Automating NIST SP 800-171 Requirements with Tenable SecurityCenter Continuous View®

October 10, 2016

Table of Contents

I. Introduction

Tenable Network Security, Inc. serves customers worldwide, and each of our customers has a unique set of security and compliance requirements. This paper provides insight to how Tenable™ addresses the National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-171, "*Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*".

Specifically, this paper describes how Tenable SecurityCenter Continuous View® (SecurityCenter CV™) can help meet the guidelines and practices outlined in NIST SP 800-171. Non-government organizations can use this publication as a guideline for protecting controlled unclassified information (CUI) that they handle. Tenable's solution is scalable across all organizational sizes and can be adapted for specific use across multiple industries.

What is NIST SP 800-171

NIST SP 800-171 was released in June 2015 as a result of the Federal Information Security Modernization Act (FISMA), and is intended for non-government organizations as recommended guidelines for protecting CUI. It has been recognized that the federal government is utilizing third parties to complete multiple objectives. This publication offers those third parties guidelines for the acceptable protection of CUI. This is done across 14 CUI security requirements:

- Access Control
- Awareness and Training
- Audit and Accountability
- Configuration Management
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical Protection
- Risk Assessment
- Security Assessment
- System and Communications Protection
- System and Information Integrity

Tenable's Solution

SecurityCenter CV is Tenable's market-defining continuous network monitoring solution, providing the most comprehensive and integrated view of network health. It integrates vulnerability and threat management helping security and compliance teams to find vulnerabilities, the threats that exploit them and systems already compromised with pinpoint accuracy. This facilitates forensic and incident responses across traditional, virtual, mobile and cloud infrastructures. Tenable SecurityCenter CV enables this capability through five unique sensors:

Active Scanning – Active scanning examines the devices on the network, running processes and services, configuration settings and vulnerabilities. Periodically scanning the network, servers, desktops and applications helps prioritize security efforts to mitigate threats and weaknesses.

Intelligent Connectors – Intelligent connectors improve efficiency and provide context by leveraging existing infrastructure and investments, as well as systems of record, to build an intelligent fabric of information. Tenable analyzes this information to prioritize threats and weaknesses, using a wide range of data sources, including Active Directory, configuration management databases (CMDBs), patch management systems, mobile device management (MDM) systems, cloud platforms, endpoint management platforms and threat intelligence.

Agent Scanning – With companies encouraging and enabling employee mobility, corporate devices aren't always connected to the corporate network when active scans take place. Agent scanning makes it possible to scan these and other transient devices. Once installed, agents can run credentialed scans without needing ongoing host credentials. Scanning with agents has minimal network impact, enabling large-scale concurrent scanning so organizations can quickly and efficiently get scan results.

Passive Listening – With increasing mobile and transient network devices, it is important to have a system in place that continuously monitors traffic, devices, applications and communications across environments. Knowing when hosts come online and taking a zero-touch approach to assess them, Tenable enables powerful, yet non-disruptive, continuous monitoring of your network.

Host Data – Tenable enables hosts to play a part in their own security hygiene, reporting on changes in their state and security posture. This is important, because most organizations can only run scans periodically. For example, if an organization scans every 29 days, they miss what happens in between. Without having to run scans, Tenable analyzes host activity, users and changes, to provide context around vulnerabilities, malicious activity and anomalous behavior.

Together these sensors enable continuous network monitoring and critical context to facilitate a proactive security program.

II. SecurityCenter CV and the NIST SP 800-171 Requirements

SecurityCenter CV Dashboards

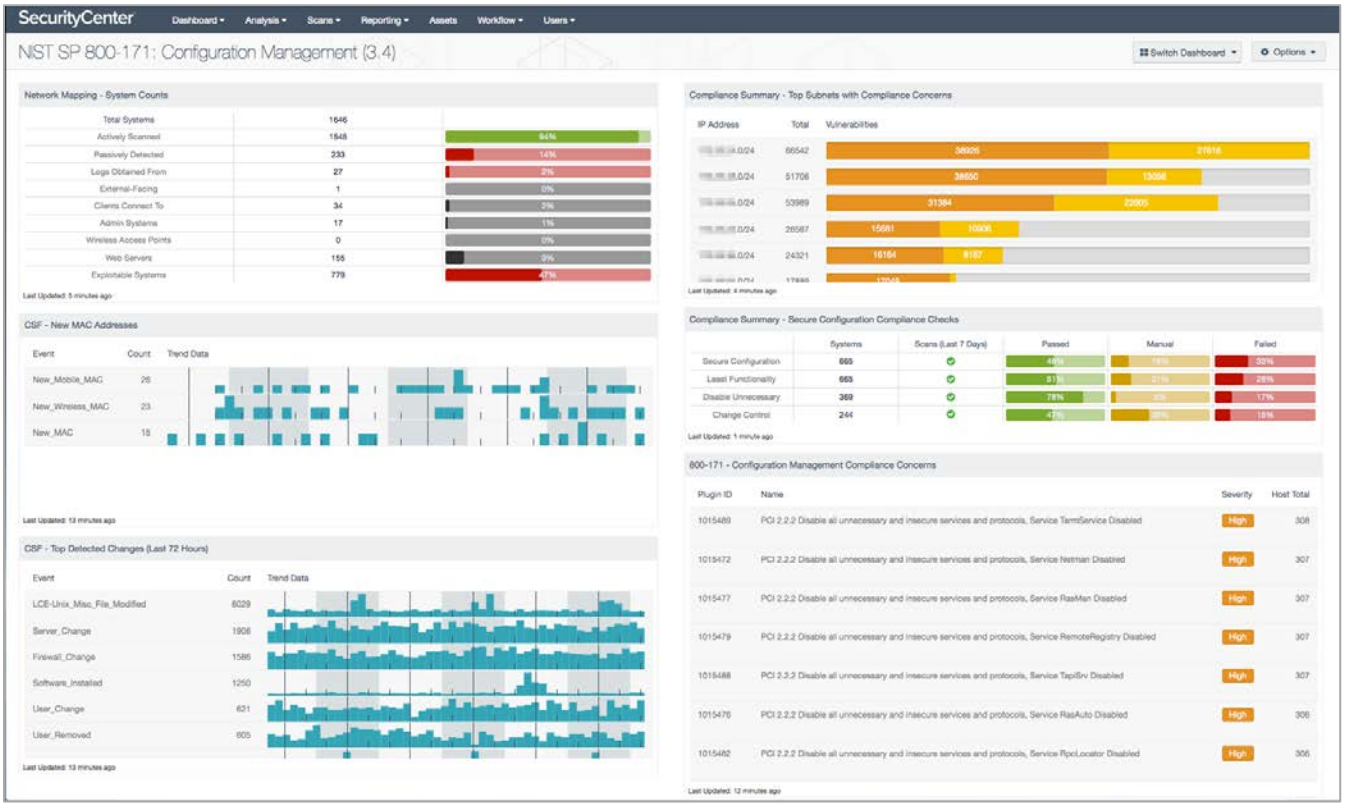
SecurityCenter CV enables organizations to automate many of NIST SP 800-171's technical requirements by providing continuous network monitoring as a robust solution that addresses their scope. These capabilities are used together with risk classification, assessment and mitigation in a scalable enterprise management system. When an organization decides to implement NIST SP 800-171, SecurityCenter CV makes it easier to take the step towards developing a more detailed and targeted approach by monitoring the successful implementation of the framework.

Using the "Configuration Management" requirement as an example, the first two requirements are:

3.4.1 – Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

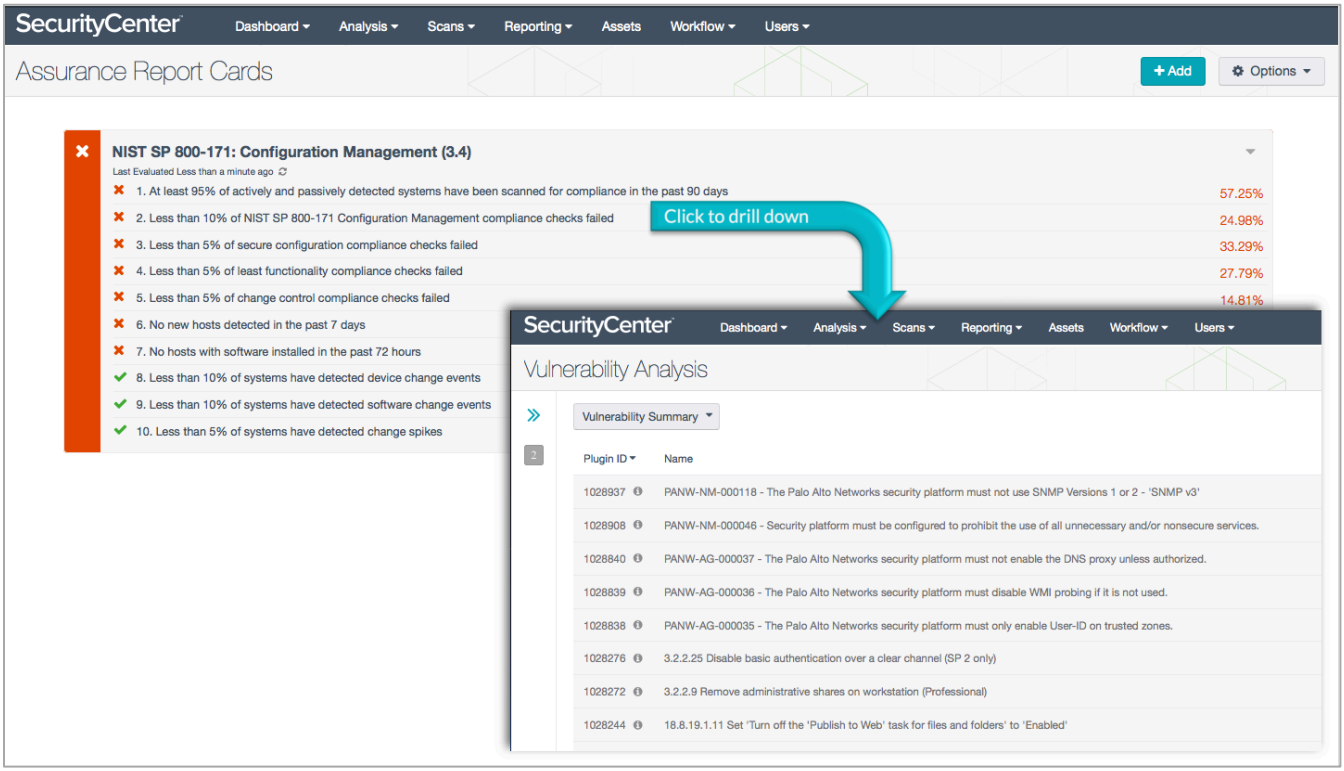
3.4.2 – Establish and enforce security configurations settings for information technology products employed in organizational information systems.

The image below contains SecurityCenter CV's "Configuration Management" dashboard. This dashboard utilizes Tenable's five sensors to provide a high-level view of an organization's environment as it relates to the NIST SP 800-171 Configuration Management requirement.



SecurityCenter CV Assurance Report Cards

In addition to dashboards, Assurance Report Cards® (ARCs) can be used to gain insight to an organization's alignment with NIST SP 800-171 guidelines. Where the dashboard provides detailed analysis and metrics concerning the requirement, ARCs provide a higher level "pass/fail" view. This is a useful deliverable for managers and higher level personnel interested in the organization's current alignment with NIST SP 800-171 guidelines. The Configuration Management ARC can be seen below.



Asset-Centric Analysis

SecurityCenter CV organizes network assets into categories based on data from a combination of network scanning, imported agent data, passive network monitoring, host data and integration with existing asset and network management tools. SecurityCenter CV can discover when there has been a change to the assets it is monitoring, such as the addition of a new server or device. Unauthorized and unmanaged hardware assets can be easily identified, and vulnerability assessments on hardware assets can be performed to determine and assess risk. Additionally, SecurityCenter CV possesses the capability of being able to dynamically assign devices to asset lists based on rules created by the organization. For example, a rule can be created to add all devices that have a specified vulnerability ID detected, in addition to specified ports that may be exploited by the vulnerability ID. This gives organizations a seemingly endless amount of possibilities for creating asset lists that pertain to multiple risk-based scenarios unique to each organization's environment.

SecurityCenter CV can also import data about remote hosts on a number of data points, including newly discovered vulnerabilities, unauthorized configuration changes, installed software and more. Software packages and installations can be searched for by keyword, allowing for easy identification of hosts that are using software with valid licenses or software that is unauthorized according to an established baseline. Information provided by SecurityCenter CV includes product name, version, patch level, vendor and more. Systems can be searched based upon the status of having unmanaged software installed, allowing administrators to easily identify and remediate outstanding issues with those systems.

Concurrent and Continuous Network Monitoring

SecurityCenter CV offers concurrent and continuous network monitoring of an organization's security posture. This is accomplished through monitoring network traffic at the packet layer to determine topology, services and vulnerabilities, as well as obtaining host vulnerability, configuration and event data. SecurityCenter CV has the ability to passively determine host file-level information in real time, which has tremendous forensics and situational awareness value. The ability to actively and passively determine all shared folder file contents can make it easier to identify potentially sensitive information on large networks.

Extensive network activity monitoring occurs through direct analysis of the packet stream. SecurityCenter CV can determine and report contextual information about each host on your network in real time, which is useful to analyze insider activity, employee activity and any type of malware or advanced threat.

Configuration Audits

A configuration audit is one where the auditors verify that servers and devices are configured according to an established standard and maintained with an appropriate procedure. SecurityCenter ships with several audit standards. Some of these come from best practice centers such as the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). Systems can also be audited according to USGCB and SCAP standards through the use of targeted audit files developed by Tenable.

In addition to the base audits, it is easy to create customized audits for the particular requirements of any organization. These customized audits can be loaded into SecurityCenter and made available to anyone performing configuration audits within an organization.

Once a set of audit policies have been configured in SecurityCenter, they can be repeatedly used with little effort. SecurityCenter can also perform audits intended for specific assets. Through the use of audit policies and assets, an auditor can quickly determine the compliance posture for any specified asset and assist in preventing misconfiguration of IT assets yet to be deployed.

III. Appendix A: Tenable Solutions for the NIST SP 800-171 Requirements

Note: Tenable SecurityCenter CV can help organizations automate many of the controls recommended for NIST SP 800-171. The examples below are not all-inclusive, and in many cases, SecurityCenter CV can be used for more in-depth coverage of a specific subcategory.

NIST SP 800-171 CUI Security Controls	How Tenable Can Help
3.1 Access Control	
3.1.1 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices.	SecurityCenter CV enables testing of servers to ensure they are configured with the proper level of access control, including separation of duties, and that accounts are configured with least needed privileges. Additionally, new users can be detected through continuous network monitoring, which SecurityCenter CV provides through powerful host analysis capabilities that facilitate an enterprise-wide search of a particular user's activity.
3.1.2 Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	SecurityCenter CV has the ability to identify the user IDs associated with specific network activity, allowing the organization to ensure that only authorized users are performing the activity.
3.1.3 Control the flow of CUI in accordance with approved authorizations.	SecurityCenter CV continuously listens to network data flows and can be configured to monitor for a number of specific data types (e.g., credit card data, patient health information, etc.) across specified network segments.
3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts. **3.1.6** Use non-privileged accounts or roles when accessing nonsecurity functions. **3.1.7** Prevent non-privileged users from executing privileged functions and audit the execution of such functions.	SecurityCenter CV performs continuous network monitoring to detect user account access and help ensure that accounts are only accessing systems they have authorization to access. This is done through continuous network monitoring utilizing Tenable's five sensors.
3.1.8 Limit unsuccessful logon attempts. **3.1.9** Provide privacy and security notices consistent with applicable CUI rules. **3.1.10** Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity. **3.1.11** Terminate (automatically) a user session after a defined condition.	SecurityCenter CV utilizes audit files that organizations can customize to their environment to ensure proper system configuration. Audit files can be used to monitor registry keys, such as the ones responsible for screensaver timeouts and session locks.

3.1.12 Monitor and control remote access sessions.	Through the use of agents, SecurityCenter CV can monitor and manage remote access to the environment. Network access, vulnerabilities and device configuration are monitored through agents that report device information back to SecurityCenter CV, even if the device is remote.
3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	Administrators can utilize audit files to monitor remote access servers to ensure they are compliant with the organization's cryptography standards.
3.1.14 Route remote access via managed access control points.	SecurityCenter CV can monitor unique asset groups (such as those identified as being used remotely) to ensure they are accessing the organization's environment through approved managed access points as opposed to rogue access points in the environment. These can be detected and reported to system administrators for further analysis.
3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information.	SecurityCenter CV utilizes agents to monitor remote devices with policies and configurations defined by the organization. Remote network access and system activity can all be logged, monitored and reported on to an organization's specifications to ensure users only have access to servers and applications to which they've been given rights to access.
3.1.17 Protect wireless access using authentication and encryption.	Organizations can utilize audit files to monitor and report on configuration settings to ensure proper authentication controls and encryption configurations are in place for wireless access. Alerts can be created and sent to necessary personnel should weak encryption or authentication settings be discovered.
3.1.18 Control connection of mobile devices.	SecurityCenter CV has the ability to monitor, analyze and report on various mobile device types and operating systems connected to the network for administrators to monitor. Mobile assets can be dynamically placed into a unique "mobile assets" group for review and analysis.
3.1.19 Encrypt CUI on mobile devices.	SecurityCenter CV has the ability to monitor and report settings of an organization's Mobile Device Management (MDM) system. Passcode, remote wipe and encryption settings can all be monitored with SecurityCenter CV policy audits.
3.1.20 Verify and control/limit connections to and use of external information systems.	SecurityCenter CV allows organizations to monitor connections to and from external information systems by source and destination IP addresses and counts connections made between them. This information is sortable by IP address or connection count to easily track connections for authorized and unauthorized use.
3.1.22 Control information posted or processed on publicly accessible information systems.	Through the use of audit files, SecurityCenter CV can continuously monitor and report on publicly accessible information systems to ensure they are properly secured and maintained. SecurityCenter CV also performs host analysis to track file and directory change events for administrators to review. Searches can be done on host, IP address or event type to ensure data is not being unintentionally exposed.

3.2 Awareness and Training	
3.2.1 Ensure that managers, system administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information systems. **3.2.2** Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities. **3.2.3** Provide security awareness training on recognizing and reporting potential indicators of insider threat.	For any security awareness program, data from Tenable's solutions can be used to provide real numbers about raw vulnerabilities, attacks and policy violations. An example of this would be reviewing reports or alerts for specified user IDs, to identify user-generated threats.
3.3 Audit and Accountability	
3.3.1 Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity. **3.3.2** Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions. **3.3.3** Review and update audited events.	SecurityCenter CV's reports of host analysis, active vulnerability assessments, imported agent data and continuous listening can all be stored for future reference. Reports can be scheduled at regular intervals, and alerts can be sent to the appropriate individuals when suspicious activity is detected. SecurityCenter CV can also monitor and report on a number of cybersecurity events unique to user IDs, making it simple for administrators to track user actions.
3.3.4 Alert in the event of an audit process failure.	SecurityCenter CV performs continuous network monitoring to report numerous network event types. For example, the "Event Indicator Alert" dashboard centralizes analysis of various network event types that may indicate compromise. For example, SecurityCenter CV can detect system errors on a syslog server and can alert administrators and analysts to the failed process.
3.3.5 Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious or unusual activity.	SecurityCenter CV provides simple and flexible reporting capabilities. These reports can be scheduled at regular intervals or run on demand, dependent on need. Organizations can also use ARCs and dashboards to track compliance to investigate unusual system activity and anomalies.

3.3.6 Provide audit reduction and report generation to support on-demand analysis and reporting. **3.3.7** Provide an information system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records. **3.3.8** Protect audit information and audit tools from unauthorized access, modification, and deletion.	SecurityCenter CV provides simple and flexible reporting capabilities. Email alerts can be used to signal discovery of vulnerabilities, audit failures and other events through host analysis. Reports can be scheduled to be sent to specified users. Organizations can also use SecurityCenter CV to create an asset group of systems designated as the authoritative time sources and monitor their configurations with SecurityCenter CV's NTP Server Detection plugin, which ensures they have the NTP configured.
3.3.9 Limit management of audit functionality to a subset of privileged users.	SecurityCenter CV includes multiple roles that have various privileges and access to different functionalities. For example, the Auditor role has access to scan summaries, dashboards, reports and logs but does not have the ability to actually run scans. Tenable's solutions enable testing of servers to ensure they are configured with the proper level of access control, including detecting configurations of servers that have not been locked down to a least level of privilege.
3.4 Configuration Management	
3.4.1 Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. **3.4.2** Establish and enforce security configuration settings for information technology products employed in organizational information systems. **3.4.3** Track, review, approve/disapprove, and audit changes to information systems.	Tenable provides a number of audit files based on the Center for Internet Security (CIS), NSA and vendor best-practice benchmarks that can be used to ensure servers are configured to be secure by default. SecurityCenter CV can be used to create audit templates unique to an organization's environment. For example, an organization can create an audit template that defines a particular server configuration, which a set of servers can then be audited against. This audit scan can be used as part of a change management program to determine authorized changes or review existing ones. Tenable's solutions enable testing of servers to ensure they are configured with the proper level of access control, including detecting configurations of servers that have not been locked down to a least level of privilege. SecurityCenter CV enables organizations to inventory authorized and unauthorized software, as well as asset discovery through continuous network monitoring.
3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.	Organizations can utilize SecurityCenter CV's audit files to report on the environment as it relates to information system and network access standards. These reports can be referred to when determining additional access or configuration changes within the environment.

3.4.6 Employ the principle of least functionality by configuring the information system to provide only essential capabilities. **3.4.7** Restrict, disable, and prevent the use of nonessential functions, ports, protocols, and services.	Tenable's scanning solutions enable testing of servers and desktops to ensure they are configured to the standard determined by the organization. SecurityCenter CV can be used to establish baseline configuration scans where subsequent scans can then report on discovered configuration changes, such as newly opened ports, unneeded services or unauthorized access. This enables organizations to find servers configured to have more functionality than needed, which can then be reconfigured for least needed functionality.
3.4.8 Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	SecurityCenter CV can implement rules to place dynamically discovered systems into an asset group for administrative review. For example, if a particular software package is unauthorized and is discovered, SecurityCenter CV can automatically place that host into an asset group for further review and analysis.
3.4.9 Control and monitor user-installed software.	The combination of active and passive analysis of the network identifies and inventories individual software and applications, such as operating systems, web browsers and office suites. The list of identified software and applications can then be evaluated to determine if any unauthorized software is present.
3.5 Identification and Authentication	
3.5.1 Identify information system users, processes acting on behalf of users, or devices. **3.5.2** Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	SecurityCenter CV can be used to manage data collected from active scans, continuous listening and host data analysis to continuously assess changes to servers, infrastructure devices, users, software and more. SecurityCenter CV can monitor and analyze system events by user IDs, making it simple for administrators to track user activity.
3.5.5 Prevent reuse of identifiers for a defined period. **3.5.6** Disable identifiers after a defined period of inactivity. **3.5.7** Enforce a minimum password complexity and change of characters when new passwords are created. **3.5.8** Prohibit password reuse for a specified number of generations. **3.5.9** Allow temporary password use for system logons with an immediate change to a permanent password.	Organizations can use SecurityCenter CV to audit Active Directory configuration settings to help ensure secure user ID and password practices. A unique customized audit file can be created to ensure AD servers are enforcing minimum password complexities, lengths and reuse. For Unix systems, SecurityCenter CV can utilize custom audit files that test for permissions of files, running processes and user access controls, such as an audit check on minimum password lengths. Additionally, SecurityCenter CV has plugins that test for default passwords that appear across a variety of Unix systems.
3.5.10 Store and transmit encrypted representation of passwords.	Organizations can use SecurityCenter CV to ensure systems that store passwords are configured with adequate encryption algorithms.

3.6 Incident Response	
3.6.1 Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities. **3.6.2** Track, document, and report incidents to appropriate organizational officials and/or authorities.	Organizations that make use of SecurityCenter CV can quickly provide a global picture of system activity to those responding to an incident. Using its five sensors: Active Scanning, Intelligent Connectors, Agent Scanning, Passive Listening and Host Data, organizations have access to a comprehensive solution in order to handle incidents. The information gathered from SecurityCenter CV's five sensors enable organizations to effectively respond to incidents with extensive network information, particularly in regards to end hosts. SecurityCenter CV offers useful workflow and ticketing solutions for alerting specified individuals when certain events occur. This also includes the ability to automate reactive measures, such as launching a scan, during certain events to quickly reassess the network in the event of an incident.
3.7 Maintenance	
3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI.	Organizations can utilize SecurityCenter CV reporting and audit file capabilities to gain a picture of system configurations and files before systems are removed from the environment for sanitizing.
3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in the information system.	SecurityCenter CV can perform checks on anti-virus software to ensure they are able to scan removable media for malicious code.
3.8 Media Protection	
3.8.1 Protect (physically control and securely store) information system media containing CUI, both paper and digital. **3.8.2** Limit access to CUI on information system media to authorized users.	SecurityCenter CV can utilize audit files to scan and report on system configurations to ensure they meet the organization's standards regarding system access and CUI access permissions.
3.8.7 Control the use of removable media on information system components. **3.8.8** Prohibit the use of portable storage devices when such devices have no identifiable owner.	SecurityCenter CV can report on USB device connections These can be reviewed by administrators to track use and to ensure removable media is not being used on systems where they are prohibited.
3.8.9 Protect the confidentiality of backup CUI at storage locations.	If electronic systems at the storage location are monitored by SecurityCenter CV, accesses to backup storage containing CUI can be monitored. Alerts can be sent out should unauthorized access be detected.

3.9 Personnel Security	
3.9.2 Ensure that CUI and information systems containing CUI are protected during and after personnel actions such as terminations and transfers.	SecurityCenter CV can utilize audit files to run scheduled reporting on system configurations. These reports can be referred to should the integrity of CUI data contained on those systems be suspected of being compromised.
3.10 Physical Protection	
3.10.1 Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals. **3.10.2** Protect and monitor the physical facility and support infrastructure for those information systems. **3.10.4** Maintain audit logs of physical access. **3.10.5** Control and manage physical access devices.	SecurityCenter CV supports facilities and the electronic systems that help physically secure them through continuous network monitoring and reporting of infrastructure system data. Assuming the systems store data in a standard format, their logs can be stored, analyzed and reported on through SecurityCenter CV for future audits or forensic investigations.
3.10.6 Enforce safeguarding measures for CUI at alternate work sites (remote work sites).	SecurityCenter CV receives remote device information sent to it through the use of agents. These agents report on a number of things such as user activity, newly discovered vulnerabilities and network monitoring. Devices at remote locations can be monitored with SecurityCenter CV in order to report on system activity, while still being controlled by the specified system access rights given by administrators.
3.11 Risk Assessment	
3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associates processing, storage, or transmission of CUI. **3.11.2** Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified. **3.11.3** Remediate vulnerabilities in accordance with assessments of risk.	SecurityCenter CV's management of active vulnerability assessments and continuous listening discovers changes in the network, such as new devices or network paths. Through continuous network monitoring changes in access control lists, running software and detected vulnerabilities can indicate when risk assessment policies and procedures need to be updated. Organizations can schedule scans at predetermined intervals to maintain updated and reviewable information on the latest detected vulnerabilities. Dashboards and reports can be used to monitor the security risks to the organization, which can then be remediated accordingly.

3.12 Security Assessment	
3.12 1 Periodically assess the security controls in organizational information system to determine if the controls are effective in their application. **3.12.2** Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information. **3.12.3** Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.	Tenable offers many ways to audit an organization's systems for vulnerabilities and configuration hardening recommendations. In addition, through the use of Assurance Report Cards (ARCs), managers and directors can create measurable goals of system monitoring, and vulnerability management to drive improvement in the organization's security posture.
3.13 System and Communications Protection	
3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.	SecurityCenter CV can analyze and report on user ID logs to track various system events by user. Additionally, system configurations can be monitored through audit files to ensure appropriate security settings and access permissions are placed on files and systems.
3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e. deny all, permit by exception).	SecurityCenter CV allows organizations to audit their firewall and proxy configurations to ensure they are configured as intended. Additionally, SecurityCenter CV can perform audits of configurations files offline as opposed to auditing critical network systems in production to avoid network disruption.
3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	SecurityCenter CV can audit the security of remote access infrastructure. A wide variety of data from remote access devices can be monitored such as the activity of remote employees who enter a network via VPN, network or dial-in connections. Agents gather configuration, vulnerability and policy information even when devices leave the network, and SecurityCenter CV can determine in real time if remote connections are encrypted in accordance with the site security policy.
3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	SecurityCenter CV can utilize audit files to monitor Active Directory system configurations to ensure they are configured to terminate or lock user sessions after a specified amount of time.
3.13.13 Control and monitor the use of mobile code.	SecurityCenter CV performs a wide variety of audits for vulnerabilities in mobile code. Examples include, but are not limited to, Java, Flash, ActiveX and PDF. SecurityCenter CV can also detect the presence of mobile code in transit across a network, and identify the systems involved in the transfer.

3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	SecurityCenter CV can be used to discover and monitor devices such as mobile phones and VoIP phones to ensure compliance with an organization's security standards and configurations.
3.13.15 Protect the authenticity of communications sessions.	Through continuous listening on a network, SecurityCenter CV analyzes data in motion and can detect unencrypted sessions. These sessions can be reported to administrators to perform proper configuration to enforce encrypted sessions.
3.13.16 Protect the confidentiality of CUI at rest.	SecurityCenter CV can utilize its five sensors to gather information about systems known to host CUI. For example, SecurityCenter CV can scan to search for sensitive data such as credit cards, names and Social Security numbers. It can also check for configuration compliance and report the compliance failings of devices known to store CUI.
3.14 System and Information Integrity	
3.14.1 Identify, report, and correct information and information system flaws in a timely manner.	SecurityCenter CV allows for coordination and communication among multiple organizational entities and departments, such as information system owners, system administrators, information security staff and risk management teams. SecurityCenter CV utilizes tens of thousands of plugins that include the latest vulnerability information. Summary reports and detailed reports can be generated and sent to groups, reducing the time for response and increasing team involvement across an organization.
3.14.3 Monitor information system security alerts and advisories and take appropriate actions in response.	SecurityCenter CV offers a comprehensive collection of dashboards, reports and ARCs for collecting and analyzing network data and alerts. It utilizes thousands of plugins that are updated with information about advanced threats, zero-day vulnerabilities and new regulatory compliance data.
3.14.2 Provide protection from malicious code at appropriate locations within organizational information systems.	SecurityCenter CV identifies malicious software and botneted systems with three very different methods. First, for Windows credentialed scans, Nessus examines the file checksum of every running process and supporting file against an industry index of the top 25 anti-virus vendors. Second, Nessus also leverages a high-quality botnet IP and DNS list to see if a scanned asset is part of a known botnet, communicating with a known botnet or configured with botnet information such as a DNS server or web content used to propagate the botnet. Finally, Nessus offers a variety of specific local and credentialed checks that identify specific malware activity, such as modification of the LMHOSTS file on Windows platforms.

3.14.4 Update malicious code protection mechanisms when new releases are available.	SecurityCenter CV can scan systems and compare hashes of running processes against and industry index of known malicious hashes. Additionally thousands of plugins are utilized by SecurityCenter CV for the most current vulnerability information. New plugins are added daily to ensure the most recent vulnerabilities are detectable by SecurityCenter CV.
3.14.5 Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	SecurityCenter CV provides continuous monitoring of organization systems to provide administrators with a detailed view of newly discovered vulnerabilities, system activity and audit checks. SecurityCenter CV uses policy audits to ensure anti-virus software is configured to the organization's standards to scan suspicious files for malicious code as they are downloaded, opened or executed.
3.14.6 Monitor the information system, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	SecurityCenter CV uses active scanning, continuous listening and host analysis to aid organizations in monitoring communications entering and leaving the environment. SecurityCenter CV continuously listens to all network traffic in real time to find new hosts, new vulnerabilities and new applications. It monitors the network for the same vulnerabilities detected by active scanning. In addition, SecurityCenter CV analyzes host data to passively detect and identify a variety of vulnerabilities.
3.14.7 Identify unauthorized use of the information system.	Organizations can monitor system access with the use of SecurityCenter CV's comprehensive monitoring capabilities. Users can search by system name or user ID in logs analyzed by SecurityCenter CV to determine if systems have been accessed by unauthorized users. Additionally, alerts can be configured to notify security teams when new users access hosts. These alerts can be reviewed for potentially unauthorized access. SecurityCenter CV can audit the security of remote access infrastructure as well as users accessing systems internally. A wide variety of data can be monitored to discover intrusions, non-compliant activity or other types of unauthorized access. For example, SecurityCenter CV can monitor the activity of remote employees who enter a network via VPN, network or dial-in connections. Agents gather configuration, vulnerability and policy information even when devices leave the network.

IV. About Tenable Network Security

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 global public sector, to mid-sized enterprises 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.