SECHARD
Complete Zero Trust

Security Configuration Management (SCM)

Guide for Security-Focused Configuration Management of Information Systems

Security Configuration Management

Security Configuration Management (SCM) is a critical aspect of cybersecurity that involves the systematic management and control of an organization's information system configurations to ensure their security and compliance with established standards and policies. SCM encompasses the identification, implementation, and maintenance of security settings and configurations across various hardware, software, and network components.

The primary objectives of SCM include:

- **Establishing Secure Baselines:** Defining and documenting the secure configuration settings for each system component based on industry best practices, such as guidelines from the Center for Internet Security (CIS) or the National Institute of Standards and Technology (NIST).

- **Continuous Monitoring and Enforcement:** Regularly monitoring systems to detect deviations from the secure baseline configurations and enforcing compliance through automated tools and processes.

- **Change Management:** Managing and controlling changes to system configurations to ensure that security is not compromised. This includes reviewing, testing, and approving changes before they are implemented.

- **Vulnerability Management:** Identifying and addressing vulnerabilities in system configurations that could be exploited by attackers. This involves regular scanning, patch management, and remediation activities.

- **Auditing and Reporting:** Conducting periodic audits to verify compliance with security policies and standards. SCM tools often provide reporting capabilities to document compliance status and support regulatory requirements.

Best Practices for Establishing Secure Configurations

SECHARD
Complete Zero Trust

By adhering to these best practices, organizations can establish secure configurations that minimize vulnerabilities, enhance system stability, and improve overall security posture.

- Leverage Common Secure Configurations
- Centralize Policy and Secure Configurations
- Tailor Configurations to System Roles
- Minimize Unnecessary Services (Least Functionality)
- Restrict Remote Connections
- Implement Strong Password Policies
- Deploy Endpoint Protection Platforms (EPPs)
- Utilize Cryptography
- Establish a Patch Management Process
- Control Software Installation

*Source: NIST Special Publication 800-128

Leverage Common Secure Configurations

- Organizations should base their secure configuration settings on widely recognized standards, such as those provided by the National Checklist Program. These checklists offer detailed guidance for configuring a range of commercial products to enhance security. Utilizing Security Content Automation Protocol (SCAP)-enabled tools can streamline the assessment process, allowing for automated evaluations of system configurations against established benchmarks. This approach ensures that systems are consistently configured according to industry best practices, reducing the likelihood of vulnerabilities.

- By adopting common secure configurations, organizations can benefit from the collective expertise of the cybersecurity community. These configurations are typically developed through extensive research and testing, offering a solid foundation for securing systems. Regularly updating these configurations to reflect the latest security advancements is crucial for maintaining a strong defense against evolving threats.

Centralize Policy and Common Secure Configurations for Configuration Settings

- Implementing secure configurations effectively requires a centralized approach to ensure uniformity across the organization. Tools like group policy functionality in Windows environments enable the distribution of security policies and configurations from a central point, ensuring consistency across all systems within established domains. This centralized management simplifies the enforcement of security settings and reduces the complexity of maintaining security across diverse systems.

- While a top-down approach is ideal for standardization, it's important to recognize that some systems may have unique requirements. Exceptions to the organization's general security policy may be necessary to accommodate specific needs or constraints of individual systems. Documenting and approving these exceptions as part of the baseline configuration for each system ensures that deviations are controlled and justified, maintaining overall security integrity while allowing for necessary flexibility.

Tailor Secure Configurations According to System/Component Function and Role

- Security configurations should be customized to align with the specific roles and functions of system components. For example, a server designated as a Windows domain controller may warrant more stringent security measures, such as enhanced auditing settings, compared to a standard file server. This tailored approach ensures that security settings are appropriate for the level of sensitivity and exposure of each system component.
- In environments with varying levels of exposure, such as a public-facing web server in a demilitarized zone (DMZ) versus an internal web server, the security configurations should reflect the differing risk profiles. A web server in a DMZ, for instance, should operate with minimal services and tighter security controls compared to an internal server that may have additional protections from the internal network. This differentiation helps to minimize the attack surface and protect critical assets according to their exposure and role.

Eliminate Unnecessary Ports, Services, and Protocols (Least Functionality)

- Configuring devices to adhere to the principle of least functionality is crucial for minimizing security risks. This involves disabling any ports, protocols, and services that are not essential for the device's operation or the organization's functional needs. By limiting the number of active services, the potential entry points for attackers are reduced, decreasing the overall vulnerability of the system.
- Regular reviews of open ports and available services are necessary to ensure that only those required for legitimate business purposes are enabled. Additionally, staying informed about vulnerabilities associated with specific ports, protocols, or services through resources like the NIST National Vulnerability Database can guide decisions on which elements to disable or restrict. This proactive approach to minimizing unnecessary functionalities helps to create a more secure and manageable network environment.

Limit the Use of Remote Connections

- Remote access to systems introduces potential security risks, as it provides an avenue for attackers to exploit. Limiting the use of remote connections to only those that are absolutely necessary for mission accomplishment is a prudent security measure. When remote access is required, employing secure methods such as virtual private networks (VPNs) can provide an additional layer of protection by encrypting the connection and verifying the identity of users.

- Implementing strict access controls and monitoring for remote connections is essential to detect and prevent unauthorized access. Regularly reviewing and updating remote access policies and configurations to align with current security best practices and organizational needs can further enhance the security of remote connections. By carefully managing and securing remote access, organizations can maintain flexibility in operations while safeguarding against potential threats.

Develop Strong Password Policies

- Robust password policies are a fundamental aspect of securing privileged identities. Organizations should enforce complex password requirements, including length, complexity, and expiration policies, to strengthen the security of authentication mechanisms. Educating users on the importance of secure password practices, such as avoiding common or easily guessable passwords, is also crucial to prevent password-related breaches.

- In addition to setting strong password policies, organizations should implement measures to ensure that passwords are stored and transmitted securely. This includes using encryption to protect passwords at rest and in transit, as well as employing secure password management tools to help users manage their credentials safely. Regularly auditing password policies and practices can help identify areas for improvement and ensure ongoing compliance with security standards.

Implement Endpoint Protection Platforms (EPPs)

- Endpoints, such as laptops, desktops, and mobile devices, are often targeted by attackers due to their accessibility and the valuable data they may contain. Implementing Endpoint Protection Platforms (EPPs) provides a comprehensive security solution that can include anti-malware, personal firewalls, host-based intrusion detection and prevention systems (IDPS), and other security features. These tools work together to detect and prevent a wide range of threats, from viruses and malware to more sophisticated attacks.

- Anti-malware software is a critical component of EPPs, offering protection against a variety of malicious software. It should be configured to automatically update its signatures and scan files and systems regularly. Personal firewalls help control network traffic to and from the endpoint, while host-based IDPS monitors the system for suspicious activity. Organizations should ensure that EPPs are properly configured and regularly updated to maintain their effectiveness in protecting endpoints from emerging threats.

Use Cryptography

- Cryptography plays a vital role in protecting the confidentiality and integrity of data, especially for systems that handle sensitive information. Implementing encryption for data at rest, such as using full disk encryption or file-level encryption, helps prevent unauthorized access to stored data. For data in transit, secure communication protocols like SSL/TLS or VPN connections should be used to encrypt network traffic.

- Key management is an essential aspect of cryptographic security, ensuring that encryption keys are securely generated, stored, and managed throughout their lifecycle. Organizations should adopt strong encryption standards and algorithms that are widely recognized as secure and regularly review their cryptographic practices to ensure they remain effective against evolving threats.

Develop a Patch Management Process

- A robust patch management process is crucial for maintaining the security of systems and applications. This involves regularly identifying, testing, and applying patches to fix vulnerabilities and address security issues. Integrating patch management into the security configuration management process ensures that patches are assessed for their security impact and implemented in a controlled manner.

- The patch management process should include mechanisms for tracking and verifying the successful application of patches. Regular assessments should be conducted to ensure that systems are up to date with the latest patches, and any deviations from the baseline configuration should be documented and reviewed. Automating patch management processes, where possible, can help streamline operations and reduce the risk of human error.

Control Software Installation

- Controlling the installation of software is critical to preventing the introduction of vulnerabilities and malware into the system. Organizations should adopt a centralized approach to software management, where possible, to ensure that only authorized and secure software is installed. This can be achieved through whitelisting approved software, verifying the integrity of software packages using checksums or digital signatures, and restricting the installation of software from untrusted sources.

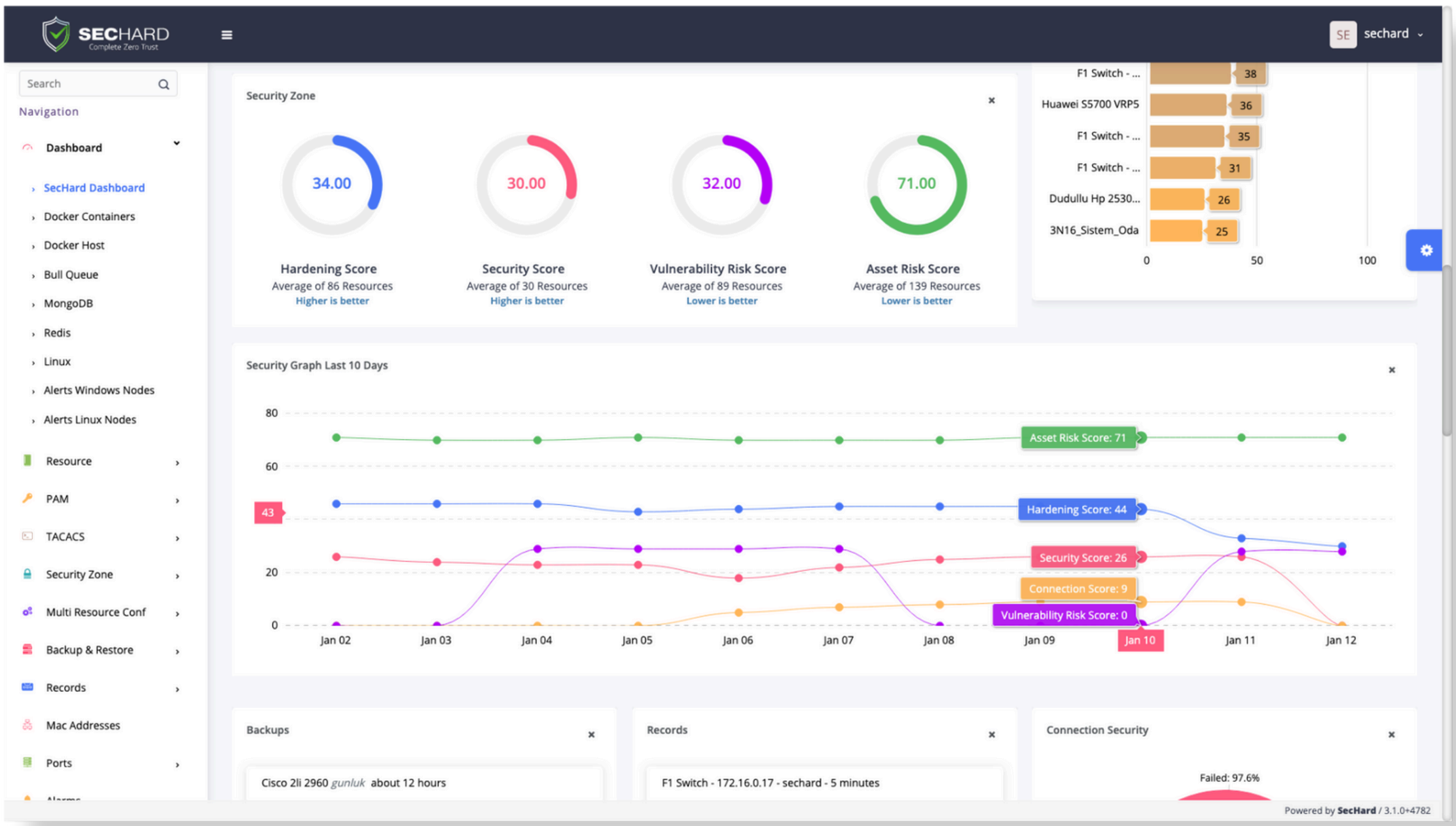
- Additional controls, such as restricting the use of removable media or limiting software installation to specific directories or domains, can further reduce the risk of unauthorized software installations. Regular audits and monitoring of installed software can help detect and address any deviations from approved software configurations, maintaining the integrity of the system.

SecHard Zero Trust Orchestrator

SecHard provides automated security hardening auditing, scoring, and remediation for servers, clients, network devices, applications, databases, and more.

According to CIS, in order to have a secure operating system, it is necessary to change approximately four hundred security settings on a Microsoft Windows Server running with the default settings. There are most probably hundreds of missing security settings on the computer that you have. In an enterprise network with hundreds or thousands of IT assets, reporting and remediating all these deficiencies can be an operation that will take years for IT teams.

With SecHard, enterprises can easily add their own, unique controls and run them on thousands of different assets. In this way, special audit and automatic remediations can be produced for both common and non-common technologies such as Operating Systems, Network Devices, Applications, IoT, SCADA, Swift, POS and many more.



sales@sechard.com

SECHARD
Complete Zero Trust

Contact us • Get Started • Contact us • Get Started

SecHard Zero Trust Orchestrator

SECHARD
Complete Zero Trust

SecHard Zero Trust Orchestrator is a multi-module software for implementing Zero Trust Architecture designed to facilitate compliance with the Executive Office of Presidential memorandum (M-22-09), NIST SP 800-207, and Gartner Adaptive Security Architecture.

It also supports compliance with CBDDO compliance, CIS V7.1, CIS V8, CMMC Compliance, HIPAA compliance, ISO 27001, ISO 27002, NIST 800-171r2, NIST 800-207A, NIST 800-210, NIST 800-53r5, PCI DSS, SOX Compliance, GDPR, KSA SAMA, KSA ECC, Egypt Financial Cyber Security Framework Digital v1 compliance. SecHard Zero Trust Orchestrator is built on the principles of zero-trust security, which means it treats all devices and users as untrusted and verifies every access request before granting access.

SecHard Zero Trust Orchestrator modules, such as Security Hardening, Privileged Access Manager, Asset Manager, Vulnerability Manager, Risk Manager, Device Manager, Performance Monitor, Key Manager, TACACS+ Server, and Syslog Server, work together seamlessly to provide a comprehensive set of tools that facilitate compliance with industry standards.

Contact us today to learn more about how Sechard can help you achieve your cybersecurity goals!

sales@sechard.com