tenable

SOLUTION BRIEF

NIST SP 800-53 & TENABLE

Streamline Technical Controls

Most U.S. federal information systems must base their security and privacy controls in NIST Special Publication (SP 800-53v4, *Security and Privacy Controls for Federal Information Systems and Organizations*. However, compliance is not limited to the federal government. Many other organizations are required to comply with SP 800-53. For example, California's State Administrative Manual requires state agencies, departments and offices to use NIST SP 800-53 in the planning, development, implementation, and maintenance of their information security programs.

CHALLENGES OF IMPLEMENTING, ASSESSING & MONITORING 800-53 TECHICAL CONTROLS

FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, and NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, inform organizations as they select, tailor, implement and obtain assurance evidence for controls from the SP 800-53 security control catalog.

Most of the SP 800-53 controls can be categorized as being either administrative or technical. Administrative controls are typically implemented with processes and/or procedures and are often assessed with questionnaires or interviews. Technical controls typically interact directly with information systems and must be implemented and assessed with security technology. Both administrative and technical controls are challenging. However, technical controls present unique challenges discussed below:

Tools to automate controls: Due to the potentially high data volume, you must automate technical controls, and automation requires multiple data acquisition technologies to continuously monitor desktops, laptops, servers, on premises applications, SaaS applications, network devices, and the like. The diversity of monitoring targets often results in multiple, discrete tools.

Integration among tools: Multiple, discrete tools operating independently cannot deliver best results. A simple example is that security tools may send event to log management products. A more complex example is a tool that detects a new device when it connects to the network should be able to trigger an immediate vulnerability scan and configuration assessment of that device.

Unified reporting: Tool integration does not guarantee unified reporting. Staff resources are frequently squandered playing the spreadsheet game where someone who understands the data must reconcile it, analyze it and then present it to various stakeholders.

Ongoing Security Assessment: Obtaining initial authorization to operate is merely a good start. However, most networks are highly dynamic, so you cannot rely on periodic snapshots to safeguard covered information. You must also monitor security controls on an ongoing basis to ensure their continued effectiveness. When you discover inevitable weaknesses, you must communicate them.

AUTOMATE CONTROL MONITORING & ASSESSMENT

Tenable.sc (formerly SecurityCenter) enables you to measure, visualize and effectively communicate adherence to many SP 800-53 technical security controls. It achieves this by automating their operation and monitoring, and performing assessments to ensure they have been implemented correctly, operating as intended, and producing the desired outcome.

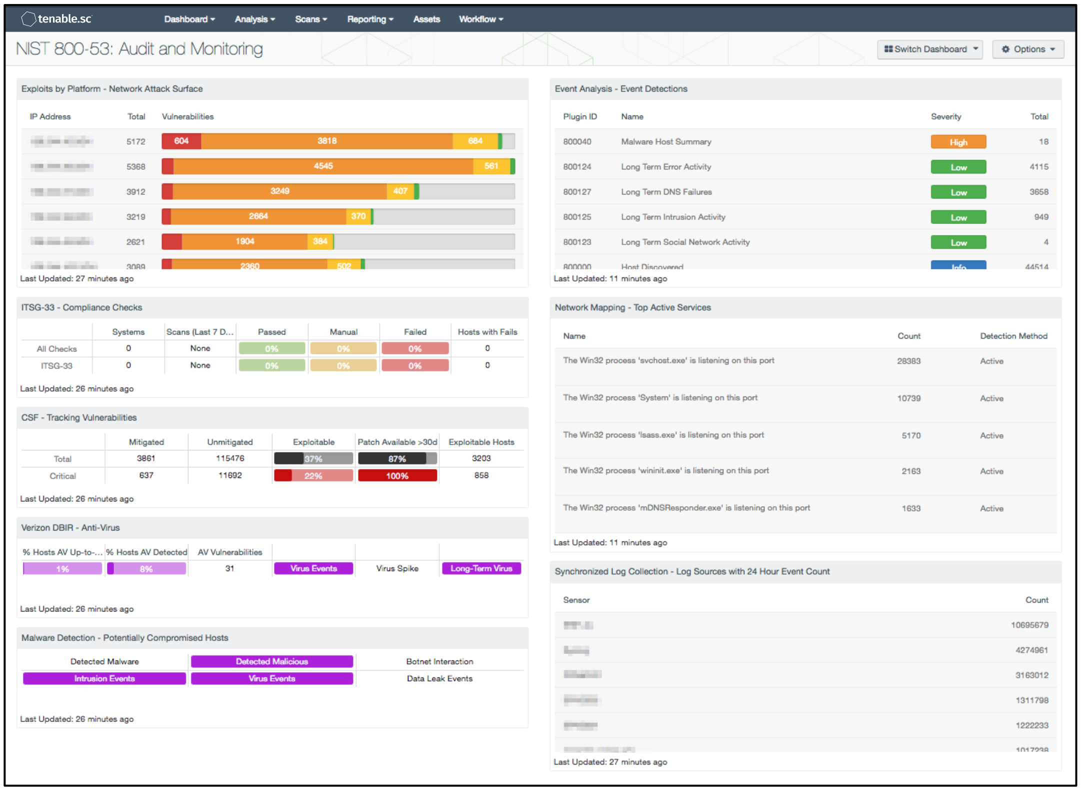
Tenable.sc will fit your specific needs. It delivers broad and continuous coverage across your entire environment, including physical, cloud, virtualized and mobile systems used in IT and industrial control networks. Dynamic asset lists enable you to logically segment, manage and report on the status of specific systems, such as those used for specific missions or business processes. Intelligent connectors to your existing security products audit configurations and analyze events to identify weaknesses in the controls.

MONITOR, ASSESS & COMMUNICATE

Information system owners, authorizing officials, and security control assessors are now scrutinizing security more than ever. You must provide them with the information they need, when they need it, without spending your time manually analyzing and summarizing data.

Tenable.sc provides fully customizable reports, dashboards and Assurance Report Card (ARC) templates—all out-of-the-box. You can use them "as-is" or quickly and easily tailor them to meet your specific security and business needs. For example, you can tailor dashboards for specific assets or business systems.

Tenable reports, dashboards and ARCs demonstrate adherence with security controls to stakeholders that may have the right to assess your security.



NIST 800-53: Audit and Monitoring

Exploits by Platform - Network Attack Surface

IP Address	Total	Vulnerabilities
[redacted]	5172	604 / 3818 / 684
[redacted]	5368	4545 / 561
[redacted]	3912	3249 / 407
[redacted]	3219	2664 / 370
[redacted]	2621	1904 / 384
[redacted]	3089	2360 / 502

Last Updated: 27 minutes ago

Event Analysis - Event Detections

Plugin ID	Name	Severity	Total
800040	Malware Host Summary	High	18
800124	Long Term Error Activity	Low	4115
800127	Long Term DNS Failures	Low	3658
800125	Long Term Intrusion Activity	Low	949
800123	Long Term Social Network Activity	Low	4
800000	Host Discovered	Info	44514

Last Updated: 11 minutes ago

ITSG-33 - Compliance Checks

	Systems	Scans (Last 7 D...	Passed	Manual	Failed	Hosts with Fails
All Checks	0	None	0%	0%	0%	0
ITSG-33	0	None	0%	0%	0%	0

Last Updated: 26 minutes ago

Network Mapping - Top Active Services

Name	Count	Detection Method
The Win32 process 'svchost.exe' is listening on this port	28383	Active
The Win32 process 'System' is listening on this port	10739	Active
The Win32 process 'lsass.exe' is listening on this port	5170	Active
The Win32 process 'wininit.exe' is listening on this port	2163	Active
The Win32 process 'mDNSResponder.exe' is listening on this port	1633	Active

Last Updated: 11 minutes ago

CSF - Tracking Vulnerabilities

	Mitigated	Unmitigated	Exploitable	Patch Available >30d	Exploitable Hosts
Total	3861	115476	37%	87%	3203
Critical	637	11692	22%	100%	858

Last Updated: 26 minutes ago

Verizon DBIR - Anti-Virus

% Hosts AV Up-to-...	% Hosts AV Detected	AV Vulnerabilities			
1%	8%	31	Virus Events	Virus Spike	Long-Term Virus

Last Updated: 26 minutes ago

Synchronized Log Collection - Log Sources with 24 Hour Event Count

Sensor	Count
[redacted]	10695679
[redacted]	4274961
[redacted]	3163012
[redacted]	1311798
[redacted]	1222233
[redacted]	1017238

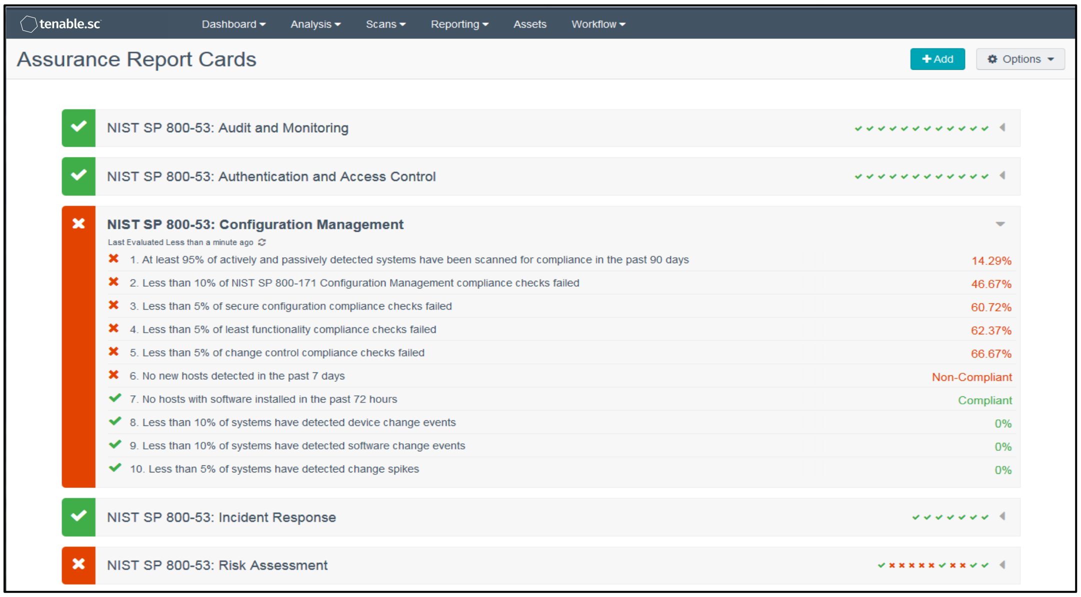
Last Updated: 27 minutes ago

Malware Detection - Potentially Compromised Hosts

Detected Malware	Detected Malicious	Botnet Interaction
Intrusion Events	Virus Events	Data Leak Events

Last Updated: 26 minutes ago

Interactive dashboards consolidate information that you can quickly drill into



Assurance Report Cards

✓ NIST SP 800-53: Audit and Monitoring ✓✓✓✓✓✓✓✓✓✓✓✓

✓ NIST SP 800-53: Authentication and Access Control ✓✓✓✓✓✓✓✓✓✓✓✓

✗ **NIST SP 800-53: Configuration Management**

Last Evaluated Less than a minute ago

✗	1. At least 95% of actively and passively detected systems have been scanned for compliance in the past 90 days	14.29%
✗	2. Less than 10% of NIST SP 800-171 Configuration Management compliance checks failed	46.67%
✗	3. Less than 5% of secure configuration compliance checks failed	60.72%
✗	4. Less than 5% of least functionality compliance checks failed	62.37%
✗	5. Less than 5% of change control compliance checks failed	66.67%
✗	6. No new hosts detected in the past 7 days	Non-Compliant
✓	7. No hosts with software installed in the past 72 hours	Compliant
✓	8. Less than 10% of systems have detected device change events	0%
✓	9. Less than 10% of systems have detected software change events	0%
✓	10. Less than 5% of systems have detected change spikes	0%

✓ NIST SP 800-53: Incident Response ✓✓✓✓✓✓✓

✗ NIST SP 800-53: Risk Assessment ✓✗✗✗✗✗✓✗✗✓✓

Assurance Report Cards present security status at a high level for non-technical audience

ARCs complement the Tenable comprehensive data collection approach, which uses a combination of active scanning, agent scanning, intelligent connectors to your third-party systems, passive listening and host data monitoring to assess the protection status of your complete infrastructure. Together, these capabilities enable you to:

- Measure, visualize and effectively communicate the technical security controls that help you manage risk
- Communicate security status to information systems owners and other stakeholders
- Understand the context you need to prioritize remediation

TENABLE.SC SP 800-53 CAPABILITIES

- **Conformance Assessment** – Automate the assessment of many NIST SP 800-53 technical controls to determine if they are implemented correctly, operating as intended and producing the desired outcome
- **Continuous Monitoring** – Benefit from both active and passive monitoring to ensure all stakeholders have real-time visibility into your security posture
- **Complete Coverage** – Gain continuous visibility across your IT networks and industrial control systems, including physical and virtual infrastructure, cloud and mobile environments
- **Assurance and Reports** – Use customizable reports, dashboards and Assurance Report Cards to evaluate and communicate security status

ABOUT TENABLE

Tenable®, Inc. is the Cyber Exposure company. Over 24,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 25 percent of the Global 2000 and large government agencies. Learn more at tenable.com.

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