Continuous Network Monitoring

Eliminate periodic assessment processes that expose security and compliance programs to failure
Continuous Network Monitoring

Continuous network monitoring and assessment is an evolving best practice to effectively address today’s threats, technology risks, and changing regulatory requirements. Periodic and static vulnerability and configuration security assessments are no longer sufficient to address today’s security and compliance environment.

Continuous network monitoring is the only effective countermeasure that an enterprise can implement to address today’s cyber threats. Traditionally, periodic vulnerability and configuration assessments are performed on scheduled basis: sometimes yearly, quarterly, or monthly. Organizations then analyze results, validate and prioritize vulnerabilities and configuration risks, schedule and apply patching and remediation, and develop management and compliance reports. The process is repeated during the next assessment cycle.

This periodic, scheduled cycle leaves gaps during which there is no automatic discovery of new assets that might be vulnerable, no certainty that remediation efforts were successfully applied, and no correlation of vulnerable assets to actual events happening within the network to detect a cyber threat. During those gaps new assets may be added, countermeasures turned off, or vulnerabilities introduced.

In short, periodic assessments result in knowledge gaps and have limited value when an incident occurs. Continuous network monitoring eliminates those gaps.

What Is Continuous Network Monitoring?

Continuous monitoring is the process of constantly and persistently monitoring technological assets, vulnerabilities, configurations, and (importantly) current network events to discover new assets that may be vulnerable and detect anomalies or other suspicious activities.

Continuous network monitoring requires the integration of core technologies with applied intelligence that combined gives an enterprise the ability to implement and maintain an effective and efficient continuous monitoring and assessment program.

By orchestrating internal processes with the core technologies outlined below, organizations can create the baseline operational and technical capabilities to support:

- real-time asset discovery
- real-time situational awareness of vulnerabilities and events
- real-time incident response

Core technologies for continuous network monitoring

No single technology can deliver comprehensive and continuous monitoring. You need to integrate the following core technologies:

- Vulnerability and configuration assessment or scanning to establish a baseline of assets and scan for vulnerabilities and configuration information
- Network span port to capture network events in real time
- Log Correlation Engine (LCE) or Security Information and Event Management (SIEM) technology to store, correlate, and analyze current network events and any system and/or IPS/IDS logs against vulnerability and configuration assessment results
- Centralized management console to visualize, analyze, and review the current state of assets, vulnerabilities, configurations, and events. This console will help you develop correlation and other anomaly-based rules, manage remediation workflow and incident response, and generate alerts on the discovery of new assets or vulnerabilities.
Adding intelligence and operational capabilities
Integrating vulnerability assessment processes with log correlation and network event monitoring gives you the technical foundation for a continuous monitoring program. This integrated platform should deliver the following capabilities:

- Discover and maintain an up-to-date inventory of assets
- Classify any new assets within the environment
- Perform or execute ongoing vulnerability assessments of existing and new assets
- Execute configuration or policy security compliance assessments of all assets
- Capture and monitor network events
- Correlate and analyze events to identify and prioritize any anomaly for effective remediation and real-time actionable incident response

By adding and integrating assets, threats, vulnerabilities, configuration compliance results, network events, and other system log events with these technical capabilities, you gain significant operational intelligence capabilities. The integrated solution gives you a centralized console or dashboard for vulnerability, configuration, and event management, correlation rule development, and monitoring and analysis of events and information.

Integrating these technologies and implementing a continuous network monitoring program offers the following operational capabilities:

- Integrated network and security operation center for vulnerability management and incident response
- Advanced threat detection
- Integrated configuration and vulnerability life cycle management
- Strengthened incident response and detailed situational awareness

Benefits Of Continuous Monitoring
By implementing continuous monitoring, you can realize the following significant benefits:

- Having the operational capabilities to identify and combat new cyber threats, such as advanced persistent threats (APTs)
- Maintaining a just-in-time inventory of all assets, vulnerabilities, and security configuration gaps
- Gaining visibility into network events and activities to identify anomalies
- Dramatically improving incident response capabilities based on risks, vulnerabilities, and current events
- Strengthening compliance posture to meet escalating regulatory requirements

Additionally, continuous monitoring transforms your staff efforts from a reactive to a proactive posture. Continuous monitoring eliminates the ‘fog of war’ predicament during crisis because you have real-time or near real-time visibility of all your assets, vulnerabilities, and risks based on current events and information.

Why Is Continuous Network Monitoring Necessary?
Continuous monitoring is necessary for three primary reasons:

1. Combating today’s cyber threats
2. Mitigating risks of virtual and other new technologies
3. Positioning your organization to address growing regulatory and compliance requirements
The cyber threat environment

It is well known and widely publicized; cyber criminals and cyber warfare are real threats. These attacks are sophisticated, they are targeted, and unfortunately for the victim, they are very successful. One of the reasons for attackers’ success is that their methods have outpaced generally-accepted security practices.

It is no longer sufficient to periodically scan systems for vulnerabilities and configuration errors and regularly patch systems. Cyber criminals know that at any point in time, every enterprise has vulnerabilities and/or configuration gaps, not to mention zero day vulnerabilities. Even regular scanning and patching – whether quarterly, monthly, or even weekly – leaves an enterprise vulnerable to hacker penetration.

When sophisticated and risk-sensitive enterprises such as RSA, Lockheed Martin, and the Department of Defense get hacked, it should be a wake-up call to everyone. Enterprises need to step up their security countermeasures. Continuous monitoring is the only effective countermeasure that an enterprise can implement today.

Increasing technology risks

The pace of change and the proliferation of new technologies are increasing the technological risks an enterprise faces.

A virtual host can be provisioned on the network within minutes, whereas traditionally it would take weeks to procure and provision a physical server. Enterprises must address the risks of virtual sprawl and virtual hosts appearing on the network whether they are properly configured and patched.

Also, the increasing use of outsourced cloud computing by enterprises augments technological risks and exposures. Cloud computing services such as Amazon EC2 and Windows Azure all increase the risks of unpatched or misconfigured hosts.

Finally, the consumerization of IT, through which personal mobile and other devices are allowed access to the enterprise internal network, is another technology trend that increases enterprise technology risk.

These technology risks and others contribute to an increased risk exposure for all enterprises – yet another reason to implement an effective continuous monitoring program.

Emerging compliance risks pertaining to continuous network monitoring

Government regulatory bodies are increasingly recognizing the need for continuous monitoring. Both FFIEC (Federal Financial Institution Examination Council) and NIST (National Institute Standards & Technology) have recently issued new guidance regarding continuous monitoring. The FFIEC guidance in the IT Examination Handbook states:

A static security program provides a false sense of security and will become increasingly ineffective over time. Monitoring and updating the security program is an important part of the ongoing cyclical security process. Financial institutions should treat security as dynamic with active monitoring; prompt, ongoing risk assessment; and appropriate updates to controls. Institutions should continuously gather and analyze information regarding new threats and vulnerabilities, actual attacks on the institution or others, and the effectiveness of the existing security controls.

The National Institute of Standards and Technology is developing new guidance for federal agencies to deploy continuous network monitoring, as described in a draft NIST SP 800-137. They also have a continuous network monitoring working group in place. NIST’s defines continuous monitoring as follows:

“Continuous Monitoring is a risk management approach to cyber security that maintains an accurate picture of an organization’s security risk posture, provides visibility into assets, and leverages use of automated data feeds to quantify risk, ensure effectiveness of security controls, and implement prioritized remedies.”

Both of these regulatory activities recognize the limitations of static or periodic vulnerability assessments and will surely lead to increased scrutiny by auditors and regulators to ensure that enterprises have continuous network monitoring security programs and controls in place.
The Bottom Line
Cyber Criminal threats, new technology risks, and emerging regulatory compliance requirements all point to the crucial need to implement continuous network monitoring.

Organizations should act now to put continuous monitoring processes, capabilities, and supporting technologies in place. These include maintaining an up-to-date inventory of assets and discovery new assets in real time; classifying assets; performing ongoing vulnerability and configuration assessments; monitoring network events; correlating and analyzing events for incident response; and using dashboards/reporting to visualize, analyze, and review the current state of assets, vulnerabilities, configurations, and events.

By implementing continuous network monitoring, organizations gain the ability to identify and combat new cyber threats as they occur. With a “just-in-time” inventory of assets, vulnerabilities and security configuration gaps, you can respond in a timely manner to changes that threaten security or compliance, including virtual or mobile assets introduced with or without central knowledge and permission. And with real-time visibility into assets and configurations, you can readily adapt to changing regulatory requirements.

How Do I Move My Organization To Continuous Network Monitoring?
There are three main options for deploying the technologies necessary for an effective continuous monitoring and assessment program:

1. Build and integrate your own solution
2. Buy an integrated, out-of-the-box solution
3. Adopt a hybrid approach, continuously monitoring between scans for new assets and monitoring for unusual activity or suspected cyber threats

We will examine and analyze each of these options below.

Build your own
Using the ‘build your own’ approach means that you buy individual solutions or leverage existing technologies, integrate them, and develop the correlation algorithms to extract the necessary business intelligence to support an effective continuous monitoring security program.

Technically, this means connecting existing vulnerability and configuration assessment solutions to the SIEM, implementing necessary span port(s) to capture network events and sending them to the SIEM, developing and maintaining correlation algorithms and rules to detect and remediate vulnerabilities and/or new assets that have not been scanned, integrating a passive vulnerability scanner to the infrastructure, and building correlation algorithms to detect anomalies or cyber threats.

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leverage existing technology (e.g., SIEM)</td>
<td>Higher deployment cost to create necessary business intelligence (correlation algorithms), alerting and remediation workflow, etc.</td>
</tr>
<tr>
<td>Leverages existing SIEM (i.e., engineering and security)</td>
<td>Extended time to deploy</td>
</tr>
<tr>
<td>Potentially minimizes introducing new technologies into IT infrastructure</td>
<td>Likely will require professional services to implement and maintain</td>
</tr>
<tr>
<td></td>
<td>Divert resources from focusing on threat detection and risk mitigation to system maintenance</td>
</tr>
<tr>
<td></td>
<td>Correlation algorithms and cyber threat detection routines are not maintained by a certified vulnerability and configuration assessment vendor</td>
</tr>
</tbody>
</table>

This option is best suited for enterprises that have a mature SIEM implementation in place, have the technical and security subject matter expertise to develop and maintain increasingly complex correlation algorithms, and/or have the financial resources to obtain professional services to develop and maintain the infrastructure.
Enterprises that do not have most of these technologies in place, or do not have the financial or technical resources, should consider other deployment options.

**Buy an out-of-the-box, integrated solution**

Another option is buying an out-of-the-box solution that has all the core technologies embedded and integrated, with built-in intelligence that results in all the necessary operational capabilities for an effective ongoing monitoring program.

From a technology perspective, an out-of-the-box product contains a static vulnerability and configuration assessment solution for periodic assessments, a passive vulnerability scanner for real-time assessment of new assets, and a log correlation engine or SIEM that is optimized to store and correlate network events captured from span port(s). Correlation algorithms and rules to extract business intelligence should be included and customizable. The solution should also include a central console with dashboard capabilities to efficiently start an ongoing monitoring program from Day 1.

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fastest deployment. All technical capabilities included and optimized for Day 1 deployment.</td>
<td>May overlap with existing technology already in place (e.g., SIEM, vulnerability assessment vendor). Another console to use.*</td>
</tr>
<tr>
<td>Requires little, if any, professional services or internal development of correlation algorithms.</td>
<td>Initial capital outlay may be higher compared to other options.</td>
</tr>
<tr>
<td>No system integration required.</td>
<td></td>
</tr>
<tr>
<td>Designed for near or real-time visibility and discovery of assets, vulnerabilities, and network events.</td>
<td></td>
</tr>
<tr>
<td>Built-in intelligence developed and maintained by a certified vulnerability assessment vendor.</td>
<td></td>
</tr>
<tr>
<td>Typically contains other valuable features and capabilities such as remediation workflow, on-demand compliance reporting, database monitoring, forensic analysis, enhanced threat detection, log management monitoring, etc.</td>
<td></td>
</tr>
<tr>
<td>May create opportunities to reduce IT infrastructure complexity.*</td>
<td></td>
</tr>
<tr>
<td>Dramatically improves incident response capabilities with realtime visibility into vulnerabilities and current network events.</td>
<td></td>
</tr>
</tbody>
</table>

* Note: While an out-of-the-box solution may overlap with existing technologies in place, it also creates an opportunity to reduce IT infrastructure complexity and costs by consolidating to one integrated solution and one vendor. It might be especially attractive to enterprises that under-utilize their current SIEM solution or have limited resources to build correlation algorithms to extract actionable business intelligence.

This option is best suited for enterprises that want an effective continuous monitoring program while minimizing deployment cost, effort, and ongoing maintenance cost. It is also suited for enterprises that want to fortify their cyber threat detection capabilities, strengthen incident response capabilities, and improve compliance posture. Using this approach, enterprises can divert resources from administrative compliance governance tasks to risk mitigation tasks. Finally, this option creates an opportunity for an enterprise to reduce IT infrastructure complexity and cost, reducing the number of vendors and products by consolidating SIEM and console/dashboards to one system.

**Use a hybrid approach**

Using a hybrid approach, you buy an out-of-the-box solution only for on-line monitoring to detect new assets, then scan those new assets and monitor network events for anomalies or threat detection. This option might be embraced by enterprises that desire vulnerability assessment and threat detection capabilities in real time between the static vulnerability assessment scans, while minimizing changes to their current infrastructure.

From a technology perspective, the enterprise keeps static vulnerability and configuration assessment solutions already in place for periodic assessments. The on-line monitoring solution contains a passive vulnerability scanner for real-time assessment of new assets that may vulnerable, using the existing log correlation engine or SIEM that is optimized to store and correlate network events captured from span port(s) as a special purpose SIEM. Correlation algorithms and rules to extract business intelligence are also part of this hybrid approach.
### Advantages | Challenges
---|---
Fast deployment. All technical capabilities included and optimized for Day 1 operational readiness. | May overlap with existing SIEM technology already in place. Another console to use*
Requires little, if any, professional services or internal development of correlation algorithms. | Improves but does not dramatically surpass incident response capabilities.
No system integration required. | No correlation of static and online vulnerability and configuration assessment results.
Designed for near or real-time visibility and discovery of new assets, vulnerabilities assessment, and network events threat monitoring between static assessment cycles. | Compliance reporting and governance compliance cost and complexity are not reduced.
Built in intelligence developed and maintained by a certified vulnerability assessment vendor. | Opportunity cost implications compared to the integrated out-of-the-box solution.

* Note: While an out-of-the-box solution may overlap with existing SIEM technologies, in this scenario, the embedded SIEM in the vulnerability assessment tools should be considered as a special-purpose SIEM or black box.

This option is best suited for enterprises that want to implement an ongoing monitoring program while minimizing any changes to the current environment. It provides for vulnerability assessment monitoring online to close the time gap inherent with a periodic or static assessment program. It also improves cyber detection and incident response capabilities and improves an enterprise compliance posture.

### Conclusion

Periodic and static vulnerability and configuration security assessments are no longer effective to address today’s threats and risks, with rapidly changing threats and dynamic networks. Instead you need processes and technologies to support continuous network monitoring.

A continuous monitoring program includes the following tasks:

- Maintaining an up-to-date inventory of assets and discovering new assets
- Classifying assets
- Performing ongoing vulnerability and configuration security assessments
- Monitoring network events
- Correlating and analyzing events for actionable incident response
- Dashboard/analysis capabilities to visualize, analyze, and review current state of assets, vulnerabilities, configurations, and events.

With real-time or near real-time situational awareness of network events and assets, an enterprise can dramatically improve its ability to respond to an incident, proactively patch vulnerabilities before an incident occurs or becomes a major breach, and improve its compliance posture.

Enterprises have multiple viable options for implementing an effective ongoing monitoring program, ranging from building your own, buying an out-of-the-box solution, or doing something in between. Each option has advantages and challenges.

The major benefits of continuous monitoring are real-time or near real-time situational awareness of network events and assets that dramatically improves an enterprise’s ability to detect a cyber breach, respond to an incident, proactively patch vulnerabilities before an incident occurs or becomes a major breach, and improve enterprise compliance posture.

Finally, continuous monitoring re-allocates resources from administrative assessment and reporting tasks to risk mitigating actions.
About Tenable Network Security

Tenable Network Security is the leader in Unified Security Monitoring. Tenable provides enterprise-class agentless solutions for the continuous monitoring of vulnerabilities, configuration weaknesses, data leakage, log management and compromise detection to help ensure FDCC, FISMA, SANS CAG and PCI compliance. Tenable’s award-winning products are utilized by many Global 2000 organizations and Government agencies to proactively minimize network risk. For more information, please visit www.tenable.com.