tenable network security

Real-Time FISMA Compliance Monitoring

Leveraging Asset-Based Configuration and Vulnerability Analysis with Real-Time Event Management

May 16, 2013

(Revision 8)

Ron Gula – Chief Executive Officer, Chief Technology Officer

Table of Contents

Introduction

Tenable Network Security, Inc. serves customers worldwide and each of our customers has a unique set of audit and compliance requirements. This paper provides insights gained from Tenable's customers on measuring and reporting compliance audit issues in a wide variety of industries.

Specifically, this paper describes how Tenable's solutions can be leveraged to achieve Federal Information Security Monitoring Act (FISMA) compliance by ensuring that key assets are properly configured and monitored for security compliance. It is crucial to monitor for compliance in a manner as close to real-time as possible to ensure the organization does not drift out of compliance over time. The greater the gap between monitoring cycles, the more likely it is for compliance violations to occur undetected.

For more information on FISMA requirements, please refer to the links below:

- Federal Information Security Management Act (FISMA): http://iase.disa.mil/fisma/index.html
- Federal Information Security Management Act (FISMA) Implementation Project: http://csrc.nist.gov/groups/SMA/fisma/index.html
- NIST Special Publication 800-53 Revision 4 "Recommended Security Controls for Federal Information Systems": http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- E-Government Act: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107.pdf

Background

The E-Government Act, passed into law in December 2002, recognized that information security is essential to protect the nation's economic and national security interests. Title III of the E-Government Act, the Federal Information Security Management Act (FISMA), requires United States government agencies to develop, document and implement programs to protect the confidentiality, integrity and availability of IT systems. New legislation to update FISMA passed the U.S. House of Representatives in April of 2013 and is now up for review by the U.S. Senate.

FISMA and NIST

The National Institute of Standards and Technology (NIST) has the responsibility for publishing a variety of guides for implementing security controls, performing audits and certifying systems. Some of these are very specific, such as recommended settings to harden Windows servers, while others are very generic, such as how to audit change management procedures. Many of these NIST standards have been adopted by various auditors as the model for network management. In the U.S. government, many FISMA audits specifically reference NIST guidelines. Tenable can help organizations to manage or audit their networks with NIST guidelines by several ways as outlined below.

NIST Special Publication 800-37 – Information Security

As stated in **NIST Special Publication 800-37**:

> *The revised process emphasizes: (i) building information security capabilities into federal information systems through the application of state-of-the-practice management, operational, and technical security controls; (ii) maintaining awareness of the security state of information systems on an ongoing basis though enhanced monitoring processes; and (iii) providing essential information to senior leaders to facilitate decisions regarding the acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation arising from the operation and use of information systems.*

The Risk Management Framework (RMF) has the following characteristics:

- Promotes the concept of near real-time risk management and ongoing information system authorization through the implementation of robust continuous monitoring processes
- Encourages the use of automation to provide senior leaders the necessary information to make cost-effective, risk-based decisions with regard to the organizational information systems supporting their core missions and business functions

- Integrates information security into the enterprise architecture and system development life cycle

Appendix G of the publication, “Continuous Monitoring”, states that:

> *A well-designed and well-managed continuous monitoring program can effectively transform an otherwise static security control assessment and risk determination process into a dynamic process that provides essential, near real-time security status-related information to organizational officials in order to take appropriate risk mitigation actions and make cost-effective, risk-based decisions regarding the operation of the information system. Continuous monitoring programs provide organizations with an effective mechanism to update security plans, security assessment reports, and plans of action and milestones.*

NIST Special Publication 800-53 – Security Controls

As stated in **NIST Special Publication 800-53**:

Security controls are the safeguards/countermeasures prescribed for information systems or organizations that are designed to: (i) protect the confidentiality, integrity, and availability of information that is processed, stored, and transmitted by those systems/organizations; and (ii) satisfy a set of defined security requirements.

Key questions for an organization to ask are:

- What are the security controls needed to fulfill their mission?
- Have they been properly implemented?
- Are they working?

The publication contains 18 different types of security control families such as “Contingency Planning” and “Media Protection”. Each of these controls has several specific requirements. For example, AC-7 specifies how “Unsuccessful Logon Attempts” should be handled.

How Tenable Can Help

The consensus view of Tenable’s customer base is that FISMA audits are primarily focused on describing methods used to protect data. SecurityCenter streamlines this process by enabling federal customers to easily measure vulnerabilities and discover security problems, asset by asset. In some cases, SecurityCenter also helps manage asset discovery. Some Tenable customers use the output from compliance and vulnerability scans to fulfill POA&M reporting requirements.

Specifically, Tenable also provides several configuration audit policies based on various publications from NIST, the NSA and Tenable’s interpretation of typical FISMA audit questions. These audit files are a generic baseline and are not intended to certify compliance without modification for the organization’s specific requirements. In some cases, Tenable has helped customers convert their corporate-wide configuration guides into repeatable audits that can be scheduled with SecurityCenter.

“Appendix A” details exactly which control mechanisms can be monitored or audited by Tenable’s solutions. Note that some of the NIST controls are related to requirements that cannot be monitored by Tenable’s solutions. For example, Tenable’s solutions cannot ensure that cables and servers are physically secured behind a locked access point. However, if the access is electronically logged, this activity can be monitored by the Log Correlation Engine (LCE).

NIST Special Publication 800-92 - Guide to Computer Security Log Management

This publication identifies specific recommendations that enterprise organizations must follow when performing log analysis. In the executive summary, the publication recommends that organizations must:

- Establish policies and procedures for log management
- Prioritize log management appropriately throughout the organization
- Create and maintain a secure log management infrastructure
- Provide proper support for all staff with log management responsibilities

- Establish standard log management processes for system-level administrators

Tenable's LCE and SecurityCenter can help any organization achieve these goals. Once an organization knows which logs and devices need to be collected, Tenable can provide the agents and processing power to implement the collection. This can be done as securely as deemed necessary by an organization. Tenable's solutions are very scalable and require little effort to maintain. This brings the power of log analysis directly into system administrators' hands, without requiring a learning curve for a new log analysis tool. When all logs are gathered and analyzed by one or more LCEs, it is easy to place controls on how long logs are to be stored and how they should be disposed of.

Tenable's LCE has the ability to store, compress and search any type of ASCII log that is sent to it. Searches can be made with Boolean logic and limited to specific date ranges. There are an infinite number of searches that can be performed, such as searching DNS query records or tracking down known Ethernet (MAC) addresses in a switch, DHCP and other types of logs. All search results are saved in a compressed format along with a checksum so that they can be used as forensic evidence. Previous searches can also be re-launched against the latest logs.

Each LCE can use a local disk store or a mounted file system from a remote NAS or SAN. SecurityCenter can show the disk space usage of each LCE client.

NIST SCAP Program

Tenable is participating in the NIST Security Content Automation Program (SCAP). This program uses an XML document that contains OVAL specifications for configuration audits. These documents are created in a format known as the Extensible Configuration Checklist Description Format (XCCDF).

Tenable has developed the xTool, which generates SCAP-certified content audits as well as SCAP OVAL, XCCDF, CyberScope LASR, ASR, and ARF reports from the scan results. These audit files can be used with Nessus or SecurityCenter to then perform specific types of audits based on NIST standards.

SecurityCenter and Nessus have the ability to log into Windows, Linux, and Unix hosts and perform patch and configuration audits. Tenable has produced audit policies that test systems for recommendations based on NIST settings. These are distributed with SecurityCenter and can also be modified as required by the organization.

Auditing Concerns

Many of Tenable's customers need to perform audits for multiple standards. Often, these standards have common audit points and customers can reuse collected data from one audit to facilitate another. This saves time and money, and reduces interruption to an operating network and staff.

Performing Simultaneous and Real-Time Audits

Many Tenable customers have expressed a desire for real-time compliance monitoring. This enables organizations to proactively correct compliance violations before they become a problem. If violations are detected and corrected prior to an actual audit, the audit results will reflect positively on the organization.

Avoiding Auditor Ambiguity

A common problem across Tenable's customer base is the concept of "auditor ambiguity", where the auditor does not fully understand the intent of a requirement. To minimize repeated audits for the same types of data, large enterprises often undergo an exercise to agree on a corporate set of standards for everything from building new laptops to making firewall changes. Often, these audits are very detailed and time consuming.

The problem arises when a set of human auditors needs to read these guidelines and interpret their results. Confusion or incorrect interpretation of these guidelines can cause organizations that are in compliance to potentially fail their audits.

For example, consider a simple password policy requiring that passwords be changed every 90 days. An organization that enforces password changes every 45 days is technically not in compliance with the policy, even though the 45-day requirement is more stringent. This could cause ambiguous results from an audit. One auditor may interpret this as exceeding the guideline of 90-day expiration and consider this acceptable. However, another auditor may feel that the extra burden of more frequent password changes reduces efficiency and could increase downtime or help-desk calls.

Tenable's Solutions

Tenable offers a variety of methods to detect vulnerabilities and security events across the network. Tenable's core technology is also extremely powerful for conducting network compliance audits and communicating the results to many different types of end users.

Core Solution Description

Tenable offers four integrated technologies that create our solution:

- **SecurityCenter** – Tenable's SecurityCenter provides continuous, asset-based security and compliance monitoring. It unifies the process of asset discovery, vulnerability detection, log analysis, passive network discovery, data leakage detection, event management and configuration auditing for small and large enterprises.

- **Nessus** – Tenable's Nessus vulnerability scanner is the world-leader in active scanners, featuring high-speed discovery, asset profiling, and vulnerability analysis of the organization's security posture. Nessus scanners can be distributed throughout an entire enterprise, inside DMZs and across physically separate networks. Nessus is currently rated among the top products of its type throughout the security industry and is endorsed by professional security organizations such as the SANS Institute. Nessus is supported by a world-renowned research team and has one of the largest vulnerability knowledge bases, making it suitable for even the most complex environments.

- **Log Correlation Engine** – Tenable's Log Correlation Engine (LCE) aggregates, normalizes, correlates and analyzes event log data from the myriad of devices within your infrastructure. The Log Correlation Engine can be used to gather, compress and search logs from any application, network device, system log or other sources. This makes it an excellent tool for forensic log analysis, IT troubleshooting and compliance monitoring. The LCE can work with syslog data, or data collected by dedicated clients for Windows events, NetFlow, direct network monitoring and many other technologies.

- **Passive Vulnerability Scanner** – Tenable's Passive Vulnerability Scanner (PVS) is a network discovery and vulnerability analysis solution, delivering real-time network profiling and monitoring for continuous assessment of an organization's security posture in a non-intrusive manner. The Passive Vulnerability Scanner monitors network traffic at the packet layer to determine topology, services, and vulnerabilities. Where an active scanner takes a snapshot of the network in time, the PVS behaves like a security motion detector on the network.

The key features of Tenable's products as they relate to compliance auditing are as follows:

Asset Centric Analysis

SecurityCenter can organize network assets into categories through a combination of network scanning, passive network monitoring, and integration with existing asset and network management data tools. SecurityCenter 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.

Credentialed scans allow SecurityCenter to log into remote Windows, Unix, and Linux hosts to gather lists of software installed on those hosts. 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 includes product name, version, patch level, vendor, and more. Systems can be searched by those with unmanaged software, allowing administrators to easily identify and remediate outstanding issues with those systems.

The PVS obtains software usage information through direct traffic analysis. This unique form of software usage detection is in real-time, does not have any type of agent or network scan impact on performance or availability, and can also monitor unmanaged devices such as iPads.

The LCE can analyze system logs that indicate local configuration changes such as when software is installed, modified, or removed. It can also summarize software execution by user to ensure that any form of whitelist auditing can be performed easily and in real-time. SecurityCenter can also help inventory and manage the security vulnerabilities and configurations of the systems controlling the physical devices.

Real-time Network Monitoring

PVS delivers real-time network profiling and monitoring for continuous assessment of an organization's security posture in a non-intrusive manner. PVS monitors network traffic at the packet layer to determine topology, services, and vulnerabilities. Where an active scanner takes a snapshot of the network in time, the PVS behaves like a security motion detector on the network.

PVS has the ability to passively determine host file level information in real-time, which has tremendous forensics and situational awareness value. For large networks, being able to passively determine all shared folder contents can make identification of potentially sensitive data much easier. Sending a record of each file that was shared over the network to the LCE enables forensic analysis of employees and malware activity.

Extensive web and FTP activity monitoring occurs through direct analysis of the packet stream. By passively monitoring any HTTP or FTP transaction, PVS 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 can perform configuration audits on key assets through the use of Nessus' local checks that can log directly onto a Unix, Linux, or Windows server without the use of an installed agent.

SecurityCenter ships with several audit standards. Some of these come from best practice centers like the National Institute of Standards and Technology (NIST) and National Security Agency (NSA). Systems can also be audited according to USGCB and FDCC standards through the use of targeted audit files developed by Tenable Network Security.

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.

Security Event Audits

SecurityCenter and the Log Correlation Engine can perform the following forms of security event management:

- Secure log aggregation and storage
- Normalization of logs to facilitate analysis
- Correlation of intrusion detection events with known vulnerabilities to identify high-priority attacks
- Sophisticated anomaly and event correlation to look for successful attacks, reconnaissance activity and theft of information

Tenable ships the Log Correlation Engine with logic that can map any number of normalized events to a "compliance" event to support real-time compliance monitoring. For example, a login failure may be benign, but when it occurs on a financial asset, it must be logged at a higher priority. SecurityCenter and the Log Correlation Engine allow any organization to implement their compliance monitoring policy in real-time. These events are also available for reporting and historical records.

The Log Correlation Engine also allows for many forms of "best practice" and Human Resources (HR) monitoring. For example, unauthorized changes can be detected many different ways through network monitoring. Another useful application of the Log Correlation Engine is to determine if users recently separated from the organization are still accessing the system. All activity can be correlated against user names so that it becomes very easy to see who is doing what on the inside of the network.

Web Application Scanning

Tenable's Nessus scanner has a number of plugins that can aid in web application scanning. This functionality is useful to get an overall picture of the organization's posture before engaging in an exhaustive (and expensive) analysis of the web applications in the environment. Nessus plugins test for common web application vulnerabilities such as SQL injection, cross-site scripting (XSS), HTTP header injection, directory traversal, remote file inclusion, command execution and more.

Another useful Nessus option is the ability to enable or disable testing of embedded web servers that may be adversely affected when scanned. Many embedded web servers are static and cannot be configured with custom CGI applications. Nessus provides the ability to test these separately to save time and avoid loss of availability of embedded servers.

Nessus provides the ability for the user to adjust how Nessus tests each CGI script and determine the duration of the tests. For example, tests can be configured to stop as soon as a flaw is found or to look for all flaws. This helps to quickly determine if the site will fail compliance without performing the more exhaustive and time-consuming Nessus tests. This "low hanging fruit" approach helps organizations to quickly determine if they have issues that must be addressed before the more intensive tests are run.

Nessus also provides special features for web mirroring, allowing the user to specify which part of the web site will be crawled or excluded. The duration of the crawl process can be limited as well.

Malware and Anti-virus Auditing

Nessus 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 twenty-five 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.

In addition, Nessus has over 100 plugins that examine anti-virus software for vulnerabilities, as well as missing or outdated signatures. These cover a wide range of vendors including Trend Micro, McAfee, ClamAV, Bitdefender, Kaspersky, ESET, F-Secure, and more. The ability to audit servers to determine if anti-virus signatures are being updated properly provides a second level of protection for an organization.

Tenable also offers 12 audit policies that Nessus can leverage to determine if a particular vendor's anti-virus software is installed, currently running, and/or configured to start after system boot-up. These checks can help ensure any type of network-wide anti-virus program is working as expected and is providing the appropriate level of defense.

Both PVS and LCE offer a great capability to detect malicious software and virus outbreaks, including performing near real-time forensic investigations of virus outbreaks, identifying authentication logs associated with botnet/worm probes, and identification of shared files indicative of a virus infection. LCE also works with logs from many anti-virus vendors, which makes it much easier to investigate how an outbreak or infection occurred.

Appendix A: Tenable Solutions for NIST Special Publication 800-53 Rev. 4

Note: This section was based on the content of NIST Special Publication 800-53 Rev. 4. Only controls relevant to Tenable's solutions are described here.

The following acronyms are used:

- SC – SecurityCenter
- LCE – Log Correlation Engine
- PVS – Passive Vulnerability Scanner

NIST ID	Control Name	How Tenable Can Help
Access Control		
AC-1	ACCESS CONTROL POLICY AND PROCEDURES	Tenable's solutions test for default accounts and process logs and/or network activity to audit the access control policies in use for any type of system, application or network access control. Tenable's products can also detect changes to network access control policies through the use of repeated network scans, passive network monitoring and log analysis. Tenable's LCE provides full log aggregation, storage and search capabilities. The LCE correlates logs from a variety of devices and can generate alerts for a number of access attempt types (failure, repeated attempts, access from new device, etc.). Logs can also be associated with discrete user IDs, which facilitates tracking insider activity. SC unifies access data and provides a large number of filters to analyze user activity. The LCE can be used to perform a search for any type of ASCII log. Searches can be made with Boolean logic and limited to specific date ranges.
AC-2	ACCOUNT MANAGEMENT	Tenable's solutions can test for the presence of inactive, suspended or terminated accounts and determine if they have been disabled. The presence of the account through network and/or log analysis can also be detected.
AC-3	ACCESS ENFORCEMENT	Tenable scanning solutions enable testing of servers and desktops to ensure they are configured with the proper level of access control. This can include identification of open ports, specific services as well as user access rights. Tenable's PVS passively monitors 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.
AC-5	SEPARATION OF DUTIES	Tenable's solutions enable testing of servers to ensure they are configured with the proper level of access control, including separation of duties for default and new accounts. Tenable's LCE provides the ability to associate an IP address with a user name, which aids in monitoring insiders for separation of duties. SC can manage multiple LCEs and provides powerful log search

		capabilities across multiple LCE instances. This facilitates an enterprise-wide search of a particular user's activity. SC can define and segregate user roles so that audit users can only see events from LCEs to which they have been granted access. In addition, custom roles can be created to give users specific permissions based on their job duties. For example, a user who will be viewing vulnerability data only and not performing Nessus scans could be created with a role assigned the "View Vulnerability Data" and "No Scanning" permissions.
AC-6	LEAST PRIVILEGE	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. For example, a running service on a server can be tested to see which user privileges it is operating with. 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 with the Nessus scanner to ensure servers are configured to be secure by default.
AC-7	UNSUCCESSFUL LOGON ATTEMPTS	Nessus configuration audit policies can ensure that systems are configured to log login failures. The LCE can also be used to log all successful logins, login failures and generate appropriate alerts. LCE login failures are normalized across all applications and network devices, not just operating systems. The full log search capability provided in SC and the LCE can be used to monitor unsuccessful login attempts across the enterprise and determine a pattern of attack.
AC-8	SYSTEM USE NOTIFICATION	Tenable has solutions to audit network devices to ensure a default warning banner message is displayed before users can login.
AC-9	PREVIOUS LOGON (ACCESS) NOTIFICATION	Tenable has solutions to audit operating systems to ensure a previous login notification setting is enabled.
AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	Nessus and the PVS can be used to identify a wide variety of applications that offer data without requiring a unique user login. For example, Nessus can identify which systems are publishing PDF files over web pages that do not require a login. Similarly, the PVS can identify anonymous FTP servers hosting content.
AC-17	REMOTE ACCESS	Tenable's solutions can audit the security of remote access infrastructure for vulnerabilities. A wide variety of data from remote access devices can be monitored to discover intrusions or non-compliant activity. For example, Tenable's PVS can determine in real-time whether remote connections are encrypted in accordance with the site security policy.
AC-18	WIRELESS ACCESS	Tenable's solutions can detect unauthorized wireless devices on the network. The LCE and PVS can detect new systems attaching to the network through wireless devices. In addition, Nessus can audit end nodes for the presence of authorized and unauthorized wireless network interfaces. All of these methods used together provide corroborating methods of detection.
AC-19	ACCESS CONTROL FOR MOBILE DEVICES	Tenable's solutions include the ability to discover when new hosts are added to the network including new laptops, phones, and other mobile devices. The Nessus "Mobile Devices" plugin family provides the ability to obtain information from devices registered in a MDM and from Active

		Directory servers that contain information from MS Exchange servers. This currently includes Apple iPhone, Apple iPad, Windows Phone, and Android devices that supply version information, and have “checked in” to their respective servers in the last 3 months.
AC-20	USE OF EXTERNAL INFORMATION SYSTEMS	Tenable’s solutions use asset discovery and system analysis to detect systems that were not configured to be part of the normal infrastructure and generate alerts of their presence.
Awareness and Training		
AT-2	SECURITY AWARENESS TRAINING	For any security awareness program, data from Tenable’s products can be used to provide real numbers about raw vulnerabilities, attacks, and policy violations. Threat data on an entity’s internal and external systems can be a powerful security awareness tool. Tenable’s products also produce stunning three-dimensional views of complex data.
Audit and Accountability		
AU-2	AUDIT EVENTS	Tenable’s LCE has the ability to store, compress and search any log that is sent to it. The LCE can process any event that occurs on a network, recognize it as a macro set of minor events, or identify it as an otherwise uninteresting event occurring on a critical asset. The LCE maintains the full log record and provides a large variety of filters to aid in analysis. All search results are saved in a compressed format along with a checksum so that they can be used as forensic evidence. Previous searches can also be re-launched against the latest logs.
AU-3	CONTENT OF AUDIT RECORDS	Tenable’s LCE stores the full log of each event it receives. For configuration audits, the specific results of each audit are saved distinctly and can easily be analyzed.
AU-4	AUDIT STORAGE CAPACITY	Tenable’s LCE is able to monitor available disk space to ensure that administrators are alerted when storage capacity is in danger of being reached. Audit records can then be off-loaded to alternate storage systems to ensure audit record availability.
AU-5	RESPONSE TO AUDIT PROCESSING FAILURES	Tenable’s LCE can be configured to alert administrators when a hard disk is nearing capacity. Agents used by the LCE also report CPU, memory and disk utilization. SC also maintains a real-time status of all LCE servers and their clients. Each LCE can use a local disk store or a mounted file system from a remote NAS or SAN. SC can show the disk space usage of each LCE and also predict and alert when it will run out of disk space. The SC user interface includes a tab that displays the status of all LCE clients that are configured, indicating the LCE client activity. This helps to ensure that LCE client data is being transferred to the LCE server.
AU-6	AUDIT REVIEW, ANALYSIS AND REPORTING	Tenable’s LCE provides the ability to normalize billions of log events, store, compress and search any type of ASCII log that is sent to it for

		correlated events of interest or to detect anomalies. The LCE has the ability to import syslog data from multiple sources in order to analyze data from past change-control events. The LCE can also accept logs from Tripwire and correlate these events with suspicious events and IDS attacks. Searches can be made with Boolean logic and limited to specific date ranges. There are an infinite number of searches that can be performed, such as searching DNS query records or tracking down known Ethernet (MAC) addresses in switch, DHCP and other types of logs. All search results are saved in a compressed format along with a checksum so that they can be used as forensic evidence. Previous searches can also be re-launched against the latest logs.
AU-7	AUDIT REDUCTION AND REPORT GENERATION	Tenable's LCE retains the entire log record and provides a number of filters and analysis tools to simplify log analysis and generate concise reports. All logs are normalized into convenient types that align with common reporting requirements such as login failures, software installations, compromises and port scans. Any report can be exported via a CSV spreadsheet or PDF. The full log search capability provided in SC and the LCE provides the ability to quickly summarize events across the entire enterprise. All search results are saved in a compressed format along with a checksum so that they can be used as forensic evidence. Previous searches can also be re-launched against the latest logs. This enables users to quickly update a desired search pattern with the latest data.
AU-8	TIME STAMPS	All events arriving at the LCE are uniquely time-stamped.
AU-9	PROTECTION OF AUDIT INFORMATION	SC users can only access resources and see vulnerabilities, IDS events and logs for a specific range of IP addresses that they have been explicitly assigned. Resource assignment is hierarchical, which means that created users may only inherit a subset of the resources and permissions of the "creating" user.
AU-10	NON-REPUDIATION	Tenable's LCE provides the ability to track multiple log types from a variety of devices, including NetFlow data, firewall logs, operating system logs and even honeypot logs. This can help build a better picture of what has occurred during an event where some logs could be forged at the source. All this data can be searched and corroborated from SC. All search results are saved in a compressed format along with a checksum so that they can be used as forensic evidence. The LCE also performs real-time MD5 checksum file integrity monitoring that can ensure that log data is not modified after capture.
AU-11	AUDIT RECORD RETENTION	SC and the LCE provide two choices to save all LCE data: "save-all" and "archive-directory". The "save-all" option saves all LCE data to a specified flat file on the LCE system. This option provides the ability to rotate and archive log files. The "archive-directory" option saves all log data in a compressed format on the LCE that may be searched from the SC console. This option includes a script to monitor disk use and generate an alert if resources reach a configurable threshold.

Security Assessment and Authorization		
CA-2	SECURITY ASSESSMENTS	Tenable's Nessus vulnerability scanner is the world-leader in active scanners, featuring high speed discovery, configuration auditing, asset profiling, sensitive data discovery and vulnerability analysis of your security posture. The Nessus vulnerability scanner contains over 55,000 plugins with new ones added on a daily basis to scan for the latest configuration issues and vulnerabilities for a wide variety of applications and OS platforms.
CA-3	SYSTEM INTERCONNECTIONS	Tenable's LCE and PVS provide real-time monitoring of network connections and trust relationships through direct network analysis, NetFlow analysis and log analysis. These connections can be reviewed for compliance with known policies or simply monitored for suspicious activity.
CA-7	CONTINUOUS MONITORING	All of Tenable's products can be used to monitor a wide variety of security controls. Log analysis, configuration audits, vulnerability remediation and many other types of controls can be routinely accessed by Tenable products. Tenable's PVS provides real-time monitoring through passive analysis of network traffic. The PVS has about 5,600 standard plugins to detect vulnerabilities and 500 optional plugins to detect policy abuses.
CA-9	INTERNAL SYSTEM CONNECTIONS	SC, PVS, and LCE have the ability to monitor active connections and connection attempt logs between internal systems. In addition, Nessus can perform a variety of application tests to determine internal IP addresses that may be private, and assist with mapping an internal network.
Configuration Management		
CM-1	CONFIGURATION MANAGEMENT POLICY AND PROCEDURES	Tenable's products can help detect and measure violations to an established configuration management policy. SC can be used to assess specific asset classes of servers or network devices with specific audits. Similarly, real-time network analysis can discover new hosts as well as hosts operating outside of configuration guidelines. Audits are performed entirely with credentials and do not require the use of an agent. Audits are available to be performed against: • Windows 2000, XP, 2003, Vista, 2008, 7, and 8 • Red Hat, Solaris, AIX, HP-UX, Debian, SuSE and FreeBSD • Oracle, MySQL, MS SQL, DB2, and PostgreSQL databases • Applications such as IIS, Apache, Nessus and more Tenable's list of pre-configured configuration audit policies include but are not limited to: • FDCC, USGCB, and SCAP audits • DISA STIG and Checklist audits • CIS audits for Unix, Linux, and Windows • Microsoft vendor recommendations • PCI DSS configuration setting
CM-2	BASELINE CONFIGURATION	Tenable's SC can help discover the baseline of a network footprint with active and passive vulnerability analysis. If a baseline is already known, it can be loaded into SC for reference and monitoring. Tenable also offers

		many different tools to create audit policies from existing “Gold Build” or “new” corporate server or desktop images.
CM-3	CONFIGURATION CHANGE CONTROL	Any configuration changes in the network can be detected through real-time network and log monitoring, as well as through subsequent vulnerability and configuration audits.
CM-4	SECURITY IMPACT ANALYSIS	As configuration changes occur, SC can be used to manage data collected from ongoing network scans, passive network monitoring and log analysis to continuously assess the level of risk. The LCE has the ability to import syslog data from multiple sources in order to analyze data from past change-control events.
CM-5	ACCESS RESTRICTIONS FOR CHANGE	The LCE can be configured to log access control changes on specific servers. Users can also leverage SC to audit the configurations of key assets to determine if they have the proper access control settings. SC can be used to search the full log data from multiple LCEs, providing an enterprise-wide view of logged activity. The PVS can detect new hosts, new ports, new services and new vulnerabilities as they appear on the network.
CM-6	CONFIGURATION SETTINGS	SC and Nessus can be used to perform agent-less configuration audits to determine if systems are configured in compliance with a variety of industry standards. Users can customize audit files to conform to local configuration policy.
CM-7	LEAST FUNCTIONALITY	SC can quickly identify if an asset class is not supposed to have a specific setting, running service or open port. For example, for an asset class of “DMZ Web Server”, SC can list all open ports, installed software and running applications. Any system in this asset class configured differently would be instantly recognized. Similarly, all running processes and network daemons can be audited to see what system user they operate as.
CM-8	INFORMATION SYSTEM COMPONENT INVENTORY	The combination of active and passive analysis of the network aids in individual component identification. SC can categorize assets into groups by component type, hardware specifications, software specifications, or physical location.
CM-9	CONFIGURATION MANAGEMENT PLAN	SC can be used to assist with the design and implementation of a configuration management plan, define the configuration items for multiple types of information systems, and manage the configuration of such items.
CM-11	USER INSTALLED SOFTWARE	SC can find new types of software installed by users as well as monitor network traffic and logs to discover newly installed applications. Similarly, the LCE identifies when any system (desktop or server) has new software installed on it, including updates to existing software. The full log search capabilities of SC and the LCE provide an enterprise-wide view of new installations.
Contingency Planning		
CP-6	ALTERNATE STORAGE SITE	SC can be used to monitor alternate storage sites to ensure that they are secure and are running the same software versions as the primary site. Storage sites are often not maintained with the same level of diligence as

		primary processing sites. This can lead to problems if it needs to be used for storage or backup retrieval. Ongoing monitoring with SC can ensure that the alternate site contains the required resources to obtain backups and prevent additional downtime.
CP-7	ALTERNATE PROCESSING SITES	SC can be used to monitor alternate processing sites to ensure that they are secure and are running the same software versions as the primary site. Backup sites are often not maintained with the same level of diligence as the primary site. This can lead to problems if it needs to be deployed as the operational site. Ongoing monitoring with SC can ensure that the alternate site contains the required resources to resume operations with minimal downtime.
CP-10	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	SC is a valuable tool in the system recovery process that provides a record of the vulnerabilities, configuration settings and installed software that existed on a host prior to its reconstitution. SC can also be used to scan recovered systems for vulnerabilities and to ensure the latest patches and appropriate configuration settings have been deployed. Finally, SC can be used to monitor for signs of repeat attacks.
CP-11	ALTERNATE COMMUNICATIONS PROTOCOLS	Adding to the long-standing IPv6 capabilities of Nessus, both SC and PVS also support IPv6, including dual stack IPv4/IPv6 environments. Combined, Tenable's solutions create the only truly comprehensive IPv6 vulnerability assessment and management suite in the industry.
Identification and Authentication		
IA-2	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	Any system that logs user activity by user name also produces access control (login and login failures) logs. These can be used for log analysis, raw pattern searches and anomaly detection by the LCE. The LCE also provides the ability to associate an IP address with a user name and log if a user changes IP addresses. SC can be used regularly scan for default user accounts and to search the full log data from multiple LCEs, providing an enterprise-wide view of user activity.
Incident Response		
IR-1	INCIDENT RESPONSE POLICY AND PROCEDURES	SC can be used as a communications platform for all shareholders involved in the incident response process, and can be used to help define organizational incident response policies and procedures. SecurityCenter will contain a large amount of information on the targeted systems, and identifying the applications, the underlying operating systems, and even the organization in charge of a system can often shape incident response procedures.
IR-4	INCIDENT HANDLING	SC 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. Summary reports and detailed reports can be generated and sent to groups, reducing the time for response and increasing team involvement across an organization.
IR-5	INCIDENT MONITORING	SC is designed to automatically monitor systems and networks for potential security incidents and generates alerts accordingly. SC correlates many types of data along with known system configuration and vulnerabilities to reduce false positives and detect anomalies that could indicate a pending attack.

IR-6	INCIDENT REPORTING	Tenable's LCE provides the ability to normalize multiple log types from a variety of devices, including NetFlow data, firewall logs, operating system logs, process accounting, user maintenance and even honeypot logs. This can help build a better picture of what has occurred during an event where some logs could be forged at the source. The LCE can store, compress and search any type of ASCII log that is sent to it for correlated events of interest or to detect anomalies. The LCE can also accept logs from Tripwire and correlate these events with suspicious events and IDS attacks. Tenable also ships a wide variety of configuration audit policies that can be used to ensure that the sources of log data are correctly configured to send their logs. Audits currently available include: • Detection of all Windows GPO and local policy settings that refer to event logging such as audit of process creation. • Support for all types of Unix and Linux platforms to ensure that syslog is enabled and logging correctly. • The ability to audit the LCE client that is installed at the host generating logs. SC can manage multiple LCE instances. Users' searches occur across all LCEs that they have access to or can be narrowed down to a single LCE as well. All search results are saved in a compressed format along with a checksum so that they can be used as forensic evidence. Previous searches can also be re-launched to update the log data.
IR-7	INCIDENT RESPONSE ASSISTANCE	Organizations that make use of SC and the LCE can quickly provide a global picture of system activity to those responding to an incident. The PVS is also useful for discovering up to the minute configuration data on potentially compromised hosts. SC provides the ability to save all LCE data from a suspected incident in a separate report that aids in the analysis phase of incident response. All search results are saved in a compressed format along with a checksum so that they can be used as forensic evidence. Previous searches can also be re-launched to update the log data.
Maintenance		
MA-4	NONLOCAL MAINTENANCE	SC can be used to perform a before and after configuration audit of the systems undergoing maintenance. Log and network activity for the assets in question can also be monitored with the LCE. The PVS can determine in real-time if remote connections are encrypted in accordance with the site security policy.
Media Protection		
MP-7	MEDIA USE	Tenable's LCE Log Agent for Windows can make use of Windows Management Instrumentation (WMI) functionality to monitor local and remote systems for USB device, CD-ROM disc, and DVD disc activity. The full log search capability provided in SC and the LCE can be used to easily search and monitor USB activity across the enterprise.

Physical and Environmental Protection		
PE-2	PHYSICAL ACCESS AUTHORIZATIONS	The LCE can monitor user access by IP address and generate an alert on attempted access violations. The LCE also notes when a user changes IP addresses.
PE-4	ACCESS CONTROL FOR TRANSMISSION MEDIUM	SC can monitor the security profile of any network device that shares network access control transmission information.
PE-5	ACCESS CONTROL FOR OUTPUT DEVICES	SC can scan systems to ensure that screen lock capabilities are enabled.
PE-6	MONITORING PHYSICAL ACCESS	Any device that generates logs files for specific user data can be monitored by the LCE. Windows servers can also be monitored by the LCE for USB device usage.
Planning		
PL-8	INFORMATION SECURITY ARCHITECTURE	SC and 3D Tool can be used to map networks across multiple logical and physical segments. This provides a visual representation that can be used in the review and update of the information security architecture and the overall enterprise architecture.
Personnel		
PS-4	PERSONNEL TERMINATION	Tenable's solutions can audit the access control policies in use for any type of system, application, or network access control and test for the presence of inactive, suspended, and terminated to determine if they have been disabled. The presence of the account through network and/or log analysis can also be detected.
PS-7	THIRD-PARTY PERSONNEL SECURITY	SC and PVS can monitor connections to and from third-party and outsourced services into an organization's network, enabling the organization to better gather data about outside IT services, including account usage and hours of operation.
Risk Assessment		
RA-1	RISK ASSESSMENT POLICY AND PROCEDURES	As part of any risk assessment policy, all of Tenable's solutions can be used to monitor configurations, manage vulnerabilities, and monitor for security and compliance events. Security events and reports may be shared with authorized users to aid in coordination efforts.
RA-3	RISK ASSESSMENT	SC's management of active and passive vulnerability assessments discovers changes in the network such as new devices or network paths. Changes in access control lists, running software, and different types of detected vulnerabilities can indicate when risk assessment policies and procedures need to be updated.
RA-5	VULNERABILITY SCANNING	Tenable was founded on the belief that it is crucial to monitor systems in a manner as close to real-time as possible to ensure the organization does not drift out of compliance over time. The greater the gap between monitoring cycles, the more likely it is for vulnerabilities to be undetected. To achieve this goal, Tenable offers several technologies that can be leveraged:

		• Nessus can perform rapid network scans. A typical vulnerability scan can take just a few minutes. With SC, multiple Nessus scanners can be combined to perform load balanced network scans. • Nessus credential scans can be leveraged to perform highly accurate and rapid configuration and vulnerability audits. Credentialed scans also enumerate all UDP and TCP ports in just a few seconds. • The PVS monitors all network traffic in real-time to find new hosts, new vulnerabilities and new applications. It scans for the same vulnerabilities detected by the Nessus scanner.
Systems and Services Acquisition		
SA-3	SYSTEM DEVELOPMENT LIFE CYCLE	Through active scanning, passive scanning, and log correlation, Tenable's products can help ensure that security requirements are incorporated into organizational systems and architecture throughout the entire development life cycle.
SA-5	INFORMATION SYSTEM DOCUMENTATION	SC's asset discovery capabilities leverage both active and passive detection to help maintain an up-to-date network list. Any information about running processes, known vulnerabilities, configuration information, WMI data, system BIOS data and more can be used to classify systems into one or more different asset groups.
SA-8	SECURITY ENGINEERING PRINCIPLES	Any custom application will be built on non-custom objects such as various operating systems, databases and applications. Tenable offers many ways to audit these systems for vulnerabilities and configuration hardening recommendations. In addition, custom applications can be monitored with Nessus and many of Tenable's tools to ensure that no security issues have been added as a result of the custom application.
SA-10	DEVELOPER CONFIGURATION MANAGEMENT	SC can be used to provide independent verification of any patches or security issues in accordance with an established security and configuration management plan.
SA-11	DEVELOPER SECURITY TESTING AND EVALUATION	SC can be used to manage scans of software under development so developers can address any vulnerability in their software early in the development process. The LCE can be used to monitor any logs generated by the software, which can aid in documentation of security testing. Enterprise-wide log searches can aid in detecting anomalies in a particular application that could indicate an installation that is not in sync with the rest of the deployment. Nessus has a number of features that aid in web application scanning including: • The ability to perform a variety of web application audits to test for common web application vulnerabilities such as SQL injection, cross-site scripting (XSS), HTTP header injection, directory traversal, remote file inclusion and command execution. • The ability to send POST requests in addition to GET requests, which enables testing of HTML forms for vulnerabilities.

		• The ability to enable or disable testing of embedded web servers that may be adversely affected when scanned. • Nessus scans can be configured to stop as soon as a flaw is found or to look for all flaws. This helps to quickly determine if issues need to be addressed before running exhaustive scans. • Nessus provides special features for web mirroring, allowing the user to specify which part of the web site will be crawled or not.
Systems and Communication Protection		
SC-5	DENIAL OF SERVICE PROTECTION	SC can use Nessus to perform Denial of Service tests. The LCE can also be used to normalized IDS and other types of logs that may indicate denial of services attempts and generate an alert on the activity. SC can be used to search multiple LCEs across the enterprise to detect DoS activity.
SC-7	BOUNDARY PROTECTION	Multiple Nessus scanners can be placed across an enterprise to simulate remote network scans. This can let SC users test to see if certain parts of the network have excessive trust relationships with other parts. Logs from any system(s) monitoring the boundaries of a network can be sent to the LCE for normalization and analysis. The information collected by the LCE is further analyzed with the following methods: • All network connections are labeled by duration and bandwidth. This makes it very easy to look for long TCP sessions as well as sessions that transfer large amounts of data. • Each host on the network is statistically profiled such that if there is a change in “normal” traffic, the deviation is noted. For example, if a server had an increase in inbound network connections, a log stating this would be noted. With SC, it is very easy to sort, view and analyze this information to decide if this sort of anomaly is worth investigating. • Each flow is fed into a variety of correlation scripts that look for worm behavior, network scanning, and correlate attacks detected by a NIDS and with known “blacklisted” IP addresses and a variety of other threat monitoring rules. The PVS can also monitor traffic on boundary networks to detect if specific types of network data are being transmitted in violation of policy. For example, the PVS can detect the transmission of credit card data or personal health information, which could indicate a data loss incident.
SC-8	TRANSMISSION CONFIDENTALITY AND INTEGRITY	Tenable’s PVS can determine in real-time if remote connections are encrypted in accordance with the site security policy. SC and Nessus can be used to look for any non-encrypted services on specific assets that are supposed to use SSH or SSL for administration. If the LCE is also used to monitor servers, it can correlate network traffic with logins to see that only encrypted protocols are being used.
SC-18	MOBILE CODE	Nessus performs a wide variety of audits for vulnerabilities in mobile code. Examples include, but are not limited to, Java, Flash, ActiveX, and PDF. PVS can also detect the presence of mobile code in transit across a network, and identify the systems involved in the transfer.

System and Information Integrity		
SI-1	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES	Tenable's solutions can be used to monitor for compliance with any policies and procedures that specify configuration of key assets or how events from those assets are monitored and logged. The combination of the Nessus configuration audits, continuous traffic monitoring with the PVS and log analysis with the LCE present numerous opportunities to detect change in the monitored systems. Unauthorized change is the leading issue for degradation of server integrity.
SI-2	FLAW REMEDIATION	Nessus contains thousands of plugins with new checks added on a daily basis to scan for the latest system flaws and recommended security patch levels. This task can be automated in SC.
SI-3	MALICIOUS CODE PROTECTION	The LCE can be used to aggregate logs from a variety of virus and malware tools. In addition, SC can use Nessus to log in to network devices and servers and audit registry settings or file content to look for viruses and check to make sure the AV system is operational and updated. Nessus and the PVS also include many checks to see that systems are not distributing malicious code.
SI-4	INFORMATION SYSTEM MONITORING	The LCE provides event collection, normalization and correlation for hundreds of different types of devices. These events can be quickly searched and analyzed across large and small enterprises from a central SC. The LCE automatically analyzes any log for statistical significance, if it is evidence of a compromise or if there has been a compliance infraction. SC also uses Nessus and the PVS to actively and passively monitor network activity. SC unifies data from a wide variety of security devices to provide a correlated view of the enterprise security posture.
SI-5	SECURITY ALERTS, ADVISORIES AND DIRECTIVES	Nessus and PVS plugins are updated on a daily basis to detect the latest security vulnerabilities. SC can be configured to automatically update plugins and run scans on a daily basis to automatically detect if the network is vulnerable to reported security alerts and advisories.
SI-6	SECURITY FUNCTION VERIFICATION	With distributed scanners, SC can efficiently log into many different devices and determine if they have been secured correctly. The LCE correlates logs from a large variety of devices and can be used to monitor for security function failures such as the failure of a security test to launch.
SI-7	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY	The LCE can accept logs from file integrity solutions such as Tripwire. These events can be correlated with user logins and suspicious events or anomalies. Nessus can also be used to perform agent-less MD5 checksums of Linux and Unix servers to ensure that the file(s) being monitored have not been changed.

Appendix B: Tenable Solutions for NIST Special Pub 800-37

Note: This section was based on the content of NIST Special Pub 800-37. Only controls relevant to Tenable's solutions are described here.

The following acronyms are used:

- SC – SecurityCenter
- LCE – Log Correlation Engine
- PVS – Passive Vulnerability Scanner

NIST Task	Task Description	How Tenable Can Help
1-1	Categorize the information system and document the results of the security categorization in the security plan.	SC's asset discovery capabilities leverage both active and passive detection via Nessus and the PVS to help maintain an up-to-date network list. This includes the ability to determine when new devices have been added to the network, what their operating system or device type is, the topology of the network and what types of services these devices are running.
2-1	Identify the security controls that are provided by the organization as common controls for organizational information systems and document the controls in a security plan (or equivalent document).	Tenable's products can help detect and measure violations to an established desktop and server configuration management policy. SC can be used to assess specific asset classes of servers or desktops with specific configuration audits. Audits are available to be performed against: • Windows 2000, XP, 2003, Vista, 2008, 7, and 8 • Red Hat, Solaris, AIX, HP-UX, Debian, SuSE and FreeBSD • Oracle, MySQL, MS SQL, DB2, and PostgreSQL databases • Applications such as IIS, Apache, Nessus and more Tenable's list of pre-configured configuration audit policies include but are not limited to: • FDCC/USGCB and SCAP audits • DISA STIG and Checklist audits • CIS audits for Linux, Unix, and Windows • Microsoft vendor recommendations • PCI configuration settings
2-2	Select the security controls for the information system and document the controls in the security plan.	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. For example, a running service on a server can be tested to see which user privileges it is operating with. 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 with the Nessus scanner to ensure servers are configured to be secure by default.
2-3	Develop a strategy for the continuous monitoring of security control effectiveness and any proposed or actual	SC provides continuous, asset-based security and compliance monitoring. It unifies the process of asset discovery, vulnerability detection, log analysis, passive network discovery, data leakage detection, event management and configuration auditing for small and large enterprises.

	changes to the information system and its environment of operation.	
3-1	Implement the security controls specified in the security plan.	Tenable ships the LCE with logic that can map any number of normalized events to a “compliance” event to support real-time compliance monitoring. SC and the LCE allow any organization to implement their compliance monitoring policy in real-time. These events are also available for reporting and historical records.
4-2	Assess the security controls in accordance with the assessment procedures defined in the security assessment plan.	Tenable’s products can help detect and measure violations to an established network device and firewall configuration management policy. Specifically, Tenable solutions can be used to: • Scan networks or specific assets for a list of open ports. This can be used to test against a known access control policy. • Scan for excessive trust relationships. Multiple Nessus scanners can be placed throughout the network to perform scans from different vantage points. For example, this can test how much access a DMZ has to a developer network or vice versa.
4-3	Prepare the security assessment report documenting the issues, findings, and recommendations from the security control assessment.	When an incident is reported, having all network activity, system logs, configuration data and firewall logs at an analyst’s fingertips can help them quickly categorize the type of incident they are dealing with. When an analyst detects a potential compromise, abuse or other type of anomaly with Tenable’s products, they also have enough information to make a determination to start an incident response exercise.
4-4	Conduct initial remediation actions on security controls based on the findings and recommendations of the security assessment report and reassess remediated control(s), as appropriate.	Tenable’s solutions provide tools that can aid in the incident response process in two strategic areas. These are: • Detecting the incident • Responding quickly to an incident The ability to detect an incident efficiently and in an automated manner is often overlooked. Most automation for detecting incidents generates many false positives that make it unreliable. Tenable’s approach is to correlate many types of data along with known system configuration and vulnerabilities.
5-1	Prepare the plan of action and milestones based on the findings and recommendations of the security assessment report excluding any remediation actions taken.	Tenable was founded on the belief that it is crucial to monitor systems in a manner as close to real-time as possible to ensure the organization does not drift out of compliance over time. The greater the gap between monitoring cycles, the more likely it is for vulnerabilities to be undetected. To achieve this goal, Tenable offers several technologies that can be leveraged: • Nessus can perform rapid network scans. A typical vulnerability scan can take just a few minutes. With SC, multiple Nessus scanners can be combined to perform load balanced network scans. • Credentialed Nessus scans can be leveraged to perform highly accurate and rapid configuration and vulnerability audits. Credentialed scans also enumerate all UDP and TCP ports in just a few seconds. The PVS monitors all network traffic in real-time to find new hosts, new vulnerabilities and new applications. It scans for the same vulnerabilities detected by the Nessus scanner.

5-3	Determine the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.	SC includes trending and reporting tools that can help demonstrate the types of security deficiencies that can be fed back into a security awareness program. For example, if an organization was struggling with the requirement to apply patches within 30 days of release, then more training could be conducted about the importance of this, the risk to the organization and why the corporate policy addresses this issue. A different organization might be patching systems efficiently, but could also have a higher frequency of virus outbreaks that could indicate that more user training is in order. Tenable also offers a variety of training and certification programs for Nessus and all of our enterprise products. These certification programs can be used to ensure that your security team has the right set of training and skills to operate the Tenable products.
6-1	Determine the security impact of proposed or actual changes to the information system and its environment of operation.	SC's asset discovery capabilities leverage both active and passive detection via Nessus and the PVS to help maintain an up-to-date network list. This includes the ability to determine when new devices have been added to the network, what their operating system or device type is, the topology of the network and what types of services these devices are running. For Linux and Windows operating systems, Nessus can leverage information about running processes, known vulnerabilities, configuration information, WMI data, system BIOS data and more to classify systems into one or more different asset groups. SC can also be used to determine authorized or unauthorized devices in several different ways: • Any type of detected change can be audited. New hosts, new services and software can all be identified through SC. SC allows inspection of any vulnerability, service or node for when it was first seen or last seen. The PVS allows for real-time alerting of new hosts and finally, for any scan controlled by SC, an automatic list of "new" hosts is automatically discovered. • SC has a sophisticated method for classifying hosts. For example, corporations that leverage DNS names for authorized devices can use SC to identify nodes that do not have an official DNS record. SC can use combinations of the output of any active or passive scan to classify hosts in accordance with various types of "authorized" and "unauthorized" device lists. SC can also leverage automatic classification of hosts based on complex rules that reflect deviations from policy. For example, you could identify all Linux computers in a "Windows Only" type of environment. Another example would be to identify hosts in a DMZ that have open ports against a known policy. These types of policy violations are often related to "unauthorized" devices.
6-3	Conduct remediation actions based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in the plan of action and milestones.	Tenable was founded on the belief that it is crucial to monitor systems in a manner as close to real-time as possible to ensure the organization does not drift out of compliance over time. The greater the gap between monitoring cycles, the more likely it is for vulnerabilities to be undetected. To achieve this goal, Tenable offers several technologies that can be leveraged: • Nessus can perform rapid network scans. A typical vulnerability scan can take just a few minutes. With SC, multiple Nessus scanners can

		be combined to perform load balanced network scans. • Nessus credential scans can be leveraged to perform highly accurate and rapid configuration and vulnerability audits. Credentialed scans also enumerate all UDP and TCP ports in just a few seconds. The PVS monitors all network traffic in real-time to find new hosts, new vulnerabilities and new applications. It scans for the same vulnerabilities detected by the Nessus scanner.
6-5	Report the security status of the information system (including the effectiveness of security controls employed within and inherited by the system) to the authorizing official and other appropriate organizational officials on an ongoing basis in accordance with the monitoring strategy.	SC includes trending and reporting tools that can help demonstrate the types of security deficiencies that can be fed back into the security awareness program. For example, if an organization was struggling with the requirement to apply patches within 30 days of release, then more training could be conducted about the importance of this, the risk to the organization and why the corporate policy addresses this issue. A different organization might be patching systems efficiently, but could also have a higher frequency of virus outbreaks that could indicate that more user training is in order. Tenable also offers a variety of training and certification programs for Nessus and all of our enterprise products. These certification programs can be used to ensure that your security team has the right set of training and skills to operate the Tenable products. Finally, Tenable produces a wide variety of content for our customers to help drive any type of security awareness and training program. These include: • An active corporate blog with technical and strategic posts that focus on scanning, security auditing, log analysis, insider threat detection and more. • A user discussion portal that allows Tenable's customers to exchange ideas, tools, strategies and questions with each other. • The Tenable Support Portal, which includes many knowledgebase articles on achieving certain types of capabilities with Tenable's products. A wide variety of recorded webinars about specific product features and high level security concepts such as compliance auditing and log analysis.
6-7	Implement an information system decommissioning strategy, when needed, which executes required actions when a system is removed from service.	Tenable's products can help detect and measure violations to an established configuration management policy. This can include specification of running network services as well as specific configuration settings for an operating system or application. SC can be used to assess specific asset classes of servers or network devices with specific audits. Similarly, real-time network analysis can discover new hosts as well as hosts operating outside of configuration guidelines. SC and Nessus are certified to perform FDCC and Center for Internet Security (CIS) audits. Information systems in need of decommissioning can be identified through continuous monitoring and removed from service according to the entity's decommissioning strategy.

About Tenable Network Security

Tenable Network Security, the leader in real-time vulnerability management, is the source of the Nessus vulnerability scanner and the creator of enterprise-class, agentless solutions for the continuous monitoring of vulnerabilities, configuration weaknesses, data leakage, log management, and compromise detection to help ensure network security and compliance. Tenable's award-winning products are utilized by many Global 2000 organizations and Government agencies to proactively minimize security and compliance risk. For more information, please visit http://www.tenable.com/.

GLOBAL HEADQUARTERS

Tenable Network Security
7063 Columbia Gateway Drive
Suite 100
Columbia, MD 21046
410.872.0555
www.tenable.com