Real-Time Compliance Monitoring

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

March 11, 2014

(Revision 25)

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 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 and remain undetected.

Audit criteria vary among different industries and geographic locations. New legislation is continually being developed that changes the standards for audits in these industries. It is important to be familiar with multiple compliance standards, even if they do not seem to be required at the moment. Changing legislation or shifts in an organization's business offerings require that managers keep abreast of audit criteria in other industries.

This paper addresses the needs of security managers who are new to auditing as well as those who are experienced in the audit process. An overview is provided to illustrate how Tenable's solutions enable managers to assure compliance with all the following regulations, standards and best practice guidelines:

Compliance Requirement	Related Links
Basel II/III	http://www.bis.org/publ/bcbsca.htm http://www.bis.org/bcbs/basel3.htm
Control Objectives for Information and related Technology (**COBIT**)	http://www.isaca.org/COBIT/Pages/default.aspx
DISA Security Technical Implementation Guides (**STIG**)	http://iase.disa.mil/stigs/
Federal Information Security Management Act (**FISMA**)	http://iase.disa.mil/fisma/index.html http://csrc.nist.gov/groups/SMA/fisma/index.html
United States Government Configuration Baseline (**USGCB**)	http://usgcb.nist.gov/index.html
Gramm-Leach-Bliley Act (**GLBA**)	http://www.ftc.gov/privacy/glbact/glbsub1.htm http://www.ftc.gov/privacy/privacyinitiatives/glbact.html
Health Insurance Portability and Accountability Act (**HIPAA**) and Health Information Technology for Economic and Clinical Health (**HITECH**) Act	http://www.hhs.gov/ocr/hipaa/ http://waysandmeans.house.gov/media/pdf/110/hit2.pdf
ISO 27002/17799 Security Standards	http://www.iso.org/iso/catalogue_detail?csnumber=50297
Information Technology Infrastructure Library (**ITIL**)	http://www.itil-officialsite.com/home/home.asp
Motion Picture Association of America (**MPAA**) inquiries	http://mpaa.org/contentprotection/types-of-content-theft
National Institute of Standards (**NIST**) Special Publications	http://csrc.nist.gov/publications/PubsSPs.html

National Security Agency (**NSA**) Security Configuration Guides	http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/archived_guides.shtml
North American Electric Reliability Council (**NERC**) Standards	http://www.nerc.com/page.php?cid=2
United States Nuclear Regulatory Commission **(NRC)**	http://www.nrc.gov/
Payment Card Industry Data Security Standard (**PCI DSS**)	https://www.pcisecuritystandards.org/security_standards/documents.php
Recording Industry Association of America (**RIAA**) inquiries	http://www.riaa.com/physicalpiracy.php?content_selector=piracy_online_the_law
Sarbanes-Oxley (**SOX**)	http://www.soxlaw.com/

Additional Resources	Related Links
Data Loss Prevention (**DLP**) Laws	http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx http://www.edps.europa.eu/EDPSWEB/

It is important to apply the requirements of compliance regulations and standards to the strategic business requirements that are critical to the organization. This notion is often referred to as “Corporate Governance and IT”. The goals of running the enterprise and the goals of the various audit guidelines are often much more synchronized than people realize. Once an understanding of the various audit guidelines and best practices is achieved, mapping these into the organization’s strategic goals is much easier.

What is your compliance validation process?

Tenable’s worldwide customer base provides a broad spectrum of audit requirements that cover different technologies, legislation, policies, and procedures. There are some common baselines, but as the specific technology, procedures, and critical data vary among organizations so it follows that the validation processes will also vary.

Checkbox Compliance

Tenable’s customers often need to demonstrate compliance with “checkbox” security requirements as found in certain do-it-yourself assessments or by third party assessors. These requirements tend to be in a line item format and may contain requirements such as “maintain an Intrusion Detection System” or “enforce password complexity.” These requirements are typically mandated by specific compliance guidelines or corporate directives for the particular industry.

The Payment Card Industry Data Security Standard (PCI DSS) is a comprehensive set of security standards established by the founding members of the PCI Security Standards Council, including Visa, MasterCard, American Express, Discover Financial Services, and JCB. The PCI DSS is intended to provide a common baseline to safeguard consumer cardholder data for all bank card brands. All merchants and service providers that store, process or transmit – or could impact the security of – cardholder data must comply with the PCI standard and validate this compliance on an annual basis either by third party assessment or by self-assessment. For the millions of businesses that offer web sites to purchase products, an entire industry has developed to perform automated vulnerability scan reporting. These scans test the online systems for known vulnerabilities and produce a technical report in a format specified by the PCI standard. While vulnerability scanning is important, it is not the only component of the PCI DSS, as described later in this paper.

Performing Simultaneous and Real-Time Audits

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

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

Tenable's Solutions

Core Solution Description

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

Tenable offers four basic solutions:

- **SecurityCenter CV** – Tenable's SecurityCenter Continuous View (SCCV) 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 for immediate forensic and incident response across traditional, virtual, mobile, and cloud infrastructures. Tenable SCCV enables this capability through a unique foundation that consolidates vulnerability scan, network sniffing, and event log data in a single, unified platform. This platform provides 100% asset discovery and monitoring 100% of the time using the only security app library in the industry.

- **Nessus vulnerability scanner** – 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 software 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:

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, 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 SCAP 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 LCE 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

To support real-time compliance monitoring, Tenable ships the LCE with logic that can map any number of normalized events to a "compliance" event. 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 LCE allow any organization to implement their compliance monitoring policy in real-time. These events are also available for reporting and historical records.

The LCE 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 LCE 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 inside the network.

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 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 and also predict and alert when it will run out of disk space.

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, and command execution.

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.

Tenable and Basel

Background

Basel II is a banking compliance standard intended to minimize operational risk. An extension of the Basel Accord, Basel II, identifies operational risk as "the risk of direct or indirect loss resulting from inadequate or failed internal process, people or systems or from external events", and also defines regulatory guidelines for international banking.

The latest update to the Basel Accord, Basel III, is scheduled for implementation between 2013 and 2019, although some institutions are now being audited for compliance with it along with Basel II. The intent is to show how banks can limit their financial loses. Some of the provisions in Basel II and III overlap with SOX sections 404 (identifying risk of loss) and 409 (requirement for disclosure of loss). These are clearly related to information technology management and network security.

Where Tenable Can Help

As requirements for Basel III become clearer, Tenable is recommending that banking corporations continue to implement programs that encompass their current audit requirements. Most banking institutions that are subject to Basel II and III are also subject to many other compliance audits. If they are in compliance with other regulatory standards, they will possibly also be in compliance with Basel II and III. In particular, since most banking companies are public companies, they are already subject to Sarbanes-Oxley audits.

One of the principles of Basel II is a common form of risk assessment. Standardizing on a common form of vulnerability management can help to reduce confusion between different organizations. Once all groups are measured by the same standard, it becomes easier to identify outliers and non-compliant issues.

For large organizations, Tenable can facilitate a change in culture by providing one common framework to ensure the right information gets to the right people. Tenable's SecurityCenter can coordinate the efforts of auditors, information technology practitioners and policy makers. Normally, auditors and information technology staff are not aligned and often interfere with each other's activities. With Tenable's solutions, real-time audit and compliance reporting can become part of the IT culture.

Tenable and COBIT

Background

COBIT, formerly known as the Control Objectives for Information and related Technology, now only uses the acronym "COBIT 5" as of April 2012. It is a set of best practices that have been created by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI). The ISACA organization is primarily comprised of financial organizations such as banks, lending institutions, investment firms and insurance companies.

The COBIT process reference model has been adopted by many companies and auditors who are required to report their status with respect to the Sarbanes-Oxley (SOX) act of 2002. SOX is covered in more detail later in this document.

COBIT 5 identifies 37 governance and management processes that are grouped into the following five governance and management domains:

- Evaluate, Direct and Monitor (EDM)
- Align, Plan and Organize (APO)
- Build, Acquire and Implement (BAI)
- Deliver, Service and Support (DSS)
- Monitor, Evaluate and Assess (MEA)

The following is an overview of each of these domains with a brief description of how Tenable's solutions can aid in auditing and monitoring compliance. A more detailed look at COBIT 5 control objectives is discussed in "Appendix E".

Evaluate, Direct and Monitor (EDM)

This domain ensures that stakeholder needs are evaluated to meet organizational objectives, direction is given in the decision-making process, and that performance and compliance are monitored over time.

The processes that are part of this domain are:

- EDM01 – Ensure Governance Framework Setting and Maintenance
- EDM02 – Ensure Benefits Delivery
- EDM03 – Ensure Risk Optimization
- EDM04 – Ensure Resource Optimization
- EDM05 – Ensure Stakeholder Transparency

Ensuring risk optimization and resource optimization begins with knowing what your risks and resources are. Tenable's solutions, especially SecurityCenter, Nessus, and the Passive Vulnerability Scanner (PVS), can assist with the goals outlined in these processes, especially *EDM03 – Ensure Risk Optimization* and *EDM04 – Ensure Resource Optimization*. More details about how this can be accomplished are in "Appendix E".

Align, Plan and Organize (APO)

This domain ensures that the organization has a plan for implementing IT technology. The plan must be a living document that covers initial deployment and updates to the technology platform over time.

The processes that are part of this domain are:

- APO01 – Manage the IT Management Framework
- APO02 – Manage Strategy
- APO03 – Manage Enterprise Architecture
- APO04 – Manage Innovation
- APO05 – Manage Portfolio
- APO06 – Manage Budget and Costs
- APO07 – Manage Human Resources
- APO08 – Manage Relationships
- APO09 – Manage Service Agreements
- APO10 – Manage Suppliers
- APO11 – Manage Quality
- APO12 – Manage Risk
- APO13 – Manage Security

The ability to manage the configuration and monitor the security events of any IT asset is critical to demonstrate to an auditor that these COBIT 5 control processes are being followed. Tenable's solutions are a valuable aid for processes in this domain, particularly for *APO12 – Manage Risk* and *APO013 – Manage Security*. More details about how this can be accomplished are in "Appendix E".

Build, Acquire and Implement (BAI)

This domain has ten processes that focus on identifying, installing, and operating IT resources. The processes are as follows:

- BAI01 – Manage Programs and Projects
- BAI02 – Manage Requirements Definition
- BAI03 – Manage Solutions Identification and Build
- BAI04 – Manage Availability and Capacity
- BAI05 – Manage Organizational Change Enablement
- BAI06 – Manage Changes
- BAI07 – Manage Change Acceptance and Transitioning
- BAI08 – Manage Knowledge
- BAI09 – Manage Assets
- BAI10 – Manage Configuration

Tenable's solutions monitor changes in the IT infrastructure and aid in determining effectiveness. Changes can include access control, patching, installation of new software and hardware and network re-configuration. Tenable's solutions can find these changes in many ways through credentialed configuration audits, distributed vulnerability scans and continuous passive network analysis. Tenable's solutions can also process system and audit logs for many different devices and associate the devices with real user accounts. These logs can be used to ensure that a change was authorized and implemented by the appropriate individuals. Tenable's solutions are particularly helpful in process *BAI06 – Manage Changes*.

Control objective *BAI10 – Manage Configuration* can be achieved by SecurityCenter and Nessus' compliance configuration audits. This technology allows configuration auditing of different types of assets. The audits can be derived directly from corporate policy, which drives the configuration standards that must be followed. Tenable provides a number of sample audit files that are designed to check for compliance with many established standards. While these are not represented as official audit files for these standards, these audit files can be reviewed and customized for the organization's specific requirements. A more detailed analysis of how Tenable's solutions can help is provided in "Appendix E".

Deliver, Service and Support (DSS)

This domain focuses on IT infrastructure operation and service. The following control objectives are part of this domain:

- DSS01 – Manage Operations
- DSS02 – Manage Service Requests and Incidents
- DSS03 – Manage Problems
- DSS04 – Manage Continuity
- DSS05 – Manage Security Services
- DSS06 – Manage Business Process Controls

Tenable's multiple forms of vulnerability management and security event management are powerful operational tools for many of these processes, particularly *DSS02 – Manage Service Requests and Incidents* and *DSS05 – Manage Security Services*.

Control objective *DSS02 – Manage Service Requests and Incidents* can benefit from Tenable's LCE and SecurityCenter. In fact, all help desk functions, such as troubleshooting and general management of information about particular hosts, can benefit from the Tenable product line. A help desk can use SecurityCenter to access a variety of information about servers, applications, and performance.

Control objective *DSS04- Manage Continuity* can be assisted by Tenable's LCE and SecurityCenter, which can help identify denial of service attacks and other network disruptions.

Monitor, Evaluate and Assess (MEA)

The last domain ensures that the current IT environment is indeed serving the company in a compliant manner. The control objectives are:

- MEA01 – Monitor, Evaluate and Assess Performance and Conformance
- MEA02 – Monitor, Evaluate and Assess the System of Internal Control
- MEA03 – Monitor, Evaluate and Assess Compliance with External Requirements

Tenable's solutions can help organizations perform independent assessments of the operating IT environment against internal controls and external requirements. Tenable's Nessus vulnerability scanner provides a snapshot of the infrastructure's vulnerability status at any given time. The PVS is most effective to provide a running status of the network on a virtual real-time basis.

Tenable and DISA STIG

Background

The United States Department of Defense has produced a variety of Security Technical Implementation Guides. These guides identify a wide variety of DOD "best practices" for hardening a number of devices and systems, such as Cisco routers, mainframes, Apache servers and identity management systems. The direction for the content comes from the Defense Information Systems Agency (DISA) and there has been significant input from the National Security Agency (NSA) Systems and Network Attack Center (SNAC).

Where Tenable Can Help

Tenable offers configuration auditing per DISA STIG policies for a wide variety of Windows operating systems including Windows 7, 2003 and 2008. Similarly, Tenable also supports NSA best practice audits for the same Windows systems, the IIS web server, and user policies.

DISA has also produced several NIST SCAP XCCDF policies that can be used to audit Windows platforms against DISA STIG standards. SecurityCenter can incorporate output from Tenable's xTool that has processed SCAP content containing DISA STIG policies (such as the DISA "Gold Disk" and DISA "Platinum Disk" policies) and produce an audit policy file. This allows SecurityCenter customers to audit Windows platforms for the specific settings recommended by DISA.

Tenable and USGCB

Background

The United States Government Configuration Baseline (USGCB) is a federal government-wide initiative to create security configuration baselines and provide guidance on improving and maintaining effective configuration settings that focus primarily on security. The USGCB baseline evolved from FDCC in 2010, and now covers multiple versions of the Windows operating system, Windows firewalls, Microsoft Internet Explorer, and the Red Hat Enterprise Linux operating system.

Agent-less SCAP Audits

NIST also certifies companies using the XCCDF standard, such as Tenable, to be able to perform audits of computers. Tenable's technology is compatible with the SCAP XCCDF protocol.

Currently, NIST has provided several different policies to audit Windows technologies such as desktops, servers, and some applications such as Internet Explorer and Symantec Anti-Virus.

Tenable customers can download the SCAP content from NIST, convert it to a Nessus audit policy that can be uploaded to SecurityCenter and then perform agent-less audits of desktops and servers. Tenable also directly provides SCAP audit files derived from DISA STIG content.

Broad USGCB Monitoring

Tenable's PVS and LCE can also assist in USGCB monitoring. Both products can passively monitor a network for evidence of new systems and applications that need to be validated. For existing systems and applications, the LCE can analyze system logs that indicate local configuration changes such as new software, new users and new settings, have been applied.

Tenable and FISMA

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.

FISMA and NIST

The National Institute of Standards and Technology (NIST) has the responsibility of publishing a variety of guides for implementing security controls, performing audits and certifying systems. These specific publications are covered in the "Tenable and NIST" section later in this document.

Where Tenable Can Help

The consensus among 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 Plans of Action and Milestones (POA&M) reporting requirements.

Specifically, there are several configuration audit policies available for SecurityCenter 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.

Tenable and GLBA

Background

The Gramm-Leach-Bliley Act (GLBA) requires financial institutions to have a security monitoring process in place to discover unauthorized access or modification of non-public customer information. Organizations that obtain and control private customer information must monitor, alert and report on attempted or successful access violations. The most public side of GLBA requires disclosure of any breaches.

In particular, the "SafeGuards" section of GLBA requires companies to develop a written information security plan that describes their approach to safeguarding customer data. As part of the plan, each company must:

- Designate one or more employees to coordinate the security program
- Identify the risks to assets that contain customer information
- Deploy controls to minimize risk and then monitor those controls
- Keep the security program updated as the organization's business and type of data collected changes

Where Tenable Can Help

The primary goal of GLBA is to protect private consumer data that is collected by financial institutions and to accurately report any unauthorized disclosure of the data. Tenable can help minimize the risk of breaches by ensuring that all IT systems are operating in compliance with the corporate security guidelines. This includes identifying which systems contain sensitive data, such as customer addresses and financial information. Tenable's solutions also aid in reporting unauthorized disclosures by distinguishing relevant data from the large volume of data generated in complex networks.

The challenge for organizations that are subject to GLBA is to accurately determine which data was compromised in order to ensure that appropriate notice is given to the affected consumers. GLBA does not require that notice be given to all consumers – just those whose data was compromised. With active logging in place, Tenable can rule out systems that an attacker did not compromise. For example, if a server with a cache of data on 2,000 consumers was compromised, it is possible that the attack may have leapfrogged from that system to one containing the data of 20,000 customers. It is very valuable to be able to provide proof that this access did not occur. Tenable's LCE can be used to log this sort of data and retain it for forensic analysis.

The LCE can also be used to track all logons, logoffs and login failures for any device or application on the network. These can include positive (successful and authorized) connections, as well as potentially suspicious activity. Any of these events can be sorted by business asset or even individual network user. Suspicious activity can be identified in several ways, such as identifying brute force login attempts, identifying logins from suspicious sources (such as outside of the organization) or the use of disabled or deactivated accounts. This allows an auditor to differentiate a login failure on a backup test server from one running a production database of customer information.

The Federal Trade Commission recommends several techniques for securing information. These are outlined at the following location:

http://www.ftc.gov/os/2002/05/67fr36585.pdf

"Appendix A" of this paper shows how Tenable's solutions can assist organizations in complying with GLBA.

Tenable and HIPAA/HITECH

Background

The Health Insurance Portability and Accountability Act (HIPAA) was passed into law in 1996. The goals of the act are to standardize exchange of information between healthcare providers and to ensure patient record confidentiality. These goals are tightly related to information technology. Organizations have been required to demonstrate compliance since 2003.

In HIPAA terms, an IT organization must maintain controls that secure all information related to an individual's healthcare. This data is called Electronic Protected Health Information (EPHI).

The Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted as part of the American Recovery and Reinvestment Act of 2009. HITECH increases the scope of security and privacy protections for EPHI previously set forth by HIPAA and also addresses liability and enforcement when violations or breaches occur.

Where Tenable Can Help

Tenable solutions can lower costs of audit data collection to aid in demonstrating HIPAA and HITECH compliance.

Health care organizations are required by law to comply with HIPAA and HITECH standards, but compliance alone does not ensure a secure IT infrastructure. Tenable has many customers in the health care industry that demonstrated compliance with HIPAA and HITECH, but actually had networks that were easy for insiders and external attackers to intrude upon. Deploying Tenable's solutions ensured both compliance with HIPAA and HITECH, as well as a secure network.

In an industry where patient care is the primary focus, the IT departments of many health care organizations often do not have the staff or budget for complex solutions. Tenable's solutions, which are often less complex and easier to deploy than others, have been successfully deployed and maintained in many health care organizations. Tenable's data leakage monitoring solutions can also identify specific types of health data such as patient identifier data and information contained in Electronic Data Interchange (EDI) forms.

HIPAA also specifies a “Security Provision” which includes three safeguards for administrative, physical and technical measures. How Tenable can help healthcare organizations meet these provisions is documented in “Appendix B”.

Tenable and ISO 27002 (formerly ISO 17799)

Background

ISO 27002 (formerly referred to as ISO 17799), written by the International Organization for Standardization (ISO), establishes guidelines and standards for information security management. ISO 27002/17799 provides a best practices approach with commonly accepted goals of information security organizations, such as maintaining confidentiality, integrity and availability of information resources. The guidelines of ISO 27002/17799 are not legal requirements, but are used as an audit benchmark to certify compliance with a commonly accepted standard. ISO 27002/17799 provides best practice recommendations in the following areas of information security management:

- Security Policy
- Organization of Information Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems Acquisition, Development and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

Where Tenable Can Help

As with other compliance initiatives, Tenable’s SecurityCenter can be used in conjunction with the LCE, Nessus vulnerability scanner and PVS to monitor the confidentiality, integrity and availability of many key assets.

As per the specific ISO 27002/17799 standard, Tenable can help in the following ways:

Security Policy

With SecurityCenter, organizations can measure how their IT resources are complying with any given security policy. For example, if all computers are supposed to be running anti-virus software, SecurityCenter can test for this on a periodic or real-time basis. Some of Tenable’s customers have implemented audits for “100 page” security policies and routinely get reports for non-compliant assets.

Organization of Information Security

The use of asset-centric security metrics provided by SecurityCenter simplifies the organization of information security data. When populated with asset information or when used to automatically discover certain types of asset groups, SecurityCenter will automatically organize and trend data. This enables managers of specific business units to track data and trends only for the assets in their organization.

Asset Management

SecurityCenter can import lists of IT assets from many different types of systems. These asset lists can be used for access control, reporting and security analysis. When integrated with the Nessus vulnerability scanner or PVS, SecurityCenter can also discover new assets.

For example, a list of core Cisco routers can be imported to SecurityCenter and classified as “Cisco Routers”. SecurityCenter can be configured to add any new devices that fit the profile of a Cisco router to the list. Asset lists can be segregated so that only SecurityCenter users who are specifically authorized may access a particular list.

Another useful feature of SecurityCenter is the concept of grouped assets. For example, a typical Microsoft Exchange deployment in a large organization may contain several components: a spam filter, a backup DNS server, a mail gateway, a Windows domain controller, a SQL database for logging and a SAN to store all of the archived email. Some of these systems are clearly part of the email services, but others are more ambiguous. The routers that front for the email server are part of the “email” asset, but serve other purposes as well. SecurityCenter provides the ability to draw arbitrary lines around political boundaries for core assets.

Human Resources Security

Tenable’s SecurityCenter can assist in securing data associated with Human Resources (HR) operations. The first area of concern for Human Resources IT systems is to ensure they are secure. Through vulnerability management and asset discovery, the computers and systems used to manage an organization’s HR data can be audited for vulnerabilities.

Another area of concern for HR systems is to ensure sensitive data, such as personnel records, are not disclosed or accessed by unauthorized users. SecurityCenter and the LCE can be used to provide assurance that only authorized people have access to the data on a need-to-know basis. Specific user accounts can be audited with the LCE to discover exactly what one or more users have done. Tenable’s data leakage monitoring solutions can also identify if HR data is available on unauthorized systems. See the section of this document titled “Tenable and Data Breach Notification Laws” for more information on data loss monitoring.

A common concern for organizations is to ensure terminated users are no longer accessing the system. The LCE can be loaded with a list of recently terminated employees or third party users who are no longer authorized. The LCE can then search user names in system logs for potential abuse. This feature can also be used to search for access of user accounts at times when the user is known to be away on vacation.

Physical and Environmental Security

Physical security is a concern of auditors, but is not often at the top of most IT security manager’s lists – usually because it is managed by a different organization. Still, the data held by the computers controlling environmental and access control devices can be critical to detecting insider threats.

The LCE can be used to receive logs from physical access control devices. These can be correlated with other logs that track logins to main system servers or changes in hardware configurations. The LCE can also audit and monitor servers for insertion and removal of USB storage devices (such as external disk drives or memory sticks) that are often used to copy information. SecurityCenter can also help manage the security vulnerabilities and configurations of the systems controlling the physical devices.

Communications and Operations Management

SecurityCenter can be used to monitor the security of communications devices. Vulnerabilities and security events can be managed for phone switches, fax machines, printers and many other types of electronic devices used for communication.

Access Control

One of the greatest security challenges for large organizations is to ensure that sensitive information is only accessed by authorized individuals. This has traditionally been accomplished by a “keys to the kingdom” approach, which grants access to the entire infrastructure through a single network sign-on. This is reasonably effective when there are established boundaries that house IT assets. Today’s computing environment is more distributed, with corporate assets on multiple devices accessed from multiple locations. It is vital to ensure that access to data is monitored throughout the network, not just on the external perimeter. Monitoring access control is one of the most critical aspects of any security architecture.

SecurityCenter, the LCE, and the PVS are valuable tools that can ensure that access control is appropriately managed.

With any access control policy, the devices that enforce the policy also log both permitted and denied access activity. For example, a firewall may produce a log of denied access attempts to a database server and also log when successful access occurs. The LCE can not only gather and normalize these logs, but it can also identify the specific asset associated with the

activity. By associating logs to specific assets, the access control policy can be independently verified. The LCE also supports the import and analysis of historical logs, which allows for a more complete picture of any access control policy.

The PVS can be used to monitor network data flows and identify anomalous traffic. A large network may have specific network services, such as email, web browsing, or other applications running on segregated network segments. The PVS monitors this traffic and passes it to SecurityCenter, which can be used to analyze the network data flow and identify anomalies. For example, Tor traffic coming through a firewall that is not configured to allow Tor could indicate a security compromise. Anomalous behavior is one of the best indications of a system compromise or security violation. There may be logical explanations for the activity, which can be better determined by an investigation rather than supposition.

Finally, by using multiple Nessus scanners, SecurityCenter can perform trusted scans from various locations inside the network. This is useful for situations where an organization has trust relationships between various groups. These trust relationships can result in holes in firewall access control lists, network links which bypass security controls, or even forgotten network connections. By performing a network scan from strategic points on the network, a security analyst can discover the actual trust relationship with the remote network.

Information Systems Acquisition, Development and Maintenance

The ISO 27002/17799 requirement for Information Systems Acquisition, Development and Maintenance is similar to the requirements specified in the Information Technology Information Library (ITIL) form of network management. The ITIL network management model contains processes for implementing change control, understanding where the critical resources are on a network, implementing a repeatable build process and then fine-tuning these processes. More details about these processes and how Tenable's solutions fit into the ITIL enterprise model are detailed in the section titled "Tenable and ITIL".

Information Security Incident Management

The primary steps of the security incident management process are detection, identification, data gathering, analysis and response. If litigation is likely to occur, it is important that these steps be followed carefully to ensure that evidence is accurate and irrefutable. Tenable's solutions can greatly assist in all aspects of security incident management. SecurityCenter can detect anomalous behavior and aid in identifying and categorizing the incident. The LCE gathers and normalizes logs from all network assets in addition to any logs maintained locally on the device. This is particularly important if a security breach has occurred and litigation may be involved. It is common in computer crime cases to discover that local system logs have been tampered with to remove evidence of the activity. It is difficult, but not impossible, for an intruder to remove all evidence from log files on the system they have gained privileged access to. Often, an attacker will neglect to account for log records that are written after a connection is closed, but a skilled attacker can set up a program to remove the record after disconnect. The LCE provides an independent record of all network activity that can be used to verify local system logs and can monitor file MD5 checksums in real-time to detect modifications to files and folders that are part of an investigation. The LCE data provides critical evidence in computer crime cases.

Regardless of the incident type, SecurityCenter will contain a large amount of information on the targeted systems. Identifying the applications, the underlying operating system and even the organization in charge of a system can often shape the incident response process.

Business Continuity Management

Tenable can help any organization with many different aspects to business continuity management.

Many organizations have hot-spare servers that are put into production use if the primary server needs to be taken offline. If they are not in production use, they may not be managed or patched. If they are required to be put into service, the organization may recover from an outage, but may now be dramatically less secure than before. SecurityCenter can manage the security life cycle of these devices just like any other asset.

During a business outage or failover, Tenable's LCE is very useful for observing changes in network and server behavior. The logs gathered during a failover can be of great assistance in diagnosing the success or failure of a switch to backup devices. Also, the PVS can measure which systems on a network are now communicating with the failover servers. This can aid tremendously in troubleshooting any problems that arise.

Compliance
The last section of ISO 27002/17799 focuses on how organizations can maintain and measure compliance issues. Tenable's focus is to assess the compliance of a network through configuration analysis and monitoring events for impact to network compliance.

Tenable and ITIL

Background
The Information Technology Information Library (ITIL) specifies several techniques for running a network with high availability, integrity and confidentiality. The concepts of ITIL revolve around implementation of change management, knowing where the critical assets are, having a repeatable build process and then auditing these processes for continuous improvement. Tenable's vulnerability scanning, policy auditing, log analysis and passive monitoring can greatly assist in accelerating these processes for any enterprise.

ITIL has relevance to compliance auditing because it is much better to run a network efficiently and pass an audit than to not pass an audit and scramble to implement non-existent controls. Organizations that have had robust network management solutions have often been found to pass compliance audits with very minor changes in their control processes.

Change Management
The basic concept of change management is that most network and application outages are self-inflicted. By minimizing the amount of change, there are less outages and higher uptime.

SecurityCenter, the LCE, the Nessus vulnerability scanner and the PVS can be used to discover changes in the network that should not have occurred or are against policy. Discovery of new hosts and new applications is easily accomplished with these tools. For complex enterprise networks, this process can be implemented on different levels of granularity based on the asset type. For example, a new Linux computer may be an anomaly on the desktop network, where a new Windows laptop would not. However, in the DMZ, any new computer is of interest and should be investigated.

Finding Fragile Artifacts
The concept of primary servers or assets is different between organizations. ITIL practitioners look for servers and resources that are "fragile" or "brittle" and not resistant to change. These are often the most complex devices on the network. Locking down changes to these devices increases their uptime.

Tenable can help identify where these fragile systems are to aid in security monitoring. Through asset management, SecurityCenter can be used to manage all of the vulnerabilities and log events for all of the devices that make up the artifacts. For example, a PeopleSoft application may be comprised of multiple database, firewall, authentication and server components. Identifying them as a whole as well as being able to drill into their specific issues facilitates management of the artifact.

Repeatable Build Process
Use of a common methodology permits organizations to build laptops, desktops and servers that are easier to manage and more secure. When a common methodology is not used, the level variance in system builds increases. A network of systems with a high level of variance is more difficult to patch or manage than one with a low level of variance. Unknown or unforeseen issues can impede software rollouts, causing compatibility issues with security patches.

SecurityCenter and its active and passive scanning components can identify new and existing hosts that are not configured correctly. SecurityCenter can log into network servers and validate their configurations against a known database of settings. Unique tests for each asset class can be performed for each asset. This can lead to low levels of variance in the systems on your network and increase ease of management.

Improvement Through Metrics
The last component of ITIL is to continuously tune the network management process. SecurityCenter can produce many different types of metrics, any of which can be adopted by an enterprise for tracking. For example, an organization may wish to adopt strategies to limit virus outbreaks. The ability to detect virus-infected systems in different organizations is facilitated with SecurityCenter in many different ways.

Tenable and NIST

Background

The National Institute of Standards (NIST) has published a variety of IT security related guidelines. Some of these are very specific, such as recommended settings to harden Windows servers, and others are very generic, such as how to audit change management procedures. Various auditors have adopted many of these NIST standards 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 in several ways as outlined below.

NIST Special Publication 800-53 – Security Controls

As quoted from the publication: "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 its mission?
- Have they been implemented?
- Are they working?

The publication recommends 18 different types of controls 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.

"Appendix C" details exactly which control mechanisms can be monitored or audited by Tenable's solutions.

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

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

- 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 devices need to be monitored and which logs 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 also very scalable and require little effort to maintain. This can bring 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 becomes very easy to place controls on how long logs are to be stored and how they should be disposed.

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).

Windows Hardening Guides

SecurityCenter and Nessus both 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 policies can be modified for either more stringent or less stringent audits.

Tenable and NSA

Background

The INFOSEC group of the National Security Agency (specifically the Systems Network and Attack Center – SNAC) has released several configuration guides to harden Unix, Linux, and Window servers. These guides are typically written as a report and include recommendations for some specific settings.

Tenable Audit Policies

Tenable has developed several Windows, Linux, and Unix audit policies based on the NSA guidelines. These policies can be used to develop customized audit tests.

NSA content is also available as part of the NIST SCAP program. Many of the NSA hardening guides have been described in XCCDF/OVAL format and can be interpreted by SecurityCenter and Nessus.

Tenable and NERC CIP Standards

Background

The North American Electrical Reliability Council (NERC) has approved a set of cyber security standards to help support the reliability of the bulk power system. The standards are labeled from CIP-002-1 through CIP-009-1. Each CIP has the following focus areas:

- CIP-002 – Critical Cyber Asset Identification
- CIP-003 – Security Management Controls
- CIP-004 – Personnel and Training
- CIP-005 – Electronic Security Perimeters
- CIP-006 – Physical Security of Critical Cyber Assets
- CIP-007 – Systems Security Management
- CIP-008 – Incident Reporting and Response Planning
- CIP-009 – Recovery Plans for Critical Cyber Assets

Tenable's Role in Maintaining NERC Compliance

For many years, the cyber assets critical to power generation, transmission, and distribution used proprietary protocols, systems, and networks. The security vulnerabilities and threats to these legacy SCADA and DCS systems were quite different from what an enterprise network faced.

This is changing now that many control systems have implemented Ethernet and TCP/IP networks and are using operating systems, databases, and web servers commonly found in an enterprise network. This is happening first in the control center, which increasingly uses the same types of network, server, and storage hardware commonly found in enterprise data centers. IP to the substation or plant floor is also becoming increasingly common and there is a growing market for industrial networking devices such as hardened routers and switches that allow support communication among PLCS, IEDs, and RTUs with Ethernet interfaces.

Not only does the technology now more closely resemble traditional IT networks, but interest among the hacker/researcher community has dramatically increased in recent years, with an increasing number of high profile vulnerability disclosures and proof of concept exploits for SCADA vulnerabilities.

Many of the NERC CIP requirements involve “Critical Cyber Assets” and “Electronic Security Perimeters”. Tenable’s solutions can identify rogue systems within Electronic Security Perimeters, unauthorized communication with Critical Cyber Assets and help meet the monitoring requirements of the NERC standards.

System availability is the most critical security requirement in most electric SCADA and DCS. Many organizations are hesitant to use technology that may impact legitimate communication, even if the probability is small. Tenable’s passive analysis is an ideal solution for these environments because it will not alter or block any communication, yet will help an organization comply with certain NERC CIP requirements.

Specific Tenable Offerings

Tenable offers layered solutions for scanning SCADA systems and devices:

- Nessus can perform both uncredentialed and credentialed scans of SCADA systems for a wide range of vulnerabilities.
- Specific SCADA plugins are available through a partnership with Digital Bond. These plugins discover and scan SCADA devices for known and newly discovered vulnerabilities.
- The Passive Vulnerability Scanner scans network traffic for potential problems. Passive scanning is invaluable for devices considered “unscannable” and offers coverage not available through active scanning technology alone.

With over 300 Nessus and PVS plugins that discover and assess the security posture of common SCADA applications, devices and protocols currently available, Tenable is uniquely positioned to address the components within SCADA and control system networks as well as the applications and operating systems that are common to both traditional IT and SCADA networks.

See “Appendix F” for details on each of the requirements outlined by each CIP. In some cases, all Tenable products can help perform a required action such as ongoing monitoring. The data gathered from Tenable products can often be used as a basis for establishing well-grounded policies.

Digital Bond Configuration Audits

To address the risks posed by increased connectivity with the Internet and enterprise networks, SCADA vendors are also releasing products with enhanced security features and to define best practices for securing older generations of products. Tenable Network Security has supported a Department of Energy Funded project named “Bandolier”, which defines and implements a toolset for assessing the security posture of the operating system and applications such as historians, operator consoles and communication services used by the leading vendors. Digital Bond (http://www.digitalbond.com/) has developed dozens of Nessus and SecurityCenter audit files that can be used to identify thousands of configuration weaknesses in a wide variety of control system applications. These configuration tools are available to customers of Digital Bond’s subscription service that includes access to their knowledge base, original SCADA security content and much more.

Tenable and Nuclear Facility Cyber Security

Background

The U.S. Nuclear Regulatory Commission’s (NRC) Office of Nuclear Regulatory Research has approved Regulatory Guide 5.71 (RG 5.71), “Cyber Security Programs for Nuclear Facilities”. This guide directly refers to Title 10, of the *Code of Federal Regulations,* Section 73.54, “Protection of Digital Computer and Communication Systems and Networks” (10 CFR 73.54), which requires NRC licensees to protect digital computer and communications systems and networks from cyber attacks that would deny access to or otherwise adversely impact those systems. Appendix A of RG 5.71 outlines a “Generic Cyber Security Plan Template” to help establish, implement, and maintain a plan for securing critical assets as part of a site’s physical protection program. Appendix B of RG 5.71 addresses “Technical Security Controls” used to protect critical assets from cyber attacks.

Tenable’s Role in Nuclear Facility Cyber Security

As outlined in RG 5.71, the steps for planning, implementing, and maintaining a cyber security plan describe how to meet the requirements of 10 CFR 73.54. Tenable’s SecurityCenter, Nessus, Passive Vulnerability Scanner, and Log Correlation Engine can all be used together to not only gain a better understanding of complex and diverse networks and systems,

but also to specifically address specific RG 5.71 guidance points such as “A.3.1.3 - Identification of Critical Digital Assets”, “A.4.1.3 - Vulnerability Assessments and Scans”, “B.2.6 - Audit Review, Analysis, and Reporting”, and many more. See “Appendix G” for details on each step of the RG 5.71 plan and how Tenable’s products can be used to help ensure the availability, integrity, and confidentiality of systems owned or operated by NRC licensees.

Tenable and PCI

Background

The Payment Card Industry Data Security Standard (PCI DSS) is a comprehensive set of security standards established by the founding members of the PCI Security Standards Council, including Visa, American Express, Discover Financial Services, and MasterCard. The PCI DSS is intended to provide a common baseline to safeguard sensitive cardholder data for all bankcard brands and is in use by many vendors who accept, transmit, process, and store credit card data. The PCI DSS specifies a variety of high-level standards for running a secure network that leads to variations in how QSAs interpret these recommendations. Tenable can help customers exceed the requirements to ensure they meet compliance.

Tenable’s Role in PCI

Tenable provides the solutions to analyze and generate reports on network security *before* undergoing a costly third party audit. By using Tenable’s vulnerability scanning, vulnerability management, log analysis, content discovery, and configuration audit tools, Tenable’s customers can identify issues audited against the PCI DSS well before the official assessment occurs. This also helps reduce the cost of the official assessment by reducing the time it takes to get the QSAs the information they need.

Tenable Network Security, Inc. is a PCI Approved Scanning Vendor (ASV), and is certified to validate vulnerability scans of Internet-facing systems for adherence to the PCI Data Security Standards (PCI DSS). The Tenable Nessus Perimeter Service includes a pre-built static PCI DSS scanning policy that adheres to the requirements of the PCI DSS. This policy may be used by merchants and service providers to initially assess their environments based on PCI DSS requirements, and also to perform vulnerability scans and generate reports that can be validated by qualified Tenable Network Security staff members to satisfy the PCI DSS ASV quarterly scanning validation requirement found in PCI DSS 11.2.2.

Many Tenable customers who are required to follow the PCI DSS are also extremely interested in Data Loss Prevention (DLP). Data Loss Prevention is an important concern for companies that handle sensitive information. Breach disclosure laws require that companies that handle consumer data must disclose all data breaches and provide remediation to protect the consumer. The cost of such breaches can be quite staggering in legal and public relations costs as well as lost business. The ability to automatically identify systems that contain customer data or consumer cardholder data makes finding unauthorized copies of data easier. This also directly addresses the PCI requirement of “never send unprotected PANs (primary account numbers, or simply the credit card number)”. If cleartext cardholder data is emailed or copied by an authorized user to an un-authorized system, it is a PCI DSS violation that Tenable’s solutions will detect and generate an alert to appropriate personnel – before it becomes a public relations nightmare. Beginning with Version 2.0, the PCI DSS requires all entities to develop, document, and execute a methodology to discover not only the locations of PCI data in storage, but also to demonstrate where PCI data is not found within the network environment. Tools such as Nessus and PVS that can detect the presence of credit card data as it traverses an enterprise network greatly helps the methodology for both determining where the card data IS as well as where it IS NOT located.

PCI Security Audit Procedures and Reporting

The PCI DSS mandates the following 12 major security requirements that an organization must adhere to in order to be considered in compliance:

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Protect all systems against malware and regularly update anti-virus software of programs
6. Develop and maintain secure systems and applications

7. Restrict access to cardholder data by business need to know
8. Identify and authenticate access to system components
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security for all personnel

In addition, entities of all levels and types that are subject to PCI must have a program in place for a qualified third party Approved Scanning Vendor (ASV) to conduct quarterly comprehensive vulnerability scans of all Internet-facing systems whether or not they may impact security of the cardholder data environment. This vulnerability scan is required to look for a comprehensive list of vulnerabilities including but not limited to the following items:

- Any vulnerability with a CVSS score of 4 or higher
- Any cross-site scripting, SQL injection or other OWASP "Top Ten" web-based application vulnerabilities
- Any evidence of outdated SSL encryption or other insecure transmission methods
- Missing system or OS patches

PCI DSS documentation addresses in detail how each of these individual requirements needs to be implemented and audited. Tenable can help organizations conform to these guidelines in many ways.

"Appendix D" details how Tenable can specifically address these guidelines. This allows any size of organization to determine if they are indeed in compliance or if there are areas that need to be addressed. The reports and data collected by Tenable's solutions can also help organizations pass assessments confidently with the knowledge they will be audited based on established tests and procedures.

In addition to satisfying the external vulnerability scanning requirements with the Nessus Perimeter Service, validating ongoing compliance with the majority of the twelve basic PCI DSS requirements can be demonstrated with other Tenable product solutions:

- All active Nessus scans can include simple Pass/Fail results based on PCI DSS requirements. This makes analyzing large numbers of servers or large numbers of vulnerability results easy and automatic.
- Tenable's LCE has the ability to store, compress, and search any type of ASCII log that is sent to it, including logs from perimeter devices, to aid in firewall monitoring and configuration. Tenable's SecurityCenter can also detect and alert on access from various points in the network using distributed active scanning and passive analysis.
- Firewall rule changes that result in open or closed ports can be monitored by comparing multiple scans, analyzing passive network data and analyzing logs from the firewalls themselves. Tenable's SecurityCenter and LCE have full log search capabilities to easily monitor firewall change activity.
- Tenable's Nessus vulnerability scanner can be used to attempt logins for various types of applications and devices to test for vendor supplied passwords.
- The security of systems protecting stored data can be assessed by Tenable's products. Access to the secured data can also be monitored with Tenable's LCE. All LCE search results are saved in a compressed format along with a MD5 checksum so that they can be used as forensic evidence.
- Tenable's PVS can be used to monitor network traffic in real-time to ensure confidential information, such as credit card numbers, is encrypted.
- Tenable's SecurityCenter can log into hosts to ensure that antivirus software is configured and functioning properly. In addition, Tenable's PVS can be used to identify systems running virus signature updates.

- SecurityCenter can use both active and passive vulnerability checks that monitor for vulnerabilities, patch levels, and insecure configurations. This is a valuable aid to maintain secure systems.
- SecurityCenter can monitor access to information by business units on a need to know basis through traffic analysis and distributed scanning. With SecurityCenter's asset centric view of a network, it is easy to see which assets connect to other assets and on which network links or ports.
- If users who access confidential information are configured with unique users IDs, then logs of access control should also exist. These logs can be captured by the LCE for analysis and sorted by individual user identifications. Logs can also be searched by user name.
- To provide controls for physical limitation of access to sensitive data, Tenable's LCE can receive authentication data from physical access control devices such as card readers. If a list of people or accounts that should or should not have access to sensitive data is provided, the LCE can also generate an alert if unauthorized user access is attempted. The Windows LCE agent can also monitor local and remote Windows servers for any insertion or removal of a USB device.
- Similarly, all access to cardholder data systems can be tracked. The LCE can track all logins, login failures, system logs, and even network activity for cardholder data systems. These logs are centralized, normalized, and correlated. Reports about incidents or security events can be created for specific asset groups under SecurityCenter.
- SecurityCenter can automate regular security testing of the systems managing credit card data. SecurityCenter offers many types of assessments such as vulnerability scanning, patch and configuration audits, as well as passive vulnerability analysis.
- If any security policy is created that specifically details how systems are to be configured, SecurityCenter can be used to audit those systems. All of Tenable's products can assist with unauthorized host detection, implementing a log management strategy, analyzing access control policies, analyzing patch management policies, and much more.

For a complete list of how Tenable can audit or assist in the monitoring of specific PCI DSS requirements, please refer to "Appendix D".

Tenable and SOX

Background

The Sarbanes-Oxley (SOX) Act of 2002 enacted a federal law requiring public companies to perform oversight, enable auditor independence and follow strict disclosure procedures for financial data. SOX requires executives of public companies to certify that their financial figures are accurate. IT systems supporting financial data must ensure that the data is accurate and has not been altered or tampered with.

The SOX Act contains many different sections, some of which pertain specifically to IT systems. Auditing IT operations for SOX compliance is generally accomplished by following guidance provided the Committee of Sponsoring Organizations of the Treadway Commission (COSO) or through the COBIT standard. Many auditors feel that COSO applies more to the accounting practices of an organization and that COBIT provides a more appropriate framework for auditing IT controls. "Appendix E" outlines in great detail how Tenable's solutions can be used to audit various parts of the COBIT framework.

Section 302 – Corporate Responsibility for Financial Reports

This section requires certification of the processes and activities used to produce financial data. The certification is asserted by the CEO and the CFO of the public company.

Many auditors broadly interpret IT controls for this section to be controls that impact anything that manages, holds or controls access to a financial data processing system. Any data processing system that can impact the quality or outcome of a financial report is subject to audit. Section 404 specifically addresses how this is to be accomplished, but some provisions in section 302 also impact the audits performed.

Tenable can help highlight anything related to security processes or access control for any financial data system. Individual pieces of security information are often easy to deal with, but on large financial networks, it may be difficult to

see how they interrelate or impact one another. Tenable's SecurityCenter can be used as the focal point of effort to determine if a financial asset is conforming to a corporate policy necessary to achieve SOX compliance.

Section 404 – Management Assessment of Internal Controls

This is the section most often referenced by vendors when referring to SOX compliance. Section 404 requires executives to issue an "Internal Control Report" which must do the following:

- Affirm the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting.
- Contain an assessment, as of the end of the most recent fiscal year of the Company, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

In other words, the company must report what it is doing to ensure the accuracy of the financial data and also provide metrics to verify how well it is working. Although there are other sections of SOX that affect IT, the main focus of audits cover how section 404 should be analyzed. It even provides guidelines for executive management to write the report.

The use of Tenable's products can help streamline any vulnerability, configuration and security event management process for IT. Using Tenable's products allows an organization to access each financial asset separately to see if it has been configured and managed correctly. Tenable also offers real-time log analysis and event management solutions that can be configured to record and generate alerts on SOX compliance events. Details on how Tenable can specifically help with section 404 are covered in the appendices.

Section 409 – Real-Time Issuer Disclosures

The responsibility to disclose changes to financial information as soon as possible leads many organizations to implement policies for real-time disclosure. Section 409 impacts IT in two general ways.

First, the need for more external communication has caused organizations to implement real-time portals to connect shareholders, consumers of information, auditors and many other consumers. All these external connections bring increased network complexity that IT has to manage. Tenable's solutions can monitor these portals to ensure they are secure, configured correctly and that all network traffic is logged for analysis.

Second, if a corporation suffers a data loss or discovers they have had unauthorized modification of financial data, they have a responsibility to disclose the event. Tenable can help with this issue several ways. The most basic way Tenable can help is to show to an auditor or corporate management that a capability is in place to accurately find intrusions or unauthorized activity through log analysis. If an incident does occur, Tenable's true value is in determining the impact of the incident. Through log analysis, it can be shown that an external hacker or an insider did not breach other financial data systems, which can minimize the "bad news" required to be reported.

Section 802 – Criminal Penalties for Alerting Documents

The SOX Act mandates penalties to executives for altering corporate documents, causing many auditors to use section 802 to justify a review of any public company's document control procedures and policies.

Tenable's solutions can help manage the security of data surrounding any electronic system containing corporate financial data. It is important to note that the term "financial data" can be loosely interpreted to include everything from the primary financial database to the CFO's laptop.

Tenable's ability to manage security information for large amounts of data systems while retaining the ability to filter, analyze and report based on asset classes is invaluable for this section.

Tenable and Data Loss Prevention Laws

Background

Data Loss Prevention (DLP) is a growing concern for organizations that handle sensitive information. The majority of states in the U.S. have enacted breach disclosure laws requiring organizations that handle consumer data to disclose all data breaches and provide remediation to protect the consumer. The European community is working on similar

legislation. The cost of data breaches can be quite staggering in legal and public relations costs as well as consumer confidence and lost business.

In the U.S., California was one of the first states to pass legislation to protect inadvertent disclosure of personal information. California's Database Breach Notification Act (SB 1386) requires any company that stores and processes personal information for residents of California to report any breach of that data. Since then, forty-six states, the District of Columbia, Puerto Rico, Guam, and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information. A list of State Security Breach Notification Laws can be viewed at the following website:

http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

Many members of the European Union (EU) have enacted privacy legislation and the European Data Protection Supervisor is currently backing data breach notification laws that will apply to all information service providers. Multiple directives and regulations have already been put into effect to help protect the privacy and security of personal and consumer data.

How Tenable Can Help

Before an incident, Tenable's solutions can be used to mitigate the risk that a theft of customer data will occur. Tenable's solutions can monitor any network to identify configuration issues and vulnerabilities. Tenable's PVS can track network data flow in real-time, which helps determine where sensitive data is located and how and to where it is being transmitted.

If an incident does occur, Tenable's solutions can help minimize the impact by determining exactly what was compromised. If a system was compromised but it does not contain sensitive data, there may be no need for disclosure. Many state regulations only require that specific data losses be disclosed. Pinpointing accurately what has been disclosed can limit what is presented to auditors, the media and law enforcement authorities. It also limits the number of customers for which the organization will have to provide remediation.

The ability to automatically identify systems that contain sensitive data or credit card information makes finding unauthorized copies of data easy. If data at rest is emailed or copied by an authorized user to an unauthorized system, it is likely a policy violation that Tenable's solutions can generate an alert on – before it becomes a public relations nightmare.

Responding to MPAA and RIAA Inquiries

Background

Tenable customers must often reply to inquiries from either the Motion Picture Association of America (MPAA) or Recording Industry Association of America (RIAA) that pertain to sharing of copyrighted content. These inquiries typically specify user names, IP addresses or activity that is involved with:

- Illegal distribution of copyrighted music and movies
- Possession of stolen, pre-released or unedited content
- Management of an index for illegal content hosted elsewhere

Neither the MPAA or RIAA is a law enforcement agency, but they do represent interests of the United States movie and recording industries. They have sued a variety of institutions and individuals for pirating and distributing music and movies.

Many organizations (especially universities, libraries and public school systems) have chosen to respond to these inquires. If your organization has a policy to respond to inquiries from the RIAA or MPAA, the act of collecting, filtering and processing the information needed for the response can be very time consuming.

How Tenable Can Help

Tenable's solutions can help mitigate the impact of MPAA/RIAA inquiries to your organization. Tenable can help identify in near real-time any hosts or servers on your network running peer to peer (P2P) applications and hosting suspicious content. Tenable's solutions can also look into almost any type of log source to find evidence of file sharing, file downloading and general activity for a suspected IP address.

Both the Nessus vulnerability scanner and the PVS can be used by SecurityCenter to discover P2P activity and potentially illegal file sharing. Nessus can be used to identify every type of file sharing and file serving technology in use today, and can also search for it on network assets where they should not be present. For example, with SecurityCenter, an analyst could report on a list of all asset types running a P2P application. Discovering a P2P application running on a server farm with high bandwidth could cause alarm. Similarly, Tenable's PVS can also identify a wide variety of common P2P tools in use. This identification is real-time and is performed through direct monitoring of network traffic.

For full audits of servers, Nessus can also identify file names that are related to pornography, copies of movies, copies of music and other types of illicit or copyrighted materials.

Tenable's LCE can be used to capture a variety of logs relevant to MPAA/RIAA inquires to analyze suspicious activity. These can include firewall and proxy logs, but can also make use of authentication, DHCP and even Network Address Translation (NAT) logs. MPAA/RIAA inquiries usually start with either an IP address or a user name. The LCE can be used to identify activity surrounding this information. Once identified, the information can be sanitized to protect the privacy of the organization.

Taking Action Before the MPAA or RIAA Calls

Tenable's products can be used proactively to ensure that illegal content is not being distributed on the Internet to limit potential abuse. Tenable recommends the following guidelines:

- **Only run file servers on known assets.**
  With the increase in bandwidth availability, it is very easy for users to install file servers on client workstations and laptops. With SecurityCenter and all of Tenable's products, the network can be monitored for new file servers or file servers running on unauthorized networks.

- **An increase in network traffic might indicate abuse.**
  Although there are many legitimate reasons for an increase in network traffic, a sudden increase in download activity could indicate that someone has configured a server to share music and it is now widely used. In this case, the LCE can be used to look for "spikes" in firewall logs, network connection logs and many other sources.

- **The best defense can be a good offense.**
  Tenable's products can minimize disclosure and potential liability for your organization, enabling legal counsel to respond to potentially frivolous inquiries from the MPAA/RIAA. SecurityCenter can be used to show reports on P2P activity showing which networks are actively communicating with Internet destinations. If the MPAA/RIAA has made an inquiry about a network or protocol not in use at your organization, Tenable's technology can prove this.

Conclusion

There are many different forms of compliance standards and provisions. Tenable's solutions focus on reducing the burden of proving adherence to many different compliance guidelines. If your organization is subject to multiple IT audit standards, leveraging solutions from Tenable can greatly facilitate demonstrating and reporting compliance with minimal resource commitment.

Appendix A: Tenable Solutions and Securing Information for GLBA

Note: The following recommended strategies came directly from the Federal Trade Commission web site at http://business.ftc.gov/documents/bus54-financial-institutions-and-customer-information-complying-safeguards-rule. Only safeguards relative to IT controls were considered. The following abbreviations will be used:

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

FTC Recommended Safeguard	Tenable Solution
Limiting access to customer information to employees who have a business reason to see it. For example, give employees who respond to customer inquiries access to customer files, but only to the extent they need it to do their jobs.	The vulnerability, compliance and security event information gathered by SC can be securely shared such that only the system or business owners know about their particular security issues. Data leakage and information sharing monitoring can be accomplished with the PVS, the LCE and Nessus scanner. This can be used to ensure that only authorized information is located only on authorized systems and accessed by authorized employees.
Controlling access to sensitive information by requiring employees to use strong passwords that must be changed on a regular basis. (Tough-to-crack passwords require the use of at least six characters, upper- and lower-case letters and a combination of letters, numbers and symbols.) Using password-activated screen savers to lock employee computers after a period of inactivity.	SC can be used to audit Unix, Linux, and Windows servers to detect violations in password configuration policy. The LCE can be used to audit all login, logoff and login-failure events. All logs can further be sorted by specific user identities.
Developing policies for employees who telecommute. For example, consider whether or how employees should be allowed to keep or access customer data at home. Additionally, require employees who use personal computers to store or access customer data to use protections against viruses, spyware and other unauthorized intrusions.	SC and the LCE can monitor the activity of remote employees who enter your network via VPN, network or dial in connections.
Imposing disciplinary measures for security policy violations.	With the use of asset discovery and configuration auditing, SC can be used to show which assets are not configured correctly. By analyzing security issues on a business asset-basis, organizations can have a better understanding of any discrepancies rather than working with just the most severe, isolated cases.
Preventing terminated employees from accessing customer information by immediately deactivating their passwords and user names and taking other appropriate measures.	The LCE can sort logs and events by authorized users such that activity from unauthorized users can be easily audited. Nessus can also be used to audit both active and deactivated users.
Know where sensitive customer information is stored and store it securely.	Nessus and the PVS can identify sensitive data in motion and at rest per multiple corporate policies.

	SC can then use this information to highlight specific assets containing sensitive data, as well the systems that depend on them (such as switches & routers) such that all security issues which may impact data disclosure can be addressed.
Take steps to ensure the secure transmission of customer information.	The LCE maintains a log of all network transactions and receives logs from systems specifically designed to look for communications containing potentially sensitive data. The PVS can also be used to look for credit card and social security number information.
Monitoring the websites of your software vendors and reading relevant industry publications for news about emerging threats and available defenses.	Through automated scanning and passive network traffic analysis, SC can keep track of each of your network and operating system vendor's security issues.
Keep logs of activity on your network and monitor them for signs of unauthorized access to customer information	The LCE can use logs from NetFlow, firewalls and direct network monitoring to keep a record of all network activity.
Use an up-to-date intrusion detection system to provide alerts on attacks	SC can receive IDS events from many of the leading vendors. These events can be sorted by targeted assets as well as be correlated with known vulnerabilities to highlight high-risk systems.
Monitor both in- and out-bound transfers of information for indications of a compromise, such as unexpectedly large amounts of data being transmitted from your system to an unknown user	The LCE has a built-in anomaly engine that detects changes in bandwidth, number of connections and time of day changes from "normal" network activity.
Insert a dummy account into each of your customer lists and monitor the account to detect any unauthorized contacts or charges	The LCE can easily be configured to look for activity on any dummy accounts. In addition, Nessus can audit systems to look for the official presence of the fake account.

Appendix B: Tenable Solutions for HIPAA Security Provisions

The following acronyms will be used:

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

Administrative Safeguards	Tenable Solution
The procedures must address access authorization, establishment, modification and termination.	The LCE can sort logs and events by authorized users such that activity from unauthorized users can be easily audited.
Internal audits play a key role in HIPAA compliance by reviewing operations with the goal of identifying potential security violations. Policies and procedures should specifically document the scope, frequency and procedures of audits. Audits should be both routine and event-based.	SC can be used to audit Linux, Unix, and Windows servers to detect violations in configuration and content policy. Nessus, the PVS and the LCE can all be used to monitor the network for potential compromises and backdoors.
Physical Safeguards	**Tenable Solution**
Controls must govern the introduction and removal of hardware and software from the network.	With network scanning and passive monitoring, SC can discover when there has been a change to the assets it is monitoring such as the addition of a new server or running a new service on an existing device. The LCE can also use network and system logs to identify when software is installed, modified or removed.
Preventing terminated employees from accessing customer information by immediately deactivating their passwords and user names and taking other appropriate measures.	The LCE can sort logs and events by authorized users such that activity from unauthorized users can be easily audited. Terminated employee accounts can also be fed into Nessus such that they can be audited per company policy.
Access to equipment containing health information must be carefully controlled and monitored.	With the LCE and SC, any type of access such as login failures, file transfers and configuration changes can be logged. Also, identification of systems with “health data” on them can be accomplished through scanning and passive monitoring. Finally, systems that contain PHI can also be audited to see if any USB devices have been connected to them.
Technical Safeguards	**Tenable Solution**
Information systems housing PHI must be protected from intrusions.	Both SC and the LCE can be used to identify network compromises, insider activity and post-attack activity. Also, identification of systems with “health data” on them can be accomplished through scanning and passive monitoring.
In addition to policies, procedures and access records, information technology documentation should also include a written record of all configuration settings on the components of the network because	SC can audit Unix, Linux, and Windows server configurations to ensure compliance. Customers can implement their own audit policies, but SC also includes policies based on NSA and NIST best practices as well as Tenable’s

these components are complex, configurable and always changing.	recommendation of a hardened server configuration.
Documented risk analysis and risk management programs are required. Covered entities must carefully consider the risks of their operations as they implement systems to comply with the act.	SC can be used to discover what assets are at the most risk or contain the most sensitive data. Using both active and passive technologies, SC can discover which systems depend upon each other or have trust relationships.

Appendix C: Tenable Solutions for NIST Special Publication 800-53

Note: This section was based on the content of NIST Special Publication 800-53 Revision 4. For the reader's convenience, only controls relevant to Tenable's solution are detailed here.

The following acronyms will be used:

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

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 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 (e.g., 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 solutions can test for the presence of accounts that should or should not be present on a system. 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 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 to ensure 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 some audit users cannot see events, some can only see normalized events and others can do unlimited log search. User access to LCE raw log data is configurable on a “per-LCE” basis.
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 which have not been locked down to a least level of privilege. For example, a running daemon or service on a server can be tested to see which user level it is operating against. Tenable also 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 network devices 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 has a variety of solutions that 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 if 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. When used with SecurityCenter, Tenable's 3D Tool also produces 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.
AU-6	AUDIT REVIEW, ANALYSIS AND REPORTING	Tenable's LCE provides the ability to normalize billions of log events, store, compress, and search for 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, compromise and port scans. Any report can be exported via 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.
AU-8	TIME STAMPS	All events arriving at the LCE are uniquely time-stamped.
AU-9	PROTECTION OF AUDIT INFORMATION	SC users can only see vulnerabilities, IDS events and logs for a specific range of IP addresses that they have been assigned to. Users may be further restricted to only view scan and IDS data that they are authorized to see by the Manager for their customer account. User access to LCE raw log data is configurable on a "per-LCE" basis.
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 that are updated 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 5600 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: • USGCB and SCAP audits • DISA STIG and Checklist audits • CIS audits for Unix, Linux, and Windows • Microsoft vendor recommendations • PCI DSS configuration settings
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	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.
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 browsed 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 SITE	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 processing 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 and 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 to 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 can be used to create reports about attackers, their activities and the logs they have left during an incident.
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.

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.
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 the 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 vulnerabilities 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 (DoS) tests. The LCE can also be used to normalized IDS and other types of logs that pertain to 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 scans 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	The Nessus vulnerability scanner contains thousands of plugins that are updated 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 uses Nessus to log into 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	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-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 D: Tenable Solutions for the Payment Card Industry Data Security Standard (PCI DSS)

Note: This section is based on the content of the PCI Data Security Standards (PCI DSS) version 3.0. Specific requirements are labeled and quoted directly from this document. PCI DSS outlines 12 major security requirements that an organization must adhere to in order to protect customer payment card data. Validation of compliance with the PCI DSS is required on an annual basis either by a Qualified Security Assessor (QSA) or through self-reporting using a Self-Assessment Questionnaire. In addition to satisfying certain requirements directly, Tenable Network Security can help monitor networks that are subject to PCI DSS requirements. Some sub-requirements that are not relevant to Tenable's solution have been omitted to save space.

Tenable Network Security, Inc. is a PCI Approved Scanning Vendor (ASV), and is certified to validate vulnerability scans of Internet-facing systems for adherence of certain aspects of the PCI Data Security Standards (PCI DSS). The Nessus Perimeter Service includes a pre-built static PCI DSS policy that adheres to the requirements of the PCI DSS v3.0. This policy may be used by merchants and providers to initially assess their environments based on PCI DSS requirements, and also to perform vulnerability scans and generate reports that can be validated by qualified Tenable Network Security staff members for the PCI DSS ASV validation requirement.

The following acronyms will be used:

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

PCI Requirement	PCI Testing Procedure	How Tenable Can Help
1.1 Establish and implement firewall and router configuration standards that include the following:	**1.1** Inspect the firewall and router configuration standards and other documentation specified below and verify that standards are complete and implemented as follows:	Tenable's LCE can accept logs from any firewall. Through the SC web interface, users can monitor logs for abuse, connections to key resources and anomalies. The PVS can also enumerate both served and browsed firewall ports, as well as which systems accept connections from the Internet.
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.	**1.2** Examine firewall and router configurations to verify that connections are restricted between untrusted networks and system components in the cardholder data environment	SC can leverage logs from firewalls for analysis to determine if unauthorized protocols are being blocked. This can be complemented with continuous passive monitoring and distributed scanning with Nessus to look for networks with incorrect firewall policies.
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	**1.3** Examine firewall and router configurations—including but not limited to the choke router at the Internet, the DMZ router and firewall, the DMZ cardholder segment, the perimeter router, and the internal cardholder network segment—to determine that there is no direct access between the Internet and system components in the internal cardholder network segment:	SC can use both the LCE and the PVS to list which assets communicate with other assets and on which ports.

1.4 Install personal firewall software on any mobile and/or employee-owned devices that connect to the Internet when outside the network (for example, laptops used by employees), and which are used to also access the network. Firewall configurations include: Specific configuration settings are defined for personal firewall software. Personal firewall software is actively running. Personal firewall software is not alterable by users of mobile and/or employee-owned devices.	**1.4.a** Verify that: Personal firewall software is required for all mobile and/or employee-owned devices that connect to the Internet (for example, laptops used by employees) when outside the network, and which are also used to access the network. Specific configuration settings are defined for personal firewall software. Personal firewall software is configured to actively run. Personal firewall software is configured to not be alterable by users of mobile and/or employee-owned devices. **1.4.b** Verify that: Personal firewall software is installed and configured per the organization's specific configuration settings. Personal firewall software is actively running. Personal firewall software is not alterable by users of mobile and/or employee-owned devices.	Nessus configuration audits can be modified to develop customized audits for these devices to ensure that the right software is installed, is running and is configured correctly.
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, *point-of-sale (*POS*)* terminals, Simple Network Management Protocol (SNMP) community strings, etc.).	**2.1** Choose a sample of system components, and attempt to log on (with system administrator help) to the devices and applications using default vendor-supplied accounts and passwords, to verify that ALL default passwords have been changed. (Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.)	Tenable's Nessus vulnerability scanner includes default password checks for many different applications, operating systems and network devices. Nessus can also be given SNMP credentials in order to audit network devices. The PVS also includes many checks for vendor supplied security issues.
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL	**2.1.1** Verify the following regarding vendor default settings for wireless environments: **2.1.1.a** Verify encryption keys were	The Nessus vulnerability scanner and PVS have many different signatures to check for common SNMP and login settings. In addition, Nessus can audit the active

wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	changed from default at installation, and are changed anytime anyone with knowledge of the keys leaves the company or changes positions **2.1.1.b** Verify default SNMP community strings on wireless devices are required to be changed on installation. **2.1.1.c** Verify default SNMP community strings are not used and passwords/passphrases on access points are not used. **2.1.1.d** Verify firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks. **2.1.1.e** Verify other security-related wireless vendor defaults were changed, if applicable.	wireless domain of each Windows device and this can be used to build a complete list of all wireless devices. The LCE can be used to log system events form network devices such as Wi-Fi appliances, NAT firewalls and other hardware.
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.	**2.2.a** Examine the organization's system configuration standards for all types of system components and verify the system configuration standards are consistent with industry-accepted hardening standards. **2.2.b** Verify that system configuration standards are updated as new vulnerability issues are identified, as defined in Requirement 6.1. **2.2.c** Verify that system configuration standards are applied when new systems are configured. **2.2.d** Verify that system configuration standards include the following procedures for all types of system components:	SC can be configured with audit policies to login to Unix and Windows devices to ensure they have been configured correctly according to the configuration standard. For devices that do not support these types of logins, Nessus and the PVS can be used to profile systems, discover open ports and identify vulnerabilities. Nessus credentialed scans can also list all open UDP and TCP ports on Unix and Windows operating systems and also identify the system process that owns each port.
2.3 Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.	**2.3** Select a sample of system components and verify that non-console administrative access is encrypted by performing the following: **2.3.a** Observe an administrator log on to each system to verify that a strong encryption method is invoked before the administrator's password is requested. **2.3.b** Review services and parameter	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, then it can correlate network traffic with logins to see that only encrypted protocols are being used. Nessus actively tests all SSL systems for compliance with PCI DSS. This includes

	files on systems to determine that Telnet and other insecure remote-login commands are not available for non-console access. **2.3.c** Verify that administrator access to any web-based management interfaces is encrypted with strong cryptography.	verification of host names that keys are tied to and testing the age of the SSL library to ensure it is up to date.
2.4 Maintain an inventory of system components that are in scope for PCI DSS.	**2.4.a** Examine system inventory to verify that a list of hardware and software components is maintained and includes a description of function/use for each.	Through active and passive scanning with Nessus and PVS, respectively, SC has the ability to maintain asset lists of systems, including software found to be installed on systems found within the cardholder data environment.
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements Processes for secure deletion of data when no longer needed Specific retention requirements for cardholder data A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.	**3.1.a** Examine the data retention and disposal policies, procedures and processes to verify they include at least the following: Legal, regulatory, and business requirements for data retention, including Specific requirements for retention of cardholder data (for example, cardholder data needs to be held for X period for Y business reasons). Secure deletion of cardholder data when no longer needed for legal, regulatory, or business reasons Coverage for all storage of cardholder data A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements.	Nessus and the PVS can be used to identify which hosts are serving different types of files, such as spreadsheets being available on a public web server. Nessus has the ability to look into these documents at rest and discover if they have confidential data, such as credit card account information. In addition, this process can be customized to local procedures to look for specific database files, authentication logs and other types of confidential data which is involved with credit card processing.
3.5 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse:	**3.5** Verify processes are specified to protect keys used for encryption of cardholder data against disclosure and misuse and include at least the following:	There are many physical and electronic methods to storing cryptographic keys. SC and the LCE can help identify these systems, report on their security issues and log access to these devices including insertion and removal of USB devices.
4.1 Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard	**4.1 a** Identify all locations where cardholder data is transmitted or received over open, public networks. Verify that the use of security protocols	SC can collect encryption information about the web portals accepting credit card data. This information can be used for reporting by asset type.

sensitive cardholder data during transmission over open, public networks.	and strong cryptography for all locations:	Nessus can be used to recognize the supported protocols that enable encrypted communications. Nessus actively tests all SSL systems for compliance with PCI DSS. This includes verification of host names that keys are tied to and testing the age of the SSL library to ensure it is up to date.
4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).	**4.2.a** If end-user messaging technologies are used to send cardholder data, observe processes for sending PAN and examine a sample of outbound transmissions as they occur to verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies.	SC and the PVS can be configured to test for several items including the presence of encryption software, the detection of an email sent that has been scripted by the software and emails sent that contain credit card data that was not encrypted.
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	**5.1** For a sample of system components including all operating system types commonly affected by malicious software, verify that anti-virus software is deployed if applicable anti-virus technology exists.	SC, Nessus, and the PVS can be used to discover installed anti-virus instances and assets if they have been updated. Nessus can be used to audit systems for the presence of a standard anti-virus solution and to also test that the solution is configured and working properly.
5.2 Ensure that all anti-virus mechanisms are maintained as follows: • Are kept current, • Perform periodic scans • Generate audit logs which are retained per PCI DSS Requirement 10.7.	**5.2 a** Examine policies and procedures to verify that anti-virus software and definitions are required to be kept up to date. **5.2.b** Examine anti-virus configurations, including the master installation of the software to verify anti-virus mechanisms are: Configured to perform automatic updates, and Configured to perform periodic scans. **5.2.c** Examine a sample of system components, including all operating system types commonly affected by malicious software, to verify that: The anti-virus software and definitions are current. Periodic scans are performed. **5.2.d** Examine anti-virus configurations, including the master	SC and Nessus can test for how recently an anti-virus product was updated and if it is running correctly. The LCE can also be used to aggregate logs from anti-virus products. The LCE normalizes logs from many different anti-virus sources, including host-based and network based (such as email anti-virus solutions).

	installation of the software and a sample of system components, to verify that: Anti-virus software log generation is enabled, and Logs are retained in accordance with PCI DSS Requirement 10.7.	
6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.	**6.1.a** Examine policies and procedures to verify that processes are defined for the following: To identify new security vulnerabilities To assign a risk ranking to vulnerabilities that includes identification of all "high risk" and "critical" vulnerabilities. To use reputable outside sources for security vulnerability information. **6.1.b** Interview responsible personnel and observe processes to verify that: New security vulnerabilities are identified. A risk ranking is assigned to vulnerabilities that includes identification of all "high" risk and "critical" vulnerabilities. Processes to identify new security vulnerabilities include using reputable outside sources for security vulnerability information.	SC and Nessus can be used to perform patch audits of Unix, Windows and router devices. This audit can occur across a sampling of the network, or all of it. Patch auditing is highly accurate and has a very low false positive and false negative rate because it uses file-based analysis to ensure that patches are deployed. Other techniques to assess patch deployment status such as looking into the registry do not perform a complete audit. The SC can also show vulnerabilities that have been "discovered" in a certain period of time. This allows reporting vulnerabilities older than 30 days. When considering systems running or operated by different groups, the SC can show which organizations are more efficient at testing and patching their systems. If the LCE or PVS are also deployed on a system, users can receive real-time feedback on how often their systems were updated, accessed and configured. This can be used to show evidence that a system is patched or configured correctly.
6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.	**6.2.a** Examine policies and procedures related to security-patch installation to verify processes are defined for: Installation of applicable critical vendor-supplied security patches within one month of release. Installation of all applicable vendor-supplied security patches within an appropriate time frame (for example, within three months). **6.2.b** For a sample of system components and related software, compare the list of security patches	When managed by the SC, periodic, continuous, daily, and many other types of vulnerability scans can be scheduled with Nessus. Nessus supports both credentialed patch audits as well as network scans. Nessus and PVS plugin information also contains CVSS2 scores to assist in rating impact and severity of vulnerabilities. The PVS watches all network traffic 24x7 and alerts in real time as new vulnerabilities are found. This product has its vulnerability detection rules updated with the same rules as Nessus does. Since it offers no impact on the local network and operates in real-time, this system will alert for new vulnerabilities

	installed on each system to the most recent vendor security-patch list, to verify the following: That applicable critical vendor-supplied security patches are installed within one month of release. All applicable vendor-supplied security patches are installed within an appropriate time frame (for example, within three months).	very reliably. Tenable also publishes its list of new vulnerability checks in a blog and RSS feed that can be used as a third party source for vulnerability information.
6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: • In accordance with PCI DSS (for example, secure authentication and logging) • Based on industry standards and/or best practices. • Incorporating information security throughout the software-development life cycle	**6.3.a** Examine written software development processes to verify that the processes are based on industry standards and/or best practices. **6.3.b** Examine written software development processes to verify that information security is included throughout the life cycle. **6.3.c** Examine written software development processes to verify that software applications are developed in accordance with PCI DSS. **6.3.d** Interview software developers to verify that written software-development processes are implemented.	Any custom application will be built upon 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. Tenable's solutions can also be used to implement and/or measure how a custom asset is being managed per NIST, ITIL and ISO standards.
6.4 Follow change control processes and procedures for all changes to system components. The processes must include the following:	**6.4** Examine policies and procedures to verify the following are defined: Development/test environments are separate from production environments with access control in place to enforce separation. A separation of duties between personnel assigned to the development/test environments and those assigned to the production environment. Production data (live PANs) are not used for testing or development. Test data and accounts are removed before a production system becomes active. Change control procedures related to	SC can help monitor patch levels and change control activity across many different asset groups. From scan to scan, any deviations from policy norms can be highlighted and trended. The LCE can be configured to log access control changes on specific servers and can monitor file MD5 checksums in real-time to detect modifications made during a change-control process.

	implementing security patches and software modifications are documented.	
6.5 Address common coding vulnerabilities in software-development processes as follows: • Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory. • Develop applications based on secure coding guidelines.	**6.5.a** Examine software-development policies and procedures to verify that training in secure coding techniques is required for developers, based on industry best practices and guidance. **6.5.b** Interview a sample of developers to verify that they are knowledgeable in secure coding techniques.	Nessus and the PVS audit the underlying operating system, underlying web servers and in many cases identify common web application security issues such as cross-site scripting and SQL injection issues. In addition, if the LCE is being used to watch any type of Web server, it will detect many of the errors generated by web application attackers which can be further used to identify security issues.
6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	**6.5.1** Injection flaws, particularly SQL injection. (Validate input to verify user data cannot modify meaning of commands and queries, utilize parameterized queries, etc.)	Nessus can check for a variety of well-known SQL injection attacks against web applications. The PVS can also be used to monitor live web sites to look for any type of error message that is indicative of potential SQL, HTML or command injection errors.
6.5.2 Buffer overflows	**6.5.2** Buffer overflow (Validate buffer boundaries and truncate input strings.)	Nessus checks for a variety of well-known vulnerabilities in web servers, applications and databases.
6.5.3 Insecure cryptographic storage	**6.5.3** Insecure cryptographic storage (Prevent cryptographic flaws, use strong cryptographic algorithms and keys)	Nessus can report a wide variety of information about the system's file systems as well as attached devices such as USB drives. Nessus can also attempt to discover files which should be encrypted based on their content.
6.5.4 Insecure communications	**6.5.4** Insecure communications (Properly encrypt all authenticated and sensitive communications)	The PVS checks for communications over a variety of protocols and can recognize and report when insecure communications are detected while in-transit.
6.5.5 Improper error handling	**6.5.5** Improper error handling (Do not leak information via error messages)	The PVS and Nessus will observe if responses to web probes return a 'catch all' error page, or if they return certain types of web error codes. If the LCE is also in use, it can read error logs from web servers and report on them as well.

6.5.6 All “high risk” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).	**6.5.6** Examine software-development policies and procedures (coding techniques address any “high risk” vulnerabilities that could affect the application, as identified in PCI DSS Requirement 6.1.)	Nessus can check for a variety of well-known attacks against web applications, operating systems, and other software. Nessus and PVS plugin information also contains CVSS2 scores and criticality ratings to assist in assessing impact and severity of vulnerabilities.
6.5.7 Cross-site scripting (XSS)	**6.5.7** Cross-site scripting (XSS) (Validate all parameters before inclusion, utilize context-sensitive escaping, etc.)	Nessus checks for a variety of XSS vulnerabilities in common applications and software solutions.
6.5.8 Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions)	**6.5.8** Improper Access Control, such as insecure direct object references, failure to restrict URL access, and directory traversal (Properly authenticate users and sanitize input. Do not expose internal object references to users.)	Nessus and the PVS perform checks for known access control vulnerabilities such as directory traversals and authentication bypass issues.
6.5.9 Cross-site request forgery (CSRF)	**6.5.9** Cross-site request forgery (CSRF). (Do not reply on authorization credentials and tokens automatically submitted by browsers.)	Nessus checks for a variety of CSRF vulnerabilities in common applications and software solutions.
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes • Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.	**6.6** For *public-facing* web applications, ensure that *either* one of the following methods are in place as follows: _ Verify that public-facing web applications are reviewed (using either manual or automated vulnerability security assessment tools or methods), as follows: - At least annually - After any changes - By an organization that specializes in application security - That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment - That all vulnerabilities are corrected - That the application is re-evaluated after the corrections _ Verify that an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) is in place:	Although Tenable does not offer solutions to evaluate source code of web applications, Nessus, the PVS and the LCE can monitor web applications for changes to the application that could imply new vulnerabilities and perhaps a new code review. For application layer firewalls, the LCE can be used to monitor the logs from such devices. Tenable recommends that these logs should also be aggregated with the actual raw logs from the application itself for a complete picture of any security incidents. Application firewalls can also be tested by leveraging external Nessus scanners to perform network scans of web resources.

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	**7.1** Examine written policy for access control, and verify that the policy incorporates 7.1.1 through 7.1.4 as follows: • Defining access needs and privilege assignments for each role • Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities • Assignment of access based on individual personnel's job classification and function • Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved.	Nessus' compliance checks can be used to audit user accounts, specific lists of users and how authentication occurs and is logged. The LCE will normalize all logs based on the user ID of the authenticated user. This allows quick and easy and accurate inspection of all logs in order to see which users have accessed systems with sensitive data. The LCE can also be configured with a list of all valid user accounts that access a particular asset group. When logins occur (failed or successful) the LCE can alert if the user in question is not on the authorized list. In addition, Tenable's sensitive data in motion and at rest detection can look for failures of this policy.
7.2 Establish an access control system for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:	**7.2** Examine system settings and vendor documentation to verify that an access control system is implemented as follows: **7.2.1** Confirm that access control systems are in place on all system components. **7.2.2** Confirm that access control systems are configured to enforce privileges assigned to individuals based on job classification and function. **7.2.3** Confirm that the access control systems have a default "deny-all" setting.	For both Unix and Windows, SC can leverage Nessus' audit policies to ensure that servers and desktops are locked down to least privilege for all users. This includes auditing the configuration of Windows security policies as well as Unix security mechanisms such as su, sudo, and SELinux. Similarly, the LCE can produce lists of users that have logged into various servers. The LCE can produce lists of users that have logged into various servers.
8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:	**8.1.1** All users are assigned a unique ID before allowing them to access system components or cardholder data. **8.1.2** Examine associated authorizations and observe system settings to verify each user ID and privileged user ID has been implemented with only the privileges specified on the documented approval. **8.1.3** Review current user access lists—for both local and remote access—to verify that their IDs have been deactivated or removed from the access lists.	Nessus compliance checks can audit Linux, Unix, and Windows operating systems to ensure that each user account has been configured per a corporate policy. The LCE can be used to show that unique users access servers and then use some sort of facility such as su or sudo to become an administrator. Users can also be tracked with LCE and SC to help ensure that user accounts have been removed or disabled upon termination.

	8.1.4 Observe user accounts to verify that any inactive accounts over 90 days old are either removed or disabled.	
8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric.	**8.2** To verify that users are authenticated using unique ID and additional authentication (for example, a password/phrase) for access to the cardholder data environment, perform the following: _ Examine documentation describing the authentication method(s) used. _ For each type of authentication method used and for each type of system component, observe an authentication to verify authentication is functioning consistent with documented authentication method(s).	Nessus compliance checks can audit Unix and Windows operating systems to ensure that each user account has been configured per a corporate policy. SC can also be used with the LCE to gather the logs from various users accessing various parts of the network. The LCE can process logs from physical access control devices as well as other forms of electronic access control.
8.3 Incorporate two-factor authentication for remote network access originating from outside the network by personnel (including users and administrators) and all third parties, (including vendor access for support or maintenance).	**8.3** Examine system configurations for remote access servers and systems to verify two-factor authentication is required for: All remote access by personnel All third-party/vendor remote access (including access to applications and system components for support or maintenance purposes).	The LCE can be used to monitor logs from these various access control processes. If desired, the LCE can also watch for network connections that were not accompanied by access control events. These logs are used to temporarily associate user IDs to IP addresses for tracking of all user activity.
8.4 Document and communicate authentication procedures and policies to all users including: • Guidance on selecting strong authentication credentials • Guidance for how users should protect their authentication credentials • Instructions not to reuse previously used passwords • Instructions to change passwords if there is any suspicion the	**8.4.a** Examine procedures and interview personnel to verify that authentication procedures and policies are distributed to all users.	Nessus can be used to audit password files to ensure that credentials are properly encrypted and not written “in the clear”. Both the PVS and LCE can also be used to audit protocols for evidence of communications that occur without encryption.

password could be compromised.		
8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: • Generic user IDs are disabled or removed. • Shared user IDs do not exist for system administration and other critical functions. • Shared and generic user IDs are not used to administer any system components.	**8.5.a** For a sample of system components, examine user ID lists to verify the following: Generic user IDs are disabled or removed. Shared user IDs for system administration activities and other critical functions do not exist. Shared and generic user IDs are not used to administer any system components.	A combination of the Nessus configuration audits as well as the LCE's ability to audit user access modifications and user creation and deletion can be accomplished.
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	**9.1** Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems in the cardholder data environment. _ Verify that access is controlled with badge readers or other devices including authorized badges and lock and key. _ Observe a system administrator's attempt to log into consoles for randomly selected systems in the cardholder environment and verify that they are "locked" to prevent unauthorized use.	The LCE can be used to track logs generated by these devices. If these logs are tied to a common account, the LCE can also then tie physical access to virtual login events. If the logins are tied to servers or networks at a particular physical facility, SC can be used to highlight those devices as part of a single asset group. This can make auditing physical access control events easier.
10.1 Implement audit trails to link all access to system components to each individual user.	**10.1** Verify through observation and interviewing the system administrator, that audit trails are enabled and active for system components and access to system components is linked to individual users.	Multiple LCEs can be used to aggregate multiple types of log sources. These can be chained together with basic time or IP address analysis, and/or more advanced scripting can be used to correlate disparate login processes.
10.2 Implement automated audit trails for all system components to reconstruct the following events:	**10.2** Through interviews of responsible personnel, observation of audit logs, and examination of audit log settings, perform the following:	SC can use compliance checks to audit servers to ensure proper logging is enabled. LCEs can be used to aggregate and normalize these audit logs.
10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.	**10.4** Examine configuration standards and processes to verify that time-synchronization technology is implemented and kept current per PCI DSS Requirements 6.1 and 6.2.	If NTP is required by policy for an organization, SC and Nessus can audit remote systems to ensure that they have been configured to use it. The version of NTP is also logged by Nessus during vulnerability scans. Any

		vulnerability associated with NTP will also be analyzed. The PVS can identify which devices are making NTP queries to the Internet. Similarly, the LCE can also provide this information when monitoring networks with the Tenable Network Monitor.
10.5 Secure audit trails so they cannot be altered.	**10.5** Interview system administrators and examine permissions to verify that audit trails are secured so that they cannot be altered as follows:	LCE uses agents that can cryptographically protect the logs in motion. In addition, SC can be used to audit itself and the LCE for security issues. The LCE can also monitor itself for activity.
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.	**10.6.1.a** Examine security policies and procedures to verify that procedures are defined for reviewing the following at least daily, either manually or via log tools: All security events Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD Logs of all critical system components Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.) **10.6.1.b** Observe processes and interview personnel to verify that the following are reviewed at least daily: All security events Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD Logs of all critical system components Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS),	SC and the LCE make analysis of all logs very easy. Tenable's correlation technology makes analysis of IDS events efficient and can highlight which events target critical and vulnerable systems. SC allows organizations to develop flexible alerting procedures for specific types of log and IDS events.

	authentication servers, e-commerce redirection servers, etc.).	
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	**10.7.a** Examine security policies and procedures to verify that they define the following: Audit log retention policies Procedures for retaining audit logs for at least one year, with a minimum of three months immediately available online. **10.7.b** Interview personnel and examine audit logs to verify that audit logs are available for at least one year. **10.7.c** Interview personnel and observe processes to verify that at least the last three months' logs can be immediately restored for analysis.	The LCE can be used to front end a log storage process. Either all normalized logs can be stored (from event reduction) or all gathered logs can be stored. The LCE can keep 3 months of logs "online" and store logs that are no longer available in an archive. Any log in this archive can be chosen to have analysis performed on. Tenable customers specify SAN or NAS storage for LCE to place their archived logs into and then SC users can choose these archives by date.
11.1 Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.	**11.1.a** Examine policies and procedures to verify processes are defined for detection and identification of both authorized and unauthorized wireless access points on a quarterly basis. **11.1.b** Verify that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following: _ WLAN cards inserted into system components _ Portable wireless devices connected to system components to create a wireless access point (for example, by USB, etc.) _ Wireless devices attached to a network port or network device **11.1.c** Examine output from recent wireless scans to verify that: Authorized and unauthorized wireless access points are identified, and The scan is performed at least quarterly for all system components and facilities. **11.1.d** If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), verify the configuration will generate alerts to notify personnel.	SC and the Nessus scanner can be used to discover wireless access points and place these in asset groups. Then a query can be performed to show if any of these networks has made connections to the payment card network. Nessus can also identify if end system nodes belong to a wireless domain. This information can be used to find unknown or unauthorized wireless access points. The LCE can make use of any log and discover MAC addresses associated with wireless devices on them.

11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). **11.2.1** Perform quarterly internal vulnerability scans and rescans as needed, until all "high-risk" vulnerabilities (as identified in Requirement 6.1) are resolved. Scans must be performed by qualified personnel. **11.2.2** Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved**.** **11.2.3** Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.	**11.2.1.a** Review the scan reports and verify that four quarterly internal scans occurred in the most recent 12-month period. **11.2.1.b** Review the scan reports and verify that the scan process includes rescans until all "high-risk" vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved. **11.2.1.c** Interview personnel to verify that the scan was performed by a qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV). **11.2.2.a** Review output from the four most recent quarters of external vulnerability scans and verify that four quarterly external vulnerability scans occurred in the most recent 12-month period. **11.2.2.b** Review the results of each quarterly scan and rescan to verify that the ASV Program Guide requirements for a passing scan have been met (for example, no vulnerabilities rated 4.0 or higher by the CVSS, and no automatic failures). **11.2.2.c** Review the scan reports to verify that the scans were completed by a PCI SSC Approved Scanning Vendor (ASV).	SC can be used to scan as often as needed to discover new hosts, changes in topology, and the presence of new vulnerabilities. This capability is further enhanced with passive vulnerability analysis through direct network monitoring. SC can keep the results of all network scans and patch audits online, including the results from the quarterly scans for the most recent 12 month period. Nessus includes a set of PCI DSS auditing plugins that ensure the requirements of each scan (full port scan, all checks enabled, etc.) are met. Tenable is a PCI Approved Scanning Vendor (PCI ASV) and can validate adherence to certain DSS requirements by performing vulnerability scans of Internet-facing environments (external scanning) through the Nessus Perimeter Service.
11.3 Implement a methodology for penetration testing that includes the following:	**11.3** Examine penetration-testing methodology and interview responsible personnel to verify a methodology is implemented that includes the following: Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115) Includes coverage for the entire CDE perimeter and critical systems Testing from both inside and outside the network Includes testing to validate any	Tenable's solutions offer many ways to discover what a penetration test *may* find. With credentialed scans, SC will know all missing patches on all systems. Nessus' vulnerability scans do not exploit targets, but they do test for the actual presence of a vulnerability. The PVS not only discovers systems and applications you may not have considered to scan, it also finds their vulnerabilities and trust relationships. SC, PVS and LCE can also emphasize when significant changes to the infrastructure have occurred.

	segmentation and scope-reduction controls Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 Defines network-layer penetration tests to include components that support network functions as well as operating systems Includes review and consideration of threats and vulnerabilities experienced in the last 12 months Specifies retention of penetration testing results and remediation activities results.	
11.4 Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date**.**	**11.4.a** Examine system configurations and network diagrams to verify that techniques (such as intrusion-detection systems and/or intrusion-prevention systems) are in place to monitor all traffic: At the perimeter of the cardholder data environment At critical points in the cardholder data environment. **11.4.b** Examine system configurations and interview responsible personnel to confirm intrusion-detection and/or intrusion-prevention techniques alert personnel of suspected compromises. **11.4.c** Examine IDS/IPS configurations and vendor documentation to verify intrusion-detection and/or intrusion-prevention techniques are configured, maintained, and updated per vendor instructions to ensure optimal protection.	SC and LCE can accept logs from IDS devices. SC performs correlation on these events with vulnerability data to reduce false positives while also minimizing false negatives. LCE can also perform event correlation on IDS events as well as correlate IDS events with anomalistic activity.
11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform	**11.5.a** Verify the use of a change-detection mechanism within the cardholder data environment by observing system settings and monitored files, as well as reviewing results from monitoring activities. _ System executables _ Application executables _ Configuration and parameter files	Nessus configuration auditing can be used to monitor when certain files change their value on Unix servers. 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

critical file comparisons at least weekly.	_ Centrally stored, historical or archived, log and audit files **11.5.b** Verify the mechanism is configured to alert personnel to unauthorized modification of critical files, and to perform critical file comparisons at least weekly.	and correlate these events with suspicious events and IDS attacks.
12.1 Establish, publish, maintain, and disseminate a security policy.	**12.1** Examine the information security policy and verify that the policy is published and disseminated to all relevant personnel (including vendors and business partners).	For any security policy, Tenable's solutions can help an organization monitor the configuration of their environment for adherence to that policy.
12.2 Implement a risk-assessment process that: • Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), • Identifies critical assets, threats, and vulnerabilities, and • Results in a formal risk assessment.	**12.2.a** Verify that an annual risk-assessment process is documented that identifies assets, threats, vulnerabilities, and results in a formal risk assessment. **12.2.b** Review risk-assessment documentation to verify that the risk-assessment process is performed at least annually and upon significant changes to the environment.	SC can simplify complex relationships between vulnerabilities, IDS events, logs, configurations and asset classes. This can help organizations identify asset groups, technologies or business units that are at risk.
12.3 Develop usage policies for critical technologies and define proper use of these technologies.	**12.3** Examine the usage policies for critical technologies and interview responsible personnel to verify the following policies are implemented and followed:	Wireless or modem communication as well as laptop use can be audited for with Nessus' compliance audit policies. SC and Nessus can be used to identify all systems that contain modems.
12.5 Assign to an individual or team the following information security management responsibilities:	**12.5** Examine information security policies and procedures to verify: The formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management. The following information security responsibilities are specifically and formally assigned:	SC can be used as a communications platform for all shareholders involved in the incident response, vulnerability management, and compliance monitoring solutions. Tenable's solutions make it easy to share logs, vulnerabilities, incidents and many other types of data that affect PCI compliance.
12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.	**12.5.2** Verify that responsibility for monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel is formally assigned.	SC can be used to monitor large amounts of logs and security events and to also share this data with end user system administrators and security staff particular to asset types. Critical alerts can be sent automatically and end users can also analyze their alerts through the SC web interface.

		The LCE can also help make sense of large volume of logs and alerts with automatic anomaly detection, sophisticated correlation rules which look for events that effect compliance and correlation of alerts with known network vulnerabilities.
12.8 Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:	**12.8** Through observation, review of policies and procedures, and review of supporting documentation, verify that processes are implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data (for example, backup tape storage facilities, managed service providers such as web-hosting companies or security service providers, those that receive data for fraud modeling purposes, etc.), as follows:	The PVS can be used to gain information about third parties without actually scanning them. Vulnerability and compliance information can be gathered to SC with just a few PVS installations. Nessus scanners subscribed to Tenable's plugin downloads can also be used to perform a scan of these vendors to see if there are any glaring PCI DSS issues.

Appendix E: Tenable Solutions for Auditing Controls with COBIT 5

Note: This section is a mapping of specific COBIT 5 control objectives and IT processes which Tenable's solutions can assist in. Only specific sub-sections related to Tenable solutions have been entered.

The following acronyms will be used:

IDS – Intrusion Detection System
SC – SecurityCenter
LCE – Log Correlation Engine
PVS – Passive Vulnerability Scanner

Process	Name	How Tenable Can Help
EDM	**Evaluate, Direct and Monitor**	
EDM01	**Ensure Governance Framework Setting and Maintenance**	
EDM01.03	Monitor the governance system	Monitor the effectiveness and performance of the governance system and implemented mechanisms (including structures, principles and processes) are operating effectively and provide appropriate oversight of IT.
EDM02	**Ensure Benefits Delivery**	
EDM02.01	Evaluate value optimization	SC, along with distributed Nessus and PVS scanners, can identify devices, operating systems and applications that are not part of the current plan by IT.
EMD02.03	Monitor value optimization	SC, along with LCE, PVS, and Nessus can generate metrics, identify significant issues, and assist in formulating corrective actions that help measure the value and benefits of resources within the IT infrastructure.
EDM03	**Ensure Risk Optimization**	
EDM03.01	Evaluate risk management	Data contained and collected by SC can be used to distill an overall status of an enterprise's exposure to IT risk. SC can help visualize how this information is related to strategic asset groups, as well as comparisons of various technologies. This presentation can help management understand where the security risks are occurring. In addition, if a corporation has acquired or is about to acquire a third party, management can also use SC to understand how their level of risk compares to the current level.
EDM03.03	Monitor risk management	Tenable's solutions can help this process in two ways. First, for any type of patch management and configuration management policies, SC can be used to audit the current state of network resources. Second, for any technologies deployed, SC can be used to test the effectiveness of controls as well as aggregate logs and events from multiple control points to provide up-to-date system data and direction for risk management.
EDM04	**Ensure Resource Optimization**	
EDM04.01	Evaluate resource management	SC, along with Nessus and PVS, allows organizations to view all IT resources in their environment and determine which resources may need to be enhanced, replaced, or reallocated.

EDM04.03	Monitor resource management	SC, along with Nessus and PVS, allows organizations to monitor resource management and identify how problems can be tracked, reported, and remediated.
EDM05	**Ensure Stakeholder Transparency**	
EDM05.02	Direct stakeholder communication and reporting	SC is capable of generating various reports for stakeholders across an organization, including executive and compliance reports, to ensure information oversight and communication.
APO	**Align, Plan and Organize**	
APO01	**Manage the IT Management Framework**	
APO01.01	Define the organizational structure	Use of SC to aggregate security, event and compliance data by large asset groups can be done on a “technology-specific” basis. This can allow an architectural board to have relevant and timely information about how the corporation’s technology has been deployed and is in use. SC is very flexible when it comes to implementing an access control policy based on need to know. Regardless of the topology of the organization chart for IT, end users, managers and auditors will only have access to what they are authorized to analyze.
APO01.02	Establish roles and responsibilities	SC can accommodate a wide variety of roles. These can be used to segment creation of users, deciding what users can/can’t do, and analyzing user activity. This allows SC to fit into any type of organizational structure. The LCE can be used to analyze system logs to determine if access control policies are being followed. SC can use Nessus compliance audits to also ensure that systems are locked down to “least use” principles.
APO01.03	Maintain the enablers of the management system	With a common set of assets that are recognizable to both the business owners and the IT owners, SC can be used to report and manage risk for many types of assets. For example, from a business perspective, there may be a complex asset named “PeopleSoft”. This asset may in turn be made up of many different IT functions such as “Database”, “Web Server”, and “Switching”. SC can be used to view and report security, compliance and incident data to the organization by providing unique views of the same data.
APO01.04	Communicate management objectives and direction	SC can be used to communicate both discreet and broad changes that need to occur to maintain a compliant network. SC’s set of ticketing tools is designed to use minimal amounts of ticketing, yet allow security and compliance managers the ability to observe broad issues as well as make small changes to some assets.
APO01.05	Optimize the placement of the IT function	SC, Nessus, PVS, and LCE are easily scalable to the size and requirements of any enterprise model, and can gather and report data according to the criticality of each IT asset.
APO01.06	Define information (data) and system ownership	SC can capture information for asset groups and their owners. This enables prioritization of Recovery Point Objectives during incident response, reporting and remediation that can be assigned to wide or granular ownership levels.
APO01.07	Manage continual improvement of processes	All of Tenable’s products can be used to measure or monitor the compliance status of any given asset and help improve upon remediation and reporting processes.

APO01.08	Maintain compliance with policies and procedures	All of Tenable's products can be used for instant audits and continuous monitoring for a variety of compliance policies. As decisions are made as to which events and configurations are to be used, SC and all other Tenable products can be used to test the network or monitor for those events. As policies are added into the operations of an organization, SC can be used to alert end users of deviations from those policies. Corrective actions can also be alerted directly to end users through SC.
APO02	**Manage Strategy**	
APO02.01	Understand enterprise direction	SC can be configured with business names and rules that reflect what executive management is expecting. In other words, SC can present all of the security information available consistently to everyone authorized in the company, regardless of level.
APO02.02	Assess the current environment, capabilities, and performance	All of Tenable's products can be used to obtain both high-level and detailed information about an organization's IT environment. SC and LCE are able to monitor system performance and identify issues in the IT environment that can impact business operations.
APO02.03	Define the target IT capabilities	SC can be used during the research phase of a plan to identify security, compliance, and performance issues that need to be addressed by the overall IT and business strategies.
APO02.04	Conduct a gap analysis	SC can be used during the research phase of a plan to identify security, compliance, and performance issues that need to be addressed by the overall IT and business strategies.
APO03	**Manage Enterprise Architecture**	
APO03.02	Define reference architecture	SC can be used to standardize various security event names and severity levels for vulnerabilities across a wide range of different asset groups. SC can also be used to securely share security information from vulnerability scans, patch audits, configuration audits, intrusion detection events, normalized logs and many other sources. Systems containing data that has been classified as being sensitive can be highlighted in SC as a unique asset group. The vulnerabilities and security events associated with these assets can then be handled uniquely. In addition, once data has been classified, it can be scanned for with Nessus.
APO03.05	Provide enterprise architecture services	Many aspects of Tenable's technologies can be used to detect unauthorized technologies and to also ensure that deployed technologies have been done so with best practices and per corporate policies for compliance monitoring.
APO04	**Manage Innovation**	
APO04.06	Monitor the implementation and use of innovation	SC, Nessus, and PVS are all capable of monitoring the implementation and use of new technologies, including various types of software, hardware, and mobile devices, as they are deployed across an IT environment.
APO05	**Manage Portfolio**	
APO05.01	Establish the target investment mix	SC is able to provide an overview of current IT technologies and the services provided by those technologies, as well as help determining current risk levels and what resources may provide the best ROI based on use and availability.

APO05.05	Maintain portfolios	In large enterprise networks, a single resource can be part of several different projects. Since each project is managed independently, SC has been designed to also manage assets as independent groups, even though some components may also reside in other assets.
APO06	**Manage Budget and Costs**	
APO06.01	Manage finance and accounting	SC's ability to aggregate and discover asset information can ensure that the IT group has an accurate knowledge of what assets are in use on their network for budget purposes.
APO06.02	Prioritize resource allocation	SC may be able to show a variety of return on investment reports for solutions deployed such as patch management, intrusion prevention, content filtering, and more. In a large organization, SC will be able to show before and after reports as this technology is deployed. This can help prioritize devices and technologies that have a high return on investment.
APO06.03	Create and maintain budgets	SC, Nessus, and the PVS can be used to identify all hosts and applications on the network. This can help assist in discovering what has been deployed and is in use. This can also help identify which software and hardware contracts need to have renewed maintenance.
APO07	**Manage Human Resources**	
APO07.01	Maintain adequate and appropriate staffing	Lists of authorized or unauthorized users can be sent to the LCE to find abuse in access control policies or attempts to re-use older accounts. SC and the LCE can be used to monitor access control and audit logs to ensure that only authorized employees have access to systems. On a broader scale, SC and the PVS can be used to observe organizational access to network assets to see if these adhere to a corporate policy. Both Nessus and the LCE can audit lists of user accounts that have access to various servers and assets. Organizations can employ the LCE to search for deviations from a "white list" of authorized users or search for login attempts using a "black list" of accounts no longer active.
APO07.03	Maintain the skills and competencies of personnel	Feedback from data gathered by SC about existing vulnerabilities, IDS events and globally outstanding issues can be fed into the training content. For example, if there were a large number of outstanding issues keeping anti-virus tools up to date, this problem can be highlighted in ongoing training.
APO08	**Manage Relationships**	
APO08.02	Identify opportunities, risks and constraints for IT to enhance the business	SC and LCE are capable of monitoring enterprise-wide system resources and performance, which enables an IT organization to identify areas where the overall business strategy can be enhanced through procurement and deployment of additional resources.
APO08.05	Provide input to the continual improvement of services	Reports generated through SC can provide an organization with detailed and timely data about enterprise IT resources, which helps with the overall decision-making process when improving upon existing business and IT services.
APO09	**Manage Service Agreements**	
APO09.01	Identify IT services	SC, using Nessus and PVS, can identify and report on all IT-enabled services that are active on the enterprise network.

APO09.02	Catalogue IT-enabled services	Users within SC can be given access to view specific asset groups, which can be grouped by organizational departments or IT-enabled services.
APO09.03	Define and prepare service agreements	For any service level agreements that speak specifically about change management or security monitoring, Tenable's solutions can be used to report on these metrics.
APO09.04	Monitor and report service levels	For any service level agreements specifically regarding change management or security monitoring, Tenable's solutions can be used to report on these metrics.
APO9.05	Review service agreements and contracts	All of Tenable's products can help produce data that can be applied to a variety of SLAs.
APO10	**Manage Suppliers**	
APO10.01	Identify and evaluate supplier relationships and contracts	At the network level, the PVS and LCE can be used to identify access from third party organizations. This can help ensure that management knows about all third party connections into the network or applications.
APO10.04	Manage supplier risk	A security profile of the IT components of a remote supplier can be measured with the PVS. This may provide enough information to raise suspicion that a supplier is not conforming to basic security guidelines. If the remote supplier submits to a network scan, SC can also identify many security issues on the supplier's network.
APO10.05	Monitor supplier performance and compliance	The LCE can be used to monitor access and activity from third party suppliers accessing the network.
APO11	**Manage Quality**	
APO11.04	Perform quality monitoring, control, and reviews	SC and LCE all have the ability to assist in quality assurance reviews through performance measurement, analysis, and reporting.
APO11.05	Integrate quality management into solutions for development and service delivery	SC's, Nessus', PVS's, and LCE's ability to discover new hosts, new applications, change to servers, changes to user accounts and un-authorized configurations allows it to be useful in finding assets that do not meet basic acquisition standards. For example, SC can make use of Nessus local compliance checks to discover unauthorized software.
APO12	**Manage Risk**	
APO12.01	Collect data	SC can be used to identify a wide variety of changes in the network that may expose or limit a vulnerability. In addition, the LCE and PVS can be used for real-time event monitoring. When combined with asset information from SC, a wide variety of business rules can be implemented that identify critical events that affect organizational risk, security and compliance.
APO12.02	Analyze risk	All of Tenable's product suite can measure the amount of vulnerabilities present on any given network or asset group. It can also track the security and compliance events that have been detected. This data can be comparatively displayed among several different asset groups. This allows both "pure" and "relative" risk assessments to be performed.

APO12.03	Maintain a risk profile	Enterprise networks and applications are complex and have many functions. Establishing a risk model to assess such a network is often a unique exercise for each enterprise network. SC can use a combination of active, passive and host-based assessment methods from trusted and untrusted sources. This allows SC to be used to have input into any risk measurement process.
APO12.04	Articulate risk	IT-related vulnerabilities and compliance gaps can be reported to stakeholders through SC and Nessus reporting. Reports can be scheduled for automatic generation or generated and communicated on-demand.
APO12.05	Define a risk management action portfolio	SC, the PVS, Nessus and the LCE can all be used to monitor how any risk action plan is being implemented. For example, if the risk plan states that all critical vendor security patches should be implemented within 90 days, SC can audit assets for deviations from this policy.
APO12.06	Respond to risk	SC can be configured with risk owners for various asset groups. These risk owners can use SC to determine appropriate responses to new vulnerability and threat information.
APO13	**Manage Security**	
APO13.01	Establish and maintain an information security management system (ISMS)	SC, while using Nessus, PVS, and LCE, provides a comprehensive approach to unified security monitoring. All of Tenable's products help to enhance an organization's security and compliance posture through the gathering, analysis, and reporting of information security and IT system-related data.
APO13.02	Define and manage an information security risk treatment plan	All of Tenable's products can be used to implement a variety of security plans at various levels throughout IT. Flexible vulnerability management can be performed with SC, Nessus and the PVS. Configuration analysis can be performed with Nessus and SC. Log retention, intrusion detection and access control verification can also be performed with LCE.
APO13.03	Monitor and review the ISMS	SC users can include system administrators, security and compliance personnel, auditors, and members of business units across an enterprise. SC allows users to be grouped by function, and groups can be given access to only the data that is relevant for their position, or data can be shared across groups for ease of communication, strategic planning, and enhancing or improving the ISMS.
BAI	**Build, Acquire and Implement**	
BAI01	**Manage Programs and Projects**	
BAI01.09	Manage program and project quality	When aligned with a QMS, SC, Nessus, PVS and LCE all have the ability to discover new hosts, new applications, change to servers, changes to user accounts and un-authorized configurations to find assets that do not meet basic program standards. For example, SC can make use of Nessus local compliance checks to discover unauthorized software.
BAI01.10	Manage program and project risk	SC, Nessus, the PVS, and the LCE can be used to report on current risks present in a project. This can be used to justify new or different technology that may mitigate the current risks.
BAI01.11	Monitor and control projects	Projects that have the ability to cause unwanted changes in the network can be monitored by SC. For example, if an organization is deploying a new type of management technology, SC and the LCE can be used to monitor logs for changes that might be incurred by the new technology.

BAI02	Manage Requirements Definition	
BAI02.01	Define and maintain business functional and technical requirements	SC can be used to identify technology deployed at an organization to ensure that it complies with procurement policies. For example, if all desktop hardware is supposed to run a Microsoft OS, scanning and monitoring for Linux or OS X computers would identify a non-conformity with functional and technical requirements.
BAI02.03	Manage requirements risk	SC, Nessus, PVS, and LCE can be used to report on current risks present in the organization. This can be used to justify new technology that may mitigate the current risks.
BAI03	**Manage Solutions Identification and Build**	
BAI03.02	Design detailed solution components	Tenable's suite of solutions can be used to monitor a variety of commercial applications and can be easily customized to monitor proprietary ones as well.
BAI03.03	Develop solution components	SC can actively and passively monitor the network for thousands of different applications and much more different vulnerabilities. These applications and underlying operating systems can have their configurations audited against recommended vendor, corporate or government policies.
BAI03.04	Procure solution components	If only certain types of hardware and software are procured, SC can monitor for deviations from this policy. This can find places within the enterprise that have procured technology outside of the official procurement process.
BAI03.05	Build solutions	Tenable's suite of solutions can be used to monitor a variety of commercial applications and can be easily customized to monitor proprietary ones as well. The concept is to develop baselines that can be audited with Nessus and scanned to include the presence of vulnerabilities, but then to also monitor the network in real-time with log analysis and packet capture to discover change, incorrect usage and compromise events.
BAI03.06	Perform quality assurance	SC, Nessus, PVS, and LCE can gather data during a quality assurance testing phase to make sure that solution components are performing as expected and do not introduce any new vulnerabilities into the enterprise environment.
BAI03.07	Prepare for solution testing	Any new products being deployed can go through a feasibility test to determine that they can pass an audit by SC as well as generate audit logs within the LCE's framework.
BAI03.08	Execute solution testing	Any new products being deployed can go through a feasibility test to determine that they can pass an audit by SC as well as generate audit logs within the LCE's framework.
BAI03.10	Maintain solutions	Tenable's product suite can help identify authorized and unauthorized changes such as patch deployment and access control list modifications.
BAI03.11	Define IT services and maintain the service portfolio	SC can track workflow and tickets for cases to ensure that changes in service options or definitions are included in the incident tracking and incident response processes.

BAI04	Manage Availability and Capacity	
BAI04.01	Assess current availability, performance and capacity and create a baseline	SC can provide accurate counts of various system types deployed on a network and how often they are used. SC and LCE can monitor availability and performance of system resources and show deviations from established baselines.
BAI04.02	Assess business impact	SC can provide accurate counts of various system types deployed on a network and how often they are used.
BAI04.04	Monitor and review availability and capacity	SC and LCE can monitor availability and performance of system resources and show deviations from established baselines. In addition, continuous network monitoring of resources can be accomplished with the PVS.
BAI04.05	Investigate and address availability, performance and capacity issues	SC can generate alerts from the LCE when system logs indicate that an issue has arisen that affects system or network availability, performance, and capacity. Alerting and ticketing options within SC ensure that appropriate personnel is notified to address issues found by SC and LCE.
BAI05	**Manage Organizational Change Enablement**	
BAI05.06	Embed new approaches	As changes take effect within an organization, SC can be used to track implemented changes, identify issues that need remediation, and enforce compliance with policies and procedures within the enterprise environment.
BAI05.07	Sustain changes	Data gathered by SC about existing vulnerabilities, IDS events, and globally outstanding issues can be fed into the training content. For example, if there were a large number of outstanding issues keeping anti-virus tools up to date, this problem can be highlighted in ongoing training.
BAI06	**Manage Changes**	
BAI06.01	Evaluate, prioritize and authorize change requests	SC can provide data on security and compliance issues that need to be remediated through a change management process. Various data points can help IT and business leaders evaluate and prioritize changes according to enterprise risk and impact to business operations.
BAI06.02	Manage emergency changes	Many different types of changes can be detected by SC and related products. Combinations of real-time and periodic tests can identify changes from repeated scans, system audits, log analysis and packet/network-traffic capture.
BAI06.03	Track and report change status	SC can use a variety of tests to determine if a machine is vulnerable or configured in a specific manner. These tests can be used to verify that a change has occurred. The LCE can also be used to view if systems have been accessed by an authorized administrator to make a change.
BAI06.04	Close and document the changes	SC can use a variety of tests to determine if a machine is vulnerable or configured in a specific manner. These tests can be used to verify that a change has occurred.
BAI07	**Manage Change Acceptance and Transitioning**	
BAI07.04	Establish a test environment	SC and Nessus can be used in a test environment to ensure that test systems adhere to established compliance standards for that environment. If the test environment is to mirror a production environment, scan results can

		be compared to understand where any gaps exist.
BAI07.05	Perform acceptance tests	SC can be used to test and re-test applications before, during and after changes. If applications are changed in parallel, both applications can be audited. SC can also be used to capture a credentialed or un-credentialed vulnerability scan as proof of how an application or set of applications was configured.
BAI07.06	Promote to production and manage releases	SC and Nessus can be used to test for software deployments as they are pushed into a production environment and identify where any deployment problems may exist. If a roll-back is needed, SC and Nessus can also test for the presence of a reverted software package.
BAI07.07	Provide early production support	All of Tenable's products can be used in production support efforts after a production release, including ticketing and alerting for security and compliance issues that may arise after a deployment.
BAI07.08	Perform a post-implementation review	SC can help report on a new implementation and provide data that can be used to compare production activity against expected outcomes of the deployment.
BAI08	**Manage Knowledge**	
BAI08.01	Nurture and facilitate a knowledge-sharing culture	As business owners and end users begin to operate their assets, SC can be modified to reflect the new owners for security and compliance issues.
BAI08.02	Identify and classify sources of information	SC can help identify and classify systems, software, users, networks, and many more different types of information sources.
BAI08.03	Organize and contextualize information into knowledge	As business owners begin to operate their assets, SC can be modified to reflect the new owners for security and compliance issues.
BAI08.04	Use and share knowledge	Reports generated by SC can be distributed to individual users or groups, and custom reports help to provide specific information of interest to specific users or groups within an organization.
BAI09	**Manage Assets**	
BAI09.01	Identify and record current assets	All assets on a network, including servers, workstations, appliances, network devices, and mobile devices, can be identified and classified by physical or logical groups when using SC, Nessus, and PVS. Software is also identified and recorded and can be filtered on to obtain deployment statistics.
BAI09.02	Manage critical assets	Critical assets can be placed into an asset group or groups in SC for one-view tracking, vulnerability and compliance scanning, and issue remediation.
BAI09.04	Optimize asset costs	SC can be used to review an organization's hardware and software assets to identify systems and packages that may need to be replaced and accounted for in future budgets.
BAI09.05	Manage licenses	SC can be used to account for all installed software packages and versions, making the license management process easier for tracking and budgeting purposes.

BAI10	Manage Configuration	
BAI10.01	Establish and maintain a configuration model	SC's active and passive techniques can help to identify systems, assets and applications that exist on the current network. These systems can have their current configurations extracted with a variety of Tenable tools, or they can be audited against a plethora of templates available from Tenable such as configuration policies from CIS, NIST, NSA, many different vendors and a variety of other compliance regulations.
BAI10.02	Establish and maintain a configuration repository and baseline	SC's active and passive techniques can help to identify systems, assets and applications that exist on the current network. These systems can have their current configurations extracted with a variety of Tenable tools, or they can be audited against a plethora of templates available from Tenable such as configuration policies from CIS, NIST, NSA, many different vendors and a variety of other compliance regulations.
BAI10.03	Maintain and control configuration items	SC can make use of Nessus' local configuration audit policies to check all or specific asset groups if they have been configured to corporate policy. As these policies change, the audit policies SC uses can also be changed.
BAI10.04	Produce status and configuration reports	SC and Nessus can be used to independently sample or broadly test for various configuration settings across an enterprise network. Configuration reports can be generated by SC to identify systems that are either in compliance or out of compliance with established configuration baselines.
BAI10.05	Verify and review integrity of the configuration repository	Asset lists and audit files can be maintained through SC to ensure that configuration baselines are reviewed and kept up-to-date with the most recent organizational standards.
DSS	**Deliver, Service and Support**	
DSS01	**Manage Operations**	
DSS01.01	Perform operational procedures	For the processing of sensitive messages, the LCE can be used to capture and analyze any audit trail of the systems generating and receiving the messages. SC can regularly perform security and compliance audits within regularly scheduled outage windows. For more in-depth auditing, Nessus can be used to scan servers and desktops for files that contain sensitive information.
DSS01.02	Manage outsourced IT services	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 usage and hours of operation.
DSS01.03	Monitor IT infrastructure	The LCE can be used to gather logs from many sources that can have an impact on IT operations. Exposing firewall, network sessions, security logs and hundreds of other devices in a common and normalized manner can enhance IT response time and increase knowledge about complex networks.
DSS02	**Manage Service Requests and Incidents**	
DSS02.01	Define incident and service request classification schemes	All of Tenable's products can be used to monitor complex IT networks in real-time for occurrences of defined security incidents, and incidents can be classified by type or severity. Tenable's vulnerability to IDS event

		correlation, log anomaly and scripting languages can be used to recognize when new incidents have occurred and classify them accordingly.
DSS02.02	Record, classify and prioritize requests and incidents	SC can record and incidents through ticketing functionality, and incidents are classified as a ticket is entered, allowing for prioritization in workflow and communication across support personnel and teams.
DSS02.04	Investigate, diagnose and allocate incidents	As incidents are reported, SC can be used to gather and log information about the hosts involved. Data collected by Tenable's products, including Nessus' malware detection capabilities, can help determine the limit of an incident. Ticketing and alerting functionality in SC enhances incident response operations and remediation efforts.
DSS02.05	Resolve and recover from incidents	Knowledge about incidents that have occurred on specific servers can be recorded through SC. SC and Nessus can be used to independently sample or broadly test for various configuration settings across an enterprise network. Repeated scans by SC as well as continuous network monitoring with the PVS can be used to identify acceptable or unacceptable network traffic after an incident has occurred, leading to faster incident recovery.
DSS02.06	Close service requests and incidents	Knowledge about incidents that have occurred on specific servers can be recorded through SC, and tickets can be closed through SC once an incident has been resolved.
DSS02.07	Track status and produce reports	If some issues, outages or incidents have corresponding logs associated with them, the LCE can be used to produce trend reports.
DSS03	**Manage Problems**	
DSS03.01	Identify and classify problems	Vulnerabilities, events, and incidents can all be identified, categorized, and classified through SC, Nessus, PVS, and LCE.
DSS03.02	Investigate and diagnose problems	Knowledge about the configuration, present vulnerabilities, present applications and system logs can be of great benefit to an IT analyzing problems. SC can be used to give IT access to this information securely.
DSS03.03	Raise known errors	Known vulnerabilities discovered by Nessus and PVS are reported along with possible solutions or workarounds. Tickets allow a history to be kept for incident resolution, which can include unique remediation solutions or workarounds.
DSS03.04	Resolve and close problems	Ticking functionality in SC allows for problem tracking from discovery to resolution and can be communicated via email to configurable groups or individuals. Tickets can be closed when an issue has been resolved to an organization's satisfaction.
DSS03.05	Perform proactive problem management	Operational data from Nessus, PVS, and LCE is gathered by SC to discover problem trends that are in need of proactive remediation efforts. SC reports and dashboards can display this information visually for easier understanding over various organizational departments and levels.
DSS04	**Manage Continuity**	
DSS04.01	Define the business continuity policy, objectives and scope	For any fail-over or disaster recovery computing resources, SC can be used to manage the security of these devices prior to an event requiring them. If the devices are in cold stand-by, SC can be configured to monitor them as soon as they go live.

DSS04.02	Maintain a continuity strategy	For any fail-over or disaster recovery computing resources, SC can be used to manage the security of these devices prior to an event requiring them. If the devices are in cold stand-by, SC can be configured to monitor them as soon as they go live.
DSS04.04	Exercise, test and review the BCP	The PVS and LCE can be used to identify the most active network resources. The LCE can be used to monitor connections to both the primary and backup IT systems. During a fail-over, the LCE can show through various logs collected that new systems are in use.
DSS04.06	Conduct continuity plan training	Information gathered by SC from Nessus, PVS, and LCE can be used in continuity training exercises to assist with the diagnosis of network and system problems, and the remediation of problems that may occur after a fail-over.
DSS04.08	Conduct post-resumption review	All of Tenable's solutions can be used to identify where data is being stored as a list of one or more asset groups. Vulnerabilities, compliance issues and security events against storage systems can be then specifically escalated, reported on and analyzed.
DSS05	**Manage Security Services**	
DSS05.01	Protect against malware	SC, Nessus, and the PVS can be used to ensure that systems have been locked down to be resistant from attack, are indeed running an updated anti-virus program and also perform testing for the presence of known viruses and backdoors. The LCE can be used to independently look for network behavior indicative of a worm, virus or spyware and can also aggregate and normalize logs from various anti-virus manufacturers.
DSS05.02	Manage network and connectivity security	The LCE can accept logs from a variety of network access control technologies such as firewalls, intrusion detection systems, intrusion prevention systems and secure switches. In addition, SC can make use of data from the PVS or distributed Nessus scanners to show how various components of the network can communicate with each other. This can expose unauthorized deviations from access control policy. SC can be used to discover applications that accept data on non-secure protocols. The LCE can also be used to search for logs indicating use of insecure data transfers. This can be accomplished on a per-asset basis as well. For more in-depth auditing, Nessus can be used to scan servers and desktops for files that contain sensitive information.
DSS05.03	Manage endpoint security	SC can be used to highlight any assets containing cryptographic keys. These assets can then be used for reporting and alerting of any outstanding vulnerabilities, access attempts or odd behavior.
DSS05.04	Manage user identity and logical access	The LCE can list which users have attempted to gain access to various system. In addition, SC, and Nessus can be used to verify that servers have been locked down such that only authorized users accounts exist. Nessus can also audit these systems to make sure these accounts have least privilege. HR systems that contain user information can be managed with SC. As uniquely identified users log into and out of various assets, the audit trail from these devices can be captured by LCE. Additionally, any type of identity log can be used to correlate real users with

		system and network activity. This allows the LCE to list which users have logged into a system, which users have failed access to sensitive systems and many other useful use cases for compliance and security monitoring.
DSS05.05	Manage physical access to IT assets	SC can be used to list various types of security technologies in use. These technologies can be grouped into specific or generic asset lists and reported on accordingly. For example, a customer could group all of their “Nessus Scanners” into an asset list for easy analysis of any vulnerabilities, security events or suspicious access attempts to them. The LCE can be configured to process access control logs from physical access control devices such as card readers. The LCE can also be configured to monitor various assets for “physical” access indicators such as logging in directly at the keyboard.
DSS05.06	Manage sensitive documents and output devices	SC is able to identify printers, scanners, and other output devices with network connections. PVS is able to observe specific file types as they travel across a network and report such activity back to SC.
DSS05.07	Monitor the infrastructure for security-related events	SC, Nessus, and the PVS offers organizations many ways to perform testing for new hosts, new applications and to monitor or facilitate the mitigation of security risks. In addition, the LCE can be used to monitor in real-time for security events related to network abuse, attacks and compromises. LCE performs normalization, aggregation and correlation of all logs including audit logs, which makes it easy to recognize new attacks and anomalies.
DSS06	**Manage Business Process Controls**	
DSS06.02	Control the processing of information	Business processes and activities can be monitored by Tenable’s products to ensure the secure processing of information, including tracking unauthorized access to business assets and materials.
DSS06.03	Manage roles, responsibilities, access privileges and levels of authority	SC can accommodate a wide variety of roles. These can be used to segment creation of users, deciding what users can/can’t do, and analyzing user activity. This allows SC to fit into any type of organizational structure. The LCE can be used to analyze system logs to determine if access control policies are being followed. SC can use Nessus compliance audits to also ensure that systems are locked down to “least use” principles.
DSS06.04	Manage errors and exceptions	All of Tenable’s solutions can be used to identify where data is being stored as a list of one or more asset groups. Vulnerabilities, compliance issues and security events against storage systems can be then specifically escalated, reported on and analyzed.
DSS06.05	Ensure traceability of information events and accountabilities	For the processing of sensitive messages, the LCE can be used to capture and analyze any audit trail of the systems generating and receiving the messages. For more in-depth auditing, Nessus can be used to scan servers and desktops for files that contain sensitive information.
DSS06.06	Secure information assets	SC can monitor the storage and transfer of information assets across the network, including transfer through the use of portable media devices, user applications, and storage devices.

MEA	Monitor, Evaluate and Assess	
MEA01	**Monitor, Evaluate and Assess Performance and Conformance**	
MEA01.01	Establish a monitoring approach	All of Tenable's products can be used to provide metrics on how well an IT organization is performing. Common security metrics, such as the number of security events, can easily be generated, but also derivative information, such as average time to remediate a security issue, may also be applicable.
MEA01.02	Set performance and conformance targets	For collection of risk and compliance data, SC can be used to trend configuration deviations from corporate policy as well as non-compliant security events.
MEA01.03	Select and process performance and conformance data	All of Tenable's products can be used to tell where IT has performed well. For example, being able to report that all changes were performed within change control windows can demonstrate how IT is following corporate guidelines.
MEA01.04	Analyze and report performance	SC can generate reports for a wide variety of IT-related performance events, such as problem remediation, availability statistics, and compliance with established corporate guidelines and standards.
MEA02	**Monitor, Evaluate and Assess the System of Internal Control**	
MEA02.01	Monitor internal controls	Data gathered through compliance audits and log analysis can be presented to managers for review.
MEA02.02	Review business process controls effectiveness	SC and LCE can be used to monitor changes to the IT network. These changes can be mapped to specific IT controls to see if they have been approved or if they are unauthorized.
MEA02.03	Perform control self-assessments	Periodic assessments of the IT environment can be performed through active scanning through Nessus and log review through LCE in order to measure the effectiveness of an organization's controls and policies.
MEA02.04	Identify and report control deficiencies	Assessment data can be gathered and reported by SC in a variety of formats to communicate identified control problems to the appropriate organizational groups, departments, or individuals.
MEA02.08	Execute assurance initiatives	Performance, compliance, and risk data gathered and reported by SC can be measured and communicated to assist in quality delivery and assurance initiatives.
MEA03	**Monitor, Evaluate and Assess Compliance with External Requirements**	
MEA03.01	Identify external compliance requirements	As corporations make decisions about which laws and regulations are applicable to IT, these will have overlapping requirements for how IT should manage their infrastructure and who can use it. Tenable's solutions enable independent internal monitoring of networks in accordance with corporate IT governance directives.
MEA03.02	Optimize response to external requirements	All of Tenable's products can be configured to help aggregate information relevant to a variety of compliance requirements.
MEA03.03	Confirm external compliance	All of Tenable's products can be configured to help aggregate information relevant to a variety of compliance requirements, including configuration management as well as sensitive data leakage.

MEA03.04	Obtain assurance of external compliance	SC can be used to generate positive compliance reports about configuration, changes and security events relevant to an organization’s regulatory responsibilities. This can be done in a near real-time basis so that small compliance issues can be discovered as they happen.

Appendix F: Tenable Solutions for NERC CIP Audits

Note: Many of the NERC CIPs pertain to policy and physical procedures.

The following acronyms will be used:

IDS – Intrusion Detection System
SC – SecurityCenter
LCE – Log Correlation Engine
PVS – Passive Vulnerability Scanner

Process	Name	How Tenable Can Help
CIP-002	**Identification of Critical Cyber Assets**	
R1	Critical Asset Identification Method	For systems that support the reliable operation of power generation and delivery, a risk assessment must be performed that analyzes the impact of each device not being available.
R2	Critical Asset Identification	Once the criteria for discovering “critical” devices has been determined, the actual assessment must be performed.
R3	Critical Cyber Asset Identification	As part of the effort to identify critical systems, Tenable’s products can be used to discover which devices are being controlled or monitored over IP networks. Active vulnerability scans can help identify all the devices on a network, but may have an availability impact on the cyber assets. Passive analysis with the PVS can ensure that all protocols, including many SCADA protocols, and all operational modes for a network are considered without any adverse impact. Tenable’s products can also identify network parties that connect to a Critical Cyber Asset over a routable IP protocol. The distinction is subtle, but this will ensure that unneeded auditing and documentation of non-critical cyber assets is avoided.
R4	Annual Approval	With a Tenable solution, organizations can gather information about a wide variety of systems. This data can be used to support a decision to add or remove an asset from the Critical Cyber Asset list. This information must be submitted to a senior manager. Having the right information can help the manager make the right decision.
CIP-003	**Security Management Controls**	
R1	Cyber Security Policy	A policy must be in place to cover CIP-002 through CIP-009. Although Tenable’s products do not specifically help draft these policies, they do provide copious evidence of the types of systems, their common weaknesses and types of attacks they suffer. Tenable’s products also assist in determining where Critical Cyber Assets are being accessed on the network. This information can help determine an access control policy. A critical aspect of the policy is that it must be able to be audited. Tenable’s products are uniquely positioned to show both policy failures and policy compliance events in both system configurations and overall activities.

R2	Leadership	Technically, all that CIP-003 requires is that a senior manager be made in charge of security responsibilities. This requirement is looking for a name and address. However, with Tenable products, a wide variety of information can be presented to the senior manager in such a way that they are better informed about their network. Tenable's products such as SC allow for a senior manager to track overall risk, threat events and compliance events that are unique to their environment.
R3	Exceptions	NERC realizes that any large network may have a reasonable need for policy exceptions. Often a cyber security policy may contain a set of requirements that become unreasonable for a specific asset. The requirement of security does not go away in these cases and must be countered with a separate compensating control. For compensating controls such as limiting access to specific users, controlling access between networks with a firewall or implementing an IDS/IPS, Tenable's products can be used to monitor the control and augment it to detect and log normal access as well violations and violation attempts. For example, not only can SC and the LCE collect firewall logs to detect who is connecting to where, but they can also alert if the firewall configuration is modified or provide a second independent layer of network monitoring.
R4	Data Protection	This requirement identifies levels of data importance and what needs to be done to protect each level. Once the protection levels have been developed, aspects of the levels can be fed into SC for auditing. Consider the following examples: • If key servers or desktops are supposed to be locked down, have certain encryption software installed and have stricter access control and logging policies, SC and Nessus' local host auditing abilities can be used to monitor for compliance. • If key systems with sensitive data are known, they can be easily watched for intrusions, access attempts and changes to their configuration. Both SC and the LCE can help monitor these systems. • SC can create on-the-fly asset groups that include these systems with sensitive data. This assists in reporting, log analysis and visualization of the security data about these systems. In addition, comparisons between different asset groups that contain sensitive data can also be made.
R5	Access Control	This requirement specifies granting access to specific types of information, not specifically access to critical cyber assets. Tenable can help monitor access control in several areas: • All user access modification, account creation and account deletion can be analyzed and reported on with the LCE. • Configuration policies for servers can be developed for auditing that ensure principals of least use. This ensures that a generic account cannot see data for other accounts or effect user privileges. SC and Nessus can be used to test for these configurations.
R6	Change Control and Configuration Management	A key feature of Tenable's product offering is to detect change. This is accomplished several ways: • Successive network vulnerability scans conducted by Nessus and SC

		always produce “change” lists of new hosts, applications and vulnerabilities. • The PVS will detect new hosts in real-time. • The LCE can analyze logs and generically alert when new hosts appear, changes to user accounts occur, changes to running configurations of network devices occur and software is added or removed to servers. The Tenable change detection capabilities can serve as a useful test of the change control policy implementation. For configuration management, Nessus and SC can be used to audit Windows, Linux, and Unix servers for best practices. Tenable has developed templates for securing and locking down servers based on public guidance from NSA, NIST and CIS that can be used to audit existing systems. Custom policies can also be developed that reflect local cyber security configuration requirements.
CIP-004	**Personnel and Training**	
R1	Awareness	For any public awareness program, data from Tenable’s products can be used to provide real numbers about raw vulnerabilities, attacks and policy violations. Threat data on a bulk electric entity’s system can be a powerful security awareness tool. Tenable’s products also produce stunning three-dimensional views of complex data.
R2	Training	All personnel who have access to cyber security assets need to undergo annual training. Training is required to include proper use of the Critical Cyber Assets, a discussion of the access controls, how critical cyber security information should be handled and how to recover a cyber security asset from a cyber security incident. For the Tenable products that monitor a Critical Cyber Asset, training should be augmented to encompass the features and capabilities that those products bring. For example, while discussing access controls, it could be discussed that the base configuration of a system, including its password policy, logging policy and permissions, are all audited by Nessus and SC on some sort of ongoing basis. Similarly, understanding that all access events are logged by proxies or firewalls and analyzed by the LCE is also relevant.
R3	Personnel Risk Assessment	Tenable’s products do not help identify any background risk in personnel working on Critical Cyber Assets, but our products can help identify malicious insiders, or identify what a particular individual has been doing. For example, Nessus can be used to audit servers to see that only authorized accounts exist. The LCE can also produce lists of which accounts have had access to certain sensitive systems.
R4	Access	Tenable’s products can help identify when a certain user is attempting to circumvent their given authority. For example, the LCE can look for login failures or access attempts in both COTS and custom applications. The LCE can also audit and report on all types of access so that trends and anomalies can be analyzed.

CIP-005	Electronic Security Perimeter(s)	
R1	Electronic Security Perimeter	An Electronic Security Perimeter (ESP) is the boundary around all Critical Cyber Assets. Typically, this is a list of all communications access point such as a modem, firewall or router. Tenable can help in the following areas that are necessary for complying with this requirement: • All Critical Cyber Assets “inside” an ESP as defined by specific access points such as firewalls, routers and modems need to be documented. All of Tenable’s products can aid in discovering and reporting about what is connected to which side of a network. • All non-critical cyber assets “inside” an ESP also need to be documented and protected. With the use of SC’s dynamic asset groups, this information can readily be analyzed for documentation support. • All cyber assets deployed to enforce or monitor asset control such as firewalls, routers and authentication servers can be discovered, reported and documented. In addition, if Tenable’s LCE is the device being used to collect these sorts of logs, then it also becomes part of the list.
R2	Electronic Access Controls	This requirement focuses on access to a Critical Cyber Asset from outside an Electronic Security Perimeter. Tenable’s products can help in several ways: • Access must be denied by default. This can be audited through the use of Nessus’ compliance checks. Servers that must be configured to offer “least privilege” by default can be routinely audited and tested in an automated fashion. • Access control points, such as firewalls and authentication servers, will generate logs that can show access granted and denied. These events can be collected by the LCE for reporting and analysis. • For periodic reporting on this sort of access control, Tenable’s products can help produce quarterly reviews of access control policies, changes in access control or user account privileges and generating lists of terminated user accounts. • Only specific ports and services are to be authorized for use through an ESP. This can be monitored through log analysis by the LCE, audited with active scanning by Nessus and monitored for on a continued basis with the PVS. • Testing that systems display an appropriate banner can also be conducted through Nessus auditing.
R3	Monitoring Electronic Access	All failed and successful external attacks must be reviewed every 90 days. Tenable’s products can help reach this requirement with a variety of real-time, trending and “instant” types of alerts. Tenable’s LCE can be used to identify a wide variety of “low and slow” attacks, denial of service attacks and successful attacks that indicate compromise or the intent to compromise. The LCE can alert specific users for specific servers when events occur that warrant notification. The LCE can also facilitate both basic log review for access control events as well as real-time notification of specific events. Neither is required by this CIP, but must be documented and be part of local procedures.
R4	Cyber Vulnerability Assessment	An annual vulnerability audit of the ESP is required. Tenable’s products are ideally suited to perform these tasks:

		• All ports that are supposed to be open can be audited with a Nessus scan. For large networks, these can be controlled and analyzed with SC. If scanning is not an option due to a potential system availability impact, the PVS can be used to discover which ports are in use. • Nessus, the PVS, and SC can be used throughout the year to perform these audits in advance of the required annual audit. This can ensure a "good test" and can help identify any deviations prior to the annual test. • To identify all access points, Tenable's products can help discover and enumerate all routers, firewalls and wireless access points. Although Tenable's products do not perform war-dialing over phone lines or radio spectrum monitoring to detect wireless access points, if these devices have IP connectivity, they can be discovered with Nessus or through network monitoring with the PVS. • For the access points themselves, a vulnerability audit is required. This can include a configuration review of system settings, an audit of missing patches and password policy testing. For any vulnerabilities found during the audit, a plan to mitigate or correct them is also required. Tenable's SC can help make recommendations to mitigate these vulnerabilities and track when they are no longer an issue.
R5	Documentation Review and Maintenance	The data collected by Tenable's products can help keep the documentation involving ESP up to date and correct. In particular, supporting documentation of the ESP must be reviewed annually and any known or detected changes to the ESP must be documented in 90 days. When using Nessus, the PVS, and SC, these sorts of changes can easily be detected and used to support documentation changes about the ESP.
CIP-006	**Physical Security of Critical Cyber Assets**	
R1	Physical Security Plan	A plan for securing physical access to the ESP and access control points must exist. Using Tenable's products to help identify all assets located within an ESP and their access control points can help ensure the proper physical security plan exists. For Critical Cyber Assets that do not use a routable protocol for control, a physical security plan is not needed. Although counter intuitive, Tenable's products can help ensure that networks without IP address do not exist. For organizations that use IP networks to implement cameras, physical sensors or other types of alarm and monitoring systems, Tenable's products can be used to "watch the watchers" and monitor that network for specific attacks and security issues.
R2	Physical Access Controls	Tenable's products do not specifically help deploy physical access controls, but they can help identify systems that need to be physically secured.
R3	Monitoring Physical Access	All logs for physical access need to be reviewed every 90 days for successful access and denied events. The LCE can be used to accept logs from a variety of physical access control devices such as card, badge or palm readers. Although not required by NERC, the LCE can also perform very customizable correlation such as observing a successful physical access event and then observing some sort of suspicious electronic event.

R4	Logging Physical Access	NERC allows a variety of means of logging physical events. For low-tech methods, such as a log book, there is not much to analyze with Tenable products. However, with electronic access control systems, the logs from those devices can be sent to the LCE.
R5	Access Log Retention	All access control logs must be retained for 90 days. For electronic physical access events, storing the events for 90 days is easily accomplished by the LCE.
R6	Maintenance And Testing	If a LCE is used to obtain logs from a live electronic log system, then the actual logs can be used as evidence that the systems are indeed working. There is a requirement to test these systems once every three years. All outages or lapses in access control enforcement also need to be documented. If a LCE is in use, it can be configured to parse the logs for electronic physical access devices and recognize events such as power-on, restart and non-enforcement modes.
CIP-007	**Systems Security Management**	
R1	Test Procedures	Because patching and security management measures can cause unwanted outages and impacted system availability, NERC requires that any significant changes to Critical Cyber Assets inside an Electronic Security Perimeter be tested. Some patches and upgrades cause security functionality to be removed or overwritten. All of Tenable's products can help detect this sort of change. Tenable's products can also help determine if the change has introduced new vulnerabilities.
R2	Ports and Services	For each Critical Cyber Asset, a list of authorized active open ports and applications should be maintained with the principal of "least use". Tenable's Nessus and PVS can be used to baseline the current network and assist in documentation of what is currently in use or what should be disabled. After this initial assessment, active and passive scanning can be used to monitor if new ports or applications have become available. This information can be used to change policy if these new ports are indeed required, or to report a policy compliance issue.
R3	Security Patch Management	According to NERC, all available patches must be analyzed within 30 days of their availability. It does not say exactly when a patch is to be deployed, just that its applicability be determined. Tenable's PVS, Nessus, and SC are ideal methods to determine missing patches across all operating systems and network hardware. With more than 54,000 active and over 6,000 passive vulnerability checks, Tenable's technology is very comprehensive. This can avoid the issues of subscribing to multiple vendor mailing lists, or hearing about the "latest" security issue but not really being affected by it.
R4	Malicious Software Prevention	Although Tenable does not offer an anti-virus product, we do ensure that common anti-virus applications are up to date. Many technical reasons such as bad network routes, incorrect DNS entries and even low disk space can prevent virus signature updates from occurring. Tenable's Nessus scanner can determine when a host is not running anti-virus software or when the device is out of date with its signatures.

		In addition to testing the viability of anti-virus software, Tenable's Nessus scanner can also test the base configuration of each operating system.
R5	Account Management	In addition to the requirements of CIP-003 R5 and CIP-004 R4, Tenable's products can also help meet the requirements of CIP-007 R5. These include: • *Generating Audit Trails* – The configuration audits of Nessus can be used to ensure that audit trails of logins, failed logins and logouts are enabled. The LCE can also be used to collect those log events and analyze them for attacks, trends and to also build reports. • *Securing Shared Accounts on Critical Cyber Assets* – The Nessus scanner can be used to test for known default accounts that exist in the Critical Cyber Assets. • *Enforcement of Password Complexity* – For technologies such as Windows, Linux, and Unix, the Nessus scanner can be used to test for a robust password policy. This can include password length, complexity and frequency of change.
R6	Security Status Monitoring	In general, Tenable's products can help monitor all Cyber Assets in the following manner: • The Nessus scanner can ensure that each system has logging enabled. • The LCE can be configured to retain all logs for 90 days. • Through the use of SC and LCE, multiple users can analyze these logs every 90 days for their specific asset groups. This ensures that system owners perform the necessary analysis. • The LCE can also perform a wide variety of attack detection, attack verification and general detection of "suspicious" events. These alerts can be sent by the SC to the specific business units or to system owners.
R7	Disposal or Redeployment	Tenable products do not assist with removal or destruction of actual data or hardware.
R8	Cyber Vulnerability Assessment	An annual vulnerability assessment of all Cyber Assets is to be performed. The following key points required by NERC are covered by Tenable products: • Determining that all unneeded ports and applications have been disabled can be determined by Nessus' active scans as well as continuous network monitoring by the PVS. • Testing for default accounts and their default passwords can be accomplished by Nessus. • Testing for the latest patches or password complexity is not required by NERC for this requirement, but can easily be accomplished by Nessus. • If any vulnerabilities are found, the SC can be used to help plan recommendations and track when vulnerabilities are patched. Prior to the annual review, if SC, Nessus and the PVS are in use, early detection of issues that would fail the annual test can be detected.
R9	Documentation and Review Maintenance	An annual review of all documentation pertaining to this CIP is required. In addition, any changes to the systems affected by this CIP must be documented within 90 days.

		Tenable's products can assist in providing the underlying evidence and content for changes.
CIP-008	**Incident Reporting and Response Planning**	
R1	Cyber Security Incident Response Plan	Each organization is responsible for developing its own incident response plan. NERC is very specific about what is to be reported. This includes: • Loss of generation by a utility or generator supply entity. Loss of ≥ 500 MW generation in the host region for 30 minutes or longer due to malicious or unknown causes. • Loss or degraded ability to control operations over a portion of the power grid. Any loss or degradation of essential control functions from malicious or unknown causes lasting 30 minutes or longer at several transmission substations, or repeated losses at a single transmission substation, associated with a portion of the grid serving 100,000 customers or more. Attacks can come from many vectors including internal and external. NERC does not require that outages due to internal negligence, such as a patch incompatibility issue, be reported. They only require that malicious events be reported. Obviously, Tenable's entire product line can be used to help deter attacks, minimize their attack surface and also assist in detecting the attack and accessing the scope of the attack. Accurately knowing where an attacker has been able to achieve illegal access can help determine the correct incident response plan. Being able to combine the vulnerability and security events into one product, such as SC, and then allowing it to be shared securely across many different organizations, can help minimize misinterpretation of logs and maintain consistent situational awareness during an incident.
R2	Cyber Security Incident Documentation	All information about an incident needs to be maintained for three years. If the LCE is in use, all logs leading up to the event can be collected. This data will be as good as the sources of logs being used. This could include system logs, network traces, intrusion detection events, access control logs, etc. In addition to the logs themselves, if SC is in use, vulnerability and configuration data can be collected about the targets involved.
CIP-009	**Recovery Plans for Critical Cyber Assets**	
R1	Recovery plans	Tenable's products can help maintain more accurate recovery plans for Critical Cyber Assets. For example, the PVS can be used to discover which nodes communicate to the Critical Cyber Assets. This can help build realistic redundancy and recovery plans. These plans must be reviewed annually. Tenable's products can also be used to keep these plans up to date with any known changes.
R2	Exercises	Each recovery plan must be tested annually. Plans can be loosely grouped by specific profiles of unique Critical Cyber Assets, and these assets can be determined effectively by Tenable products. For example, the PVS can be used to identify all nodes that speak specific SCADA protocols.
R3	Change Control	Any changes to the recovery plans must be documented within 90 days of their discovery. Tenable products can help support the addition of new Critical Cyber Assets, changes to the profiles of these devices and changes

		in access control that implies changes to the actual recovery plans themselves.
R4	Backup and Restore	NERC is not very specific when it comes to implementing backup and restore procedures. All Tenable products can be used to access the security and availability of backup technologies such as SANs and NASs. Increasingly, Tenable has been adding capabilities to the Nessus and PVS products to detect backup protocols, as well as vulnerabilities in specific backup applications such as Veritas.
R5	Testing Backup Media	Tenable products do not test for the accuracy or integrity of data on physical backup devices.

Appendix G: Tenable Solutions for Nuclear Facility Cyber Security

Note: Many of the sections of RG 5.71 pertain to technical, operational, and management security controls. This appendix addresses the "Generic Cyber Security Plan Template" in Appendix A and "Technical Security Controls" in Appendix B of RG 5.71.

The following acronyms will be used:

IDS – Intrusion Detection System
SC – SecurityCenter
LCE – Log Correlation Engine
PVS – Passive Vulnerability Scanner

Section	Name	How Tenable Can Help
A.3.1.3	Identification of Critical Digital Assets	Nessus and PVS can be used to actively and passively identify plant systems, equipment, communication systems, and networks. SC can place CDAs into asset groups specified by location, function, or criticality depending on the operational layout of the facility.
A.3.1.4	Reviews and Validation Testing	Communication pathways can be identified by the PVS and LCE, and the information gathered can be stored in SC to review network activity and configurations. 3D Tool also helps give a visual overview of a network's layout based on data maintained by SC, enabling the ability to identify network segments and devices, and perform physical testing of communication pathways.
A.3.1.5	Defense-in-Depth Protective Strategies	SC allows security managers and authorized personnel to monitor systems and devices throughout the environment, from externally-facing systems down to the desktop level. Layers of protection, such as firewalls and anti-virus, can be analyzed to ensure that all protective measures are in place and operational.
A.3.1.6	Application of Security Controls	SC allows for the review and analysis of defense models, technical controls, and attack vectors. Active and passive vulnerability scanning through Nessus and PVS, as well as log analysis through LCE, provide critical information about the effectiveness of technical and operational security controls.
A.4.1	Continuous Monitoring and Assessment	Tenable's products are designed to focus on the real-time monitoring and assessment of systems and networks. PVS and LCE provide near real-time updates found through network activity and system logs, and Nessus can be scheduled to perform active scans after plugin updates or change control windows. SC ties all of this information together to provide a continually updated assessment of an organization's security and compliance posture while continuing to monitor for new changes and vulnerabilities.
A.4.1.1	Periodic Assessment of Security Controls	Data gathered by SC can be used to assess the security controls outlined in RG 5.71. Reports related to specific controls, such as vulnerability assessment or configuration management, can be scheduled to run at a given time or generated on demand.
A.4.1.2	Effectiveness Analysis	Tenable products are able to help improve the performance of a Cyber Security Program through risk evaluation, threat detection, and workflow management that can be used to close gaps discovered in the program. Reporting and workflow tools keep personnel informed and involved with the overall security of the network and effectiveness of the controls used in the program.
A.4.1.3	Vulnerability Assessments and	Tenable's Nessus vulnerability scanner is the world-leader in active scanners, featuring high-speed discovery, asset profiling, and vulnerability analysis of the

	Scans	organization's security posture. Nessus scanners can be distributed throughout an entire enterprise, inside DMZs, and across physically separate networks. Exploitable vulnerabilities are identified through Nessus plugins, and safe checks can be enabled to reduce the risk of affecting the availability of scanned systems and devices.
A.4.2	Change Control	SC, LCE, Nessus, and PVS can be used to discover changes in the network that should not have occurred or are against policy. Discovery of new hosts and new applications is easily accomplished with these tools. Workflow and ticketing options assist with tracking the change control process from planning to completion.
A.4.2.1	Configuration Management	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.
A.4.2.2	Security Impact Analysis of Changes and Environment	Through SC, connectivity pathways and system interdependencies can be identified when performing a change impact analysis. Using Nessus, remediation scans can be performed after all change control windows, which can be used to ensure no new vulnerabilities have been introduced and report on the organization's updated security posture.
A.4.2.4	Updating Cyber Security Practices	The current status of network devices and systems, for both security posture and availability, can be reported by SC to assist with modifying security policies, procedures, and practices. 3D Tool is available to assist with providing updated network diagrams, which is useful when determining any possible changes to current policies or the security program as a whole.
B.1.1	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 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 (e.g., 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.
B.1.2	Account Management	Tenable solutions can test for the presence of accounts that should or should not be present on a system. The presence of the account through network and/or log analysis can also be detected.
B.1.3	Access Enforcement	Tenable scanning solutions enable testing of servers 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.

B.1.4	Information Flow Enforcement	Using PVS and Nessus, sensitive data in motion and at rest can be detected in near real-time and identify breaches of information flow control policy. The LCE can also be configured with a list of all valid user accounts that access a particular asset group. When logins occur (failed or successful) the LCE can alert if the user in question is not on the authorized list.
B.1.5	Separation of Functions	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 to ensure 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 some audit users cannot see events, some can only see normalized events and others can do unlimited log search. User access to LCE raw log data is configurable on a "per-LCE" basis.
B.1.6	Least Privilege	Nessus' compliance checks can be used to audit user accounts, specific lists of users, and how authentication occurs and is logged. The LCE will normalize all logs based on the user ID of the authenticated user. This allows quick and easy and accurate inspection of all logs in order to see which users have accessed systems with sensitive data.
B.1.7	Unsuccessful Login 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.
B.1.8	System Use Notification	Tenable has solutions to audit network devices to ensure a default warning banner message is displayed before users can login.
B.1.9	Previous Logon Notification	Tenable has solutions to audit network devices to ensure a previous login notification setting is enabled.
B.1.16	"Open/Insecure" Protocol Restrictions	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, then it can correlate network traffic with logins to see that only encrypted protocols are being used.
B.1.17	Wireless Access Restrictions	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.
B.1.18	Insecure and Rogue Connections	All cyber assets such as firewalls, routers, and modems need to be documented. All of Tenable's products can aid in discovering and reporting insecure or rogue connections from inside or outside of a network.
B.1.19	Access Control for Portable and Mobile Devices	Tenable's solutions include the ability to discover when new hosts are added to the network including new laptops, PDAs, or cell phones. 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.
B.2.2	Auditable 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.
B.2.3	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.
B.2.4	Audit Storage Capacity	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.
B.2.5	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.
B.2.6	Audit Review, Analysis, and Reporting	Tenable's LCE provides the ability to normalize billions of log events, store, compress, and search for 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.
B.2.7	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, compromise, and port scans. Any report can be exported via 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.
B.2.8	Time Stamps	All events arriving at the LCE are uniquely time-stamped.
B.2.9	Protection of Audit Information	SC users can only see vulnerabilities, IDS events and logs for a specific range of IP addresses that they have been assigned to. Users may be further restricted to only view scan and IDS data that they are authorized to see by the Manager for their customer account. User access to LCE raw log data is configurable on a "per-LCE" basis.
B.2.10	Nonrepudiation	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.
B.2.11	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.

About Tenable Network Security

Tenable Network Security is relied upon by more than 20,000 organizations, including the entire U.S. Department of Defense and many of the world's largest companies and governments, to stay ahead of emerging vulnerabilities, threats and compliance-related risks. Its Nessus and SecurityCenter solutions continue to set the standard to identify vulnerabilities, prevent attacks and comply with a multitude of regulatory requirements. For more information, please visit www.tenable.com.

GLOBAL HEADQUARTERS

Tenable Network Security
7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046
410.872.0555
www.tenable.com