

SecureVue™: Configuration Auditing Using the Center for Internet Security (CIS) Standards

Solution Brief

CIS: The Benchmark for Information Security

Poorly configured or mis-configured systems are the "low-hanging fruit" that most entices malicious attackers and malware. From weak password settings and incorrect file system access controls, to running applications and services with known vulnerabilities, security professionals spend an inordinate amount of time tracking down and eliminating one-off configurations that can expose an otherwise secure network to major threats.

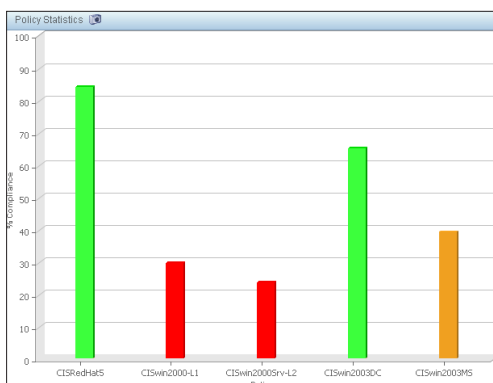
One way security professionals address this issue is by implementing standard, "security hardened" configurations. While some vendors provide recommendations for configuring their products to balance functionality with security, there has historically been no uniform set of guidelines to ensure the security of a broad range of operating systems, network devices, applications, and databases. Fortunately, the Center for Internet Security (CIS) has established a series of secure configuration benchmarks to provide comprehensive, detailed security controls for enterprise systems. The standards cover an extremely diverse range of systems, and when applied, result in a security-hardened configuration that eliminates common system-related attack vectors.

The CIS benchmarks are also used by organizations throughout the world and across a wide range of industries as the "gold standard" of technical controls to achieve compliance with major regulations, best practices, and standards. While mandates such as PCI DSS, FISMA, HIPAA, and NERC CIP provide requirements for processes and a minimal set of high-level technical controls, they leave the details of system configuration up to the organization. The CIS benchmarks provide deep, detailed sets of platform-specific security configurations that are fully compatible with most mandates. The combination of high-level processes and controls defined in these regulations, best practices, and standards, combined with the coverage in the CIS benchmarks, provides a comprehensive blueprint for achieving both compliance and security.

SecureVue: Complete CIS Configuration Auditing

eIQnetworks' SecureVue platform provides a complete solution for CIS benchmark auditing and compliance reporting. Through its integrated ComplianceVue component, the SecureVue platform provides an integrated solution for CIS configurations across a wide range of criteria, including:

- **Patch Information** including operating system versions, major installed vendor Service Packs and other critical updates, and third-party patches and drivers
- **Applications and Services** including specific versions, as well as the startup state and run level of operating system services and daemons
- **System Audit Settings** including types of events logged, access permissions to system logs, and log parameters such as maximum size, and whether logs are over-written
- **Access Controls** including individual permissions and accounting on file systems, the



SecureVue provides interactive dashboards of compliance across all supported CIS benchmark standards

Run Status: Violation [Attach To Ticket]

Node: TESTDC2K3

Policy: CISwin2003DC

Audit Policy for Windows Domain Controllers as per (CIS) benchmarks

Section: 3.1 Major Security Settings

Title: 3.1 Major Security Settings

Statement: Microsoft operating systems typically support a legacy anonymous login known as a "null session". The null session is actually a login session where both the user id and the password are blank. Although the operating system

Interpretation: Not Available

Control: 3.1.3 Network Access: Do not allow anonymous enumeration of SAM accounts and shares

In addition to protecting the list of user accounts, it also controls the list of network file shares established on the workstation. Documentation does not describe behavior if this setting conflicts with 3.1.1; however, if this setting is enabled, 3.1.1 should be enabled as well. Beware of the syntax

Rule: 3.1.3 Network Access: Do not allow anonymous enumeration of SAM accounts and shares

This security setting determines whether anonymous enumeration of SAM accounts and shares is allowed

ValueID: windows:SecurityOptions:DoNotAllowAnonEnumOfSAM

Value Fetched: Disabled

Expected Value: Enable(every expression matches some line to ensure something is present)

Is Missing Value Acceptable? NO

Do you want to ignore this rule? NO

Individual system data is fully mapped to appropriate CIS benchmark sections, with full descriptions and annotations



SecureVue's Configuration Auditing for CIS Benchmarks features:

- **Agentless Technology.** No software is required for deployment to any managed systems.
- **Centralized Management.** All systems are managed on a centralized console with access managed through full role-based access control.
- **Built-In Common Controls Library.** SecureVue ships out-of-box with over 2,500 common technical controls for Windows, UNIX, Linux, Cisco IOS, and other platforms. Users can create additional controls and map them directly to CIS benchmarks or any other compliance policy.
- **Completely Customizable.** Every CIS control can be customized to ensure that the benchmark meets organization-specific standards.
- **Scheduled and Ad Hoc Reporting.** Over fifty out-of-box CIS configuration reports are available, and can be run on-the-fly or scheduled for delivery via e-mail. Supported report formats include PDF, XLS, CVS, and others.
- **Configuration Baselines.** Individual systems or groups of systems can be compared to an unlimited number of "gold standard" baselines, and alerts can be generated when systems fall out of synchronization with their assigned baseline.
- **Updated CIS Benchmarks.** eIQnetworks continuously monitors and updates CIS benchmarks as they are released, and delivers updated content at no charge.



eIQnetworks
 31 Nagog Park
 Acton, MA 01720
 t. +1 978.266.9933
 f. +1 978.266.0004
 www.eIQnetworks.com

Windows registry, and other components

- **Security Configurations** such as password properties, anti-virus and firewall settings, and failed logon and lockout parameters
- **User Rights** identifying which users and groups have permission to perform specific functions such as local logon and running services
- **Network Parameters** including specific ports and protocols that are enabled, as well as network interface parameters such as speed and handshake

Node	% Compliance	# OK	# Violations	# Errors	Level	Compliance Status
TESTDC2K3	43	102	116	30	high	Non-compliant
92-168-80-227	43	106	112	30	high	Non-compliant
GEORGE-PC	0	0	1	247	low	Non-compliant
WA2003En3						
CAV2K9						
HLN2K9						
HUNK						

Section	Control	Rule	Status
2.2.3 Account Lockout Policy	2.2.3.1 Account lockout duration	2.2.3.1 Account lockout d...	VIOLATION
	2.2.3.2 Account lockout threshold	2.2.3.2 Account lockout t...	VIOLATION
	2.2.3.3 Reset account lockout counter after	2.2.3.3 Reset account loc...	VIOLATION
2.2.4.1 Application Log	2.2.4.1.1 Application Log: Maximum Event Log Size	2.2.4.1.1 Application Log...	OK
	2.2.4.1.2 Application Log: Restrict Guest Access	2.2.4.1.2 Application Log...	OK
	2.2.4.1.3 Application Log: Log Retention Method	2.2.4.1.3 Application Log...	OK
	2.2.4.1.4 Application Log: Log Retention	2.2.4.1.4 Application Log...	OK
2.2.4.2 Security Log	2.2.4.2.1 Security Log: Maximum Event Log Size	2.2.4.2.1 Security Log: M...	VIOLATION
	2.2.4.2.2 Security Log: Restrict Guest Access	2.2.4.2.2 Security Log: R...	OK
	2.2.4.2.3 Security Log: Log Retention Method	2.2.4.2.3 Security Log: L...	OK
2.2.4.3 System Log	2.2.4.3.1 System Log: Maximum Event Log Size	2.2.4.3.1 System Log: M...	OK
	2.2.4.3.2 System Log: Restrict Guest Access	2.2.4.3.2 System Log: Re...	OK
	2.2.4.3.3 System Log: Log Retention Method	2.2.4.3.3 System Log: Lo...	OK
	2.2.4.3.4 System Log: Log Retention	2.2.4.3.4 System Log: Lo...	OK
3.1 Major Security Settings	3.1.1 Network Access: Allow anonymous SID/Name trans...	3.1.1 Network Access: All...	OK
	3.1.2 Network Access: Do not allow anonymous enumera...	3.1.2 Network Access: D...	OK

Applied Filter Expression
 Policy Name : CISwin2003DC
 Node : TESTDC2K3

Compliance Evaluation Time: 12/01/2009 00:01:18
 Configuration Collection Time: 11/26/2009 13:22:51
 Vulnerability Collection Time: No Vulnerability Collection

SecureVue provides straightforward visualization of individual CIS benchmark controls on a per-system basis, allowing security and compliance professionals to quickly identify specific gaps

Comprehensive CIS Benchmark Coverage

SecureVue includes support for a broad spectrum of CIS operating system benchmarks, including:

- **Windows 2000 Level 1**
- **Windows 2000 Server Level 2**
- **Windows Server 2003 Domain Controllers**
- **Windows Server 2003 Member Servers**
- **Windows XP**
- **Red Hat Enterprise Linux 5**
- **Solaris 10**
- **AIX 5**

Discover how SecureVue provides comprehensive configuration auditing for CIS benchmarks to support enterprise security and compliance. Contact us at +1 877.564.7787 or email sales@eIQnetworks.com to learn more.