NIST SP 800-171 & Tenable

Streamline Control Assessment

SecurityCenter Continuous View® Security NIST SP 800-171 Capabilities

- **Conformance Assessment** - Automate the assessment of most NIST SP 800-171 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 near 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 NIST SP 800-171 reports, dashboards and Assurance Report Cards to evaluate and communicate security status

External service providers that process, store or transmit Controlled Unclassified Information (CUI) or Covered Defense Information belonging to the U.S. federal government must safeguard that CUI. These nonfederal service providers include contractors, subcontractors and service providers. Additionally, CUI is often provided to, or shared with, state and local governments, colleges and universities, and independent research organizations. NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, defines the type of security requirements service providers are likely to be contractually obligated to meet to safeguard CUI confidentiality.

Challenges of Safeguarding CUI and Covered Defense Information

NIST SP 800-171 promises to promote standardization across the previous differing regulations and conflicting guidance that in the past, often resulted in confusion and inefficiencies. However, that does not mean that 800-171 compliance is without challenges. Conforming to any security standard involves education and training, resources, and technical and other challenges. Best practices include applying project management disciplines to manage the undertaking and overcome the specific challenges discussed below.

Readiness Assessments: Prior to information system deployment, security assessments are required to prove that safeguards comply with NIST SP 800-171 or with alternative, but equally effective, security measures. If you self-assess, you must support these security assessments with comprehensive documentation to demonstrate that required controls are implemented correctly, operating as intended and producing the desired outcome. Assessing administrative controls, such as documenting security awareness training, can be manually documented. But realistically, you must automate technical control assessment.

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 the inevitable issues are discovered, you must communicate them internally and implement corrective action.

Control Consolidation: If your organization is one of the many with multiple compliance requirements, you are forced to dedicate an inordinate amount of resources to generating documentation for auditors. This is especially costly if you are using multiple systems to monitor, assess and report across multiple compliance domains. Wherever possible, you need a common set of controls and “multilingual” reporting that documents control status using domain specific language.

Metrics: You must identify metrics to assess control effectiveness and to efficiently communicate status to various internal and external stakeholders. The metrics must be appropriate for differing audiences. Technical staff needs detailed information and will take the time to understand the details. Conversely, management needs high level metrics they can review in seconds, not minutes.

Automate Control Monitoring and Assessment

Tenable SecurityCenter Continuous View® (SecurityCenter CV™) enables you to measure, visualize and effectively communicate adherence to most NIST SP 800-171 technical security controls. It achieves this by automating their operation, monitoring and assessment to ensure they are implemented correctly, operating as intended and producing the desired outcome.

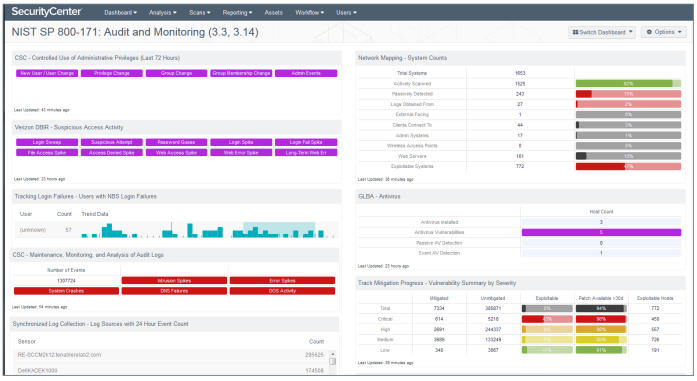
SecurityCenter CV will fit your specific needs. It delivers broad and continuous coverage across your entire environment, including physical, cloud, virtualized and mobile systems used in IT and industrial control networks. Dynamic asset lists enable you to logically segment, manage and report on the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

Monitor, Assess and Communicate

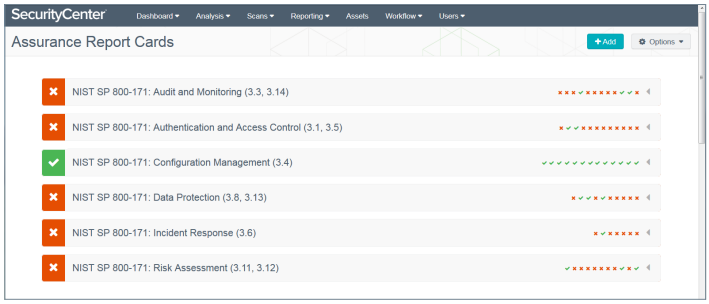
Executives, auditors and contracting officers are now scrutinizing security more than ever. You must provide them with the information they need, when they need it, without spending your time manually analyzing and summarizing data.

SecurityCenter CV provides fully customizable reports, dashboards and Assurance Report Cards (ARCs) specific to NIST SP 800-171 – 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 government agencies that may have the right to audit your security program.



Interactive dashboards consolidate information that you can quickly drill into



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

ARCs complement the Tenable comprehensive data collection approach, using 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 business partners and other external stakeholders
- Understand the context you need to prioritize remediation

About Tenable

Tenable Network Security transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats, and reduces exposure and loss. With more than one million users and more than 20,000 enterprise customers worldwide, organizations trust Tenable for proven security innovation. Tenable's customers range from Fortune Global 500 companies, to the U.S. Department of Defense, to mid-sized and small businesses in all sectors, including finance, government, healthcare, higher education, retail and energy. Transform security with Tenable, the creators of Nessus and leaders in continuous monitoring, by visiting tenable.com.

tenable™

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