Cyber Hygiene Simplified Using Tenable Solutions

Keep Pace with Security Challenges with Continuous Network Monitoring

Challenge

Today, technology is driving more change in organizations than ever before. We're highly dependent on numerous electronic devices—laptops, smartphones, tablets, and more—for both work and personal use. This is creating complexity in your IT environment, resulting in a lack of visibility and gaps in protection. Security measures aren't keeping up with the volume, frequency, diversity, and sophistication of cyber attacks. But Tenable Network Security is.

So what can an organization do? It's easy—use good cyber hygiene as outlined by the Center for Internet Security (CIS) and the Council on CyberSecurity (CCS), which means protecting and maintaining IT systems and devices appropriately and implementing cybersecurity best practices. You can make it happen with Tenable.

Tenable maintains that good cyber hygiene is built upon a robust vulnerability and threat management platform that enables you to continuously visualize the security posture of your IT infrastructure and better protect your business against advanced cyber attacks.

Cyber Hygiene Campaign Priorities & Actions

CIS and CCS launched a security awareness initiative called the "Cyber Hygiene Campaign." Designed for state, local, tribal, and territorial governments, the campaign is a multi-year effort to provide a low-cost program to achieve immediate and effective defenses against cyber attacks.

Implementing the campaign's following five priorities addresses the vast majority of known cyber threats.

1. Count: Know what's connected to and running on your network
2. Configure: Implement key security settings to help protect your systems
3. Control: Limit and manage those who have admin privileges for security settings
4. Patch: Regularly update all apps, software, and operating systems
5. Repeat: Regularly revisit the Top Priorities to form a solid foundation of cybersecurity

The Cyber Hygiene Campaign's first objective is to elicit the following top five actions:

1. Inventory authorized and unauthorized devices
2. Inventory authorized and unauthorized software
3. Develop and manage secure configurations for all devices
4. Conduct continuous (automated) vulnerability assessment and remediation
5. Actively manage and control the use of administrative privileges

The campaign aligns with the NIST Cybersecurity Framework and the CCS's 20 Critical Security Controls. Tenable's continuous network monitoring solution supports these industry guidelines as well as the Cyber Hygiene Campaign's top priorities and actions.

How Tenable Can Help

Tenable's SecurityCenter Continuous View™, or SC® CV™, enables the most comprehensive and integrated view of the health of your IT infrastructure through continuous network monitoring. SC CV continuously discovers components on the network, assesses components against security policies, reports results to accelerate remediation, and provides context-based metrics and reporting. SC CV identifies the biggest risks across your organization and allows you to manage advanced threats, zero-day vulnerabilities, and new forms of regulatory compliance. And SC CV scales, so as you grow, we grow with you.

SecurityCenter Continuous View helps maintain accurate inventories and secure device configurations, detect unauthorized software, continuously assess and remediate devices, and track the use of elevated privileges.

SC CV Key Advantages

- Vulnerability & patch management
- Configuration assessment
- Web application scanning
- Continuous network monitoring
- Malware & botnet detection
- Compliance monitoring for government, financial, retail, & healthcare regulations
- Log aggregation & correlation
- Forensic analytics & incident response
- Mobile, virtual, & cloud coverage
- Configurable dashboards & reports

SC CV enables state and local government agencies with few IT security personnel, tight cybersecurity budgets, or cybersecurity programs under development or improvement to meet the top priorities and actions.

Top 5 Priorities

SC CV can assist in implementing the top five priorities in three main ways.

1. **Discover vulnerabilities and track remediation progress**: Uses active scanning, passive monitoring, and event log analysis to detect vulnerabilities. With this information, SC CV can identify the biggest risks across your organization and assist in prioritizing and tracking remediations.
2. **Monitor the network for unauthorized or malicious activity**: Continuously monitors network traffic for suspicious activity, such as botnets, intrusions, data leakage, and suspicious user behavior, while logs are collected and correlated to discover unauthorized or malicious activity.
3. **Measure compliance**: Uses audit files to cover a wide range of major regulations and other auditable standards. The solution can perform configuration audits over a wide variety of systems.

Top 5 Actions

Continuous network monitoring identifies the biggest risks across your organization, and Tenable's unique sensors and analytics let you assess how well your security program is performing.

Inventory Authorized & Unauthorized Devices

SC CV performs automated discovery of devices by utilizing its network monitoring capability in conjunction with scanning and log collection. SC CV has the ability to discover physical, virtual, and mobile devices as soon as they connect to the network, providing visibility across your entire network.

Inventory Authorized & Unauthorized Software

SC CV can identify software installed on a computer using event correlation, passive detection, and active scanning. The Tenable solution can identify software based on vulnerabilities detected, by using fingerprinting techniques, and by tracking software installation and update log events.

Develop & Manage Secure Configurations for All Devices

Monitoring for configuration changes can be difficult. SC CV can provide detailed log events with each configuration change so event logs can be captured for network devices to monitor for configuration change events. Events like "Never Before Seen" or "New Port Usage" can be tracked. SC CV also monitors for trusted client and server connections, and can also detect when a new web server comes online and send alerts to the security team.

Conduct Continuous Vulnerability Assessment & Remediation

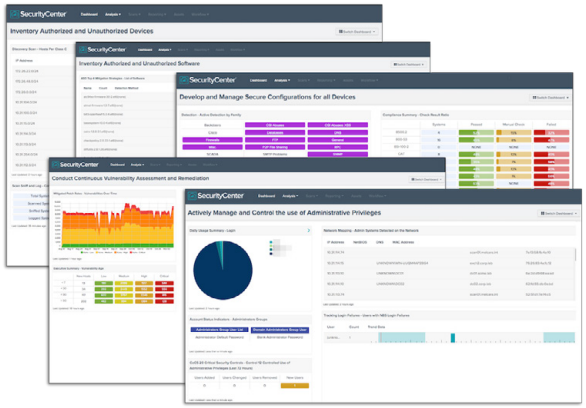
Many organizations perform periodic scanning and manually control the scans. SC CV has the ability to schedule distributed scans across scan zones. Scan zones let you assign a scanner to a group of targets, avoiding scans over WAN links or other congestion points. The best approach is to move beyond periodic scans to continuous network monitoring with SC CV. This lets you monitor your network health in real time, as well as manage risks, threats, or variances as they emerge.

Actively Manage & Control the Use of Administrative Privileges

Monitoring the use of elevated privileges and who has them is critical to the security of any organization. In today's environment of client-side attacks, this monitoring is even more crucial. The best practice is to have a system administrator with two accounts: a regular user account and an administrative account. SC CV can easily track group memberships and admin-related events.

Cyber Hygiene Dashboards & Reports

In support of the Cyber Hygiene Campaign, Tenable created a series of Cyber Hygiene dashboards. These dashboards focus on the top five actions identified by the first phase of the campaign and provide a centralized view of the devices, software, device configurations, prioritized vulnerabilities, and administrative privileges across your organization.



SC CV comes with more than 230 out-of-the-box report templates. Reports can be customized by merging chapters together. The Application Patch Rate, Nessus Scan Summary, Administrator, SCAP Audit Summary, and Network Mapping reports support the top five priorities and package dashboard information so it can be easily shared for better visibility and rapid decision making.

Next Steps

Using SecurityCenter Continuous View, state and local government agencies can effectively address the top five priorities and actions outlined in the Cyber Hygiene Campaign. With SC CV, you can create and maintain accurate inventories and secure device configurations, detect unauthorized software, continuously assess and remediate devices, and track the use of elevated privileges.

For a more detailed discussion exploring the ways SC CV addresses the top five priorities and actions outlined in the Cyber Hygiene Campaign, download the technical white paper, "Tenable Solutions for the Cyber Hygiene Campaign." To evaluate SC CV, please contact SLG_Sales@tenable.com.

For More Information: Please visit tenable.com
Contact Us: Please email us at sales@tenable.com or visit tenable.com/contact