>City, Country</th>
<th>Date Range</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Munich December 2017</td>
<td>Munich, DE</td>
<td>Dec 04, 2017 - Dec 09, 2017</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Austin Winter 2017</td>
<td>Austin, TXUS</td>
<td>Dec 04, 2017 - Dec 09, 2017</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Bangalore 2017</td>
<td>Bangalore, IN</td>
<td>Dec 11, 2017 - Dec 16, 2017</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS SEC460: Enterprise Threat Beta</td>
<td>San Diego, CAUS</td>
<td>Jan 08, 2018 - Jan 13, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Security East 2018</td>
<td>New Orleans, LA</td>
<td>Jan 08, 2018 - Jan 13, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Northern VA Winter - Reston 2018</td>
<td>Reston, VAUS</td>
<td>Jan 15, 2018 - Jan 20, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Amsterdam January 2018</td>
<td>Amsterdam, NL</td>
<td>Jan 15, 2018 - Jan 20, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dubai 2018</td>
<td>Dubai, AE</td>
<td>Jan 27, 2018 - Feb 01, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Las Vegas 2018</td>
<td>Las Vegas, NVUS</td>
<td>Jan 28, 2018 - Feb 02, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Miami 2018</td>
<td>Miami, FLUS</td>
<td>Jan 29, 2018 - Feb 03, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Cyber Threat Intelligence Summit &amp; Training 2018</td>
<td>Bethesda, MDUS</td>
<td>Jan 29, 2018 - Feb 05, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS London February 2018</td>
<td>London, GB</td>
<td>Feb 05, 2018 - Feb 10, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Scottsdale 2018</td>
<td>Scottsdale, AZUS</td>
<td>Feb 05, 2018 - Feb 10, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Southern California- Anaheim 2018</td>
<td>Anaheim, CAUS</td>
<td>Feb 12, 2018 - Feb 17, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure India 2018</td>
<td>Bangalore, IN</td>
<td>Feb 12, 2018 - Feb 17, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dallas 2018</td>
<td>Dallas, TXUS</td>
<td>Feb 19, 2018 - Feb 24, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Cloud Security Summit &amp; Training 2018</td>
<td>San Diego, CAUS</td>
<td>Feb 19, 2018 - Feb 26, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Brussels February 2018</td>
<td>Brussels, BE</td>
<td>Feb 19, 2018 - Feb 24, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure Japan 2018</td>
<td>Tokyo, JP</td>
<td>Feb 19, 2018 - Mar 03, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS New York City Winter 2018</td>
<td>New York, NYUS</td>
<td>Feb 26, 2018 - Mar 03, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>CyberThreat Summit 2018</td>
<td>London, GB</td>
<td>Feb 27, 2018 - Feb 28, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Khobar 2017</td>
<td>OnlineSA</td>
<td>Dec 02, 2017 - Dec 07, 2017</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>