SECURITY FRAMEWORKS & TENABLE

Take Your Security Program to the Next Level

There are many things you could do to improve your security, but where should you invest your resources? Many organizations are turning to security frameworks for best practices and direction for improving their security program. Their reasons for using security frameworks include:

- **Meeting due care/due diligence standards to limit liability.** Many organizations have a legal obligation to understand the cybersecurity risks they face and then implement appropriate controls to manage that risk. Failure to adequately manage risk may open the organization, its executives, and board members to legal action. For example, a U.S. appeals court recently ruled that the Federal Trade Commission has authority to pursue lawsuits accusing organizations of failing to properly safeguard consumers' information.
- **Identifying security gaps requiring additional investment.** Comparing existing security controls to those recommended by an established security framework can highlight weaknesses that require additional controls.
- **Communicating business risk to executives and board members.** Business leaders are often familiar with financial controls and will quickly grasp the concept of security controls. They will understand budget requests to implement controls needed to mitigate cyber risk.
- **Building a foundation to efficiently meet multiple compliance requirements.** Rather than tackling each compliance requirement with ad hoc controls, a security framework can provide a single, extensible foundation to meet multiple compliance requirements.
- **Discussing security with external stakeholders.** Major customers, cyber-insurance suppliers, and other business partners may have questions about an organization's security program, and security frameworks provide a structured format for discussion.

SECURITY FRAMEWORK SELECTION

Which security framework is right for your organization? The answer depends your organization's current maturity level and unique needs. A Dimensional Research study sponsored by Tenable found that in the U.S., the four most popular frameworks are PCI DSS (PCI), ISO/IEC 27001/27002 (ISO), CIS Critical Security Controls (CSC), and NIST's Framework for Improving Critical Infrastructure Cybersecurity (CSF). The research also found that organizations that use a security framework typically use more than one on average. In some cases, different frameworks were used by different parts of an organization. In other cases, a single part of an organization was using multiple frameworks.

Adopting a security framework is rarely like buying off-the-shelf clothes from a local retailer. Instead, most organizations tailor frameworks to meet their specific situation. For example, an organization could use CSF or ISO to guide risk assessment and use CSC to prioritize technical control implementation.

AUTOMATE EFFECTIVE CONFORMANCE

Tenable.sc enables you to measure, visualize, and effectively communicate adherence to security controls. Tenable.sc automates the assessment of technical controls from ISO/IEC 27001/27002, NIST Cybersecurity Framework, and CIS Critical Security Controls to ensure they are in place and operating effectively.

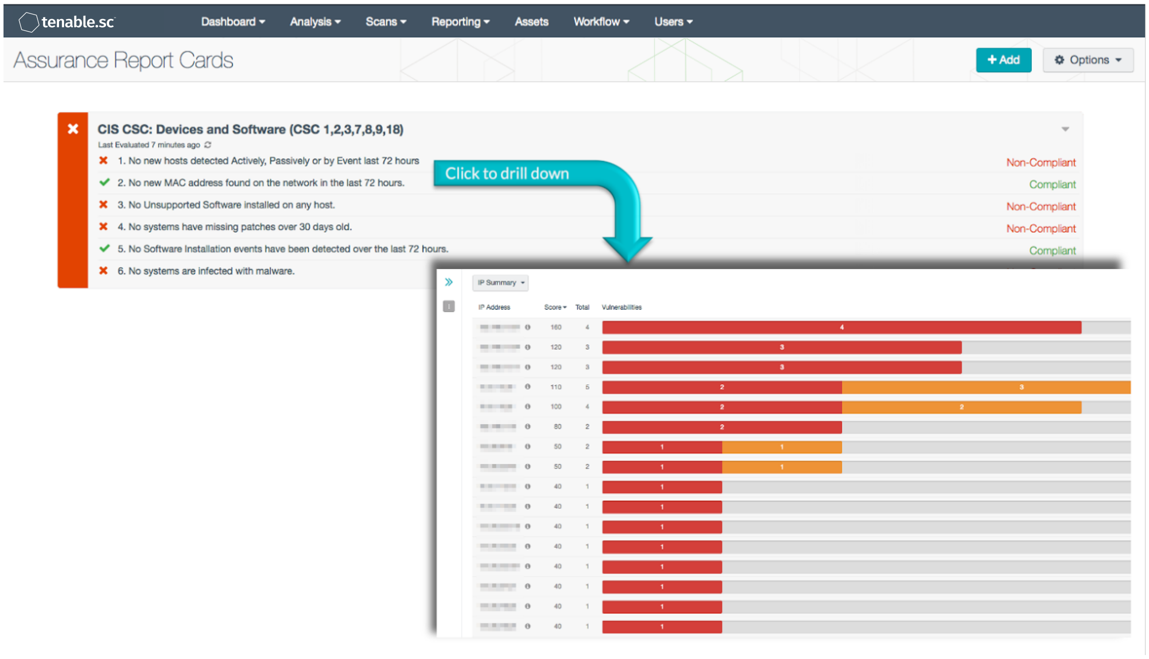
Tenable.sc will fit your specific needs. It delivers broad and continuous coverage across your entire environment, including physical, virtual, cloud, and mobile devices used in IT and industrial control networks. Dynamic asset lists let you logically segment, manage, and report on the status of specific systems, such as those used for processing EU personal data or for processing payment card data. Intelligent connectors to your existing IT and security products audit configurations and analyze events to identify control weaknesses.

COMMUNICATE SECURITY STATUS

Tenable.sc provides fully customizable reports, dashboards, and Assurance Report Cards (ARCs) specific to the leading security frameworks – 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 easily create specific reports, dashboards, and ARCs for individual lines of business.

The data that Tenable.sc gathers and analyzes for security frameworks is often the same data you need for compliance reporting. You can use compliance report templates to present the data in the formats required by multiple compliance standards. The result: redundant controls are eliminated, and the work required by each audit is reduced.

Tenable reports, dashboards, and Assurance Report Cards demonstrate adherence with best practice security controls to external business partners and large customers that may have the right to audit your security program.



Assurance Report Cards

✖ **CIS CSC: Devices and Software (CSC 1,2,3,7,8,9,18)**

Last Evaluated 7 minutes ago

✖ 1. No new hosts detected Actively, Passively or by Event last 72 hours	Non-Compliant
✓ 2. No new MAC address found on the network in the last 72 hours.	Compliant
✖ 3. No Unsupported Software installed on any host.	Non-Compliant
✖ 4. No systems have missing patches over 30 days old.	Non-Compliant
✓ 5. No Software Installation events have been detected over the last 72 hours.	Compliant
✖ 6. No systems are infected with malware.	

IP Address	Score	Total	Vulnerabilities
[redacted]	160	4	4
[redacted]	120	3	3
[redacted]	120	3	3
[redacted]	110	5	2 3
[redacted]	100	4	2 2
[redacted]	80	2	2
[redacted]	50	2	1 1
[redacted]	50	2	1 1
[redacted]	40	1	1
[redacted]	40	1	1
[redacted]	40	1	1
[redacted]	40	1	1
[redacted]	40	1	1
[redacted]	40	1	1
[redacted]	40	1	1
[redacted]	40	1	1

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

ARCs complement Tenable's 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 provide you the ability to:

- Measure, visualize, and effectively communicate the technical security controls that help you manage risk.
- Communicate security status to internal and external stakeholders.
- Understand the context you need to prioritize remediation.

TENABLE.SC SECURITY FRAMEWORK CAPABILITIES

- **Multiple Framework Support** - Select the right controls for your organization from ISO/IEC 27001/27002, NIST Cybersecurity Framework, or CIS Critical Security Controls
- **Conformance Assessment** - Automate the assessment of technical controls to determine what is in place and operating effectively.
- **Continuous Monitoring** - 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**