tenable®
network security

Continuous Compliance for Energy and Nuclear Facility Cyber Security Regulations

Leveraging Configuration and Vulnerability Analysis for Critical Assets and Infrastructure

May 2015

(Revision 2)

Table of Contents

Introduction

Tenable Network Security serves customers worldwide, and each of Tenable's customers has a unique set of audit and compliance requirements. This paper provides insights on measuring and reporting compliance in the energy and nuclear facility sectors.

Specifically, this paper describes how Tenable's solutions can be leveraged to eliminate vulnerabilities, reduce risk, and ensure compliance for critical assets and infrastructure in the energy and nuclear facility sectors by ensuring that key assets are properly configured, monitored, and assessed. It is crucial to continuously monitor for compliance 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.

This paper addresses the needs of security managers in the energy and nuclear facility sectors who are new to assessments as well as those who are experienced in the assessment 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
North American Electric Reliability Council (NERC) Standards	http://www.nerc.com/pa/stand/Pages/default.aspx
United States Nuclear Regulatory Commission (NRC) Regulatory Guide 5.71	http://nrc-stp.ornl.gov/slo/regguide571.pdf

Tenable's Solutions

Core Solution Description

Tenable offers a variety of solutions and methods to detect vulnerabilities, misconfigurations, malware, real-time threats, and security events. Tenable's core technology is also extremely powerful for conducting network compliance audits and communicating the results to practitioners, managers, and executives.

SecurityCenter Continuous View – Tenable's SecurityCenter Continuous View™ (SecurityCenter CV™) is the only continuous network monitoring™ solution, which provides the most comprehensive and integrated view of enterprise health.

- Broadest coverage of networks, devices, systems, virtual, mobile, and cloud services
- In-depth detection of vulnerabilities, misconfigurations, malware, and real-time threats
- Advanced analytics with actionable information and trending to prioritize events/alerts
- Highly customizable dashboards, reports, and workflows for rapid response
- Continuous assurance using Assurance Report Cards (ARCs) that communicate the effectiveness of security investments

SecurityCenter Continuous View is comprised of the following components:

Nessus – Tenable's Nessus® is the world's most widely-deployed vulnerability, configuration, and compliance assessment product. Nessus prevents network attacks by reducing your attack surface – identifying the vulnerabilities and configuration issues that hackers could use to penetrate your network, whether your network is on-premises, in the cloud, or hybrid.

Passive Vulnerability Scanner – Tenable's Passive Vulnerability Scanner™ (PVS™) continuously monitors network traffic to identify risks and vulnerabilities as they occur in real time. PVS helps you:

- Eliminate blind spots by identifying and analyzing transient mobile, virtual, and cloud assets
- Identify unpatched and compromised applications

- Detect unauthorized and malicious network activity
- Identify vulnerabilities 24/7 to accelerate remediation

Log Correlation Engine – Tenable's Log Correlation Engine ™ (LCE™) collects and aggregates data from firewalls, intrusion detection and prevention systems, and data loss prevention solutions, as well as raw network traffic, application logs, and user activity. LCE helps you:

- Normalize, correlate, and analyze event data from a single console
- Store, compress, and perform full-text search for rapid attack analysis
- Detect the presence of malware running in your environment
- Demonstrate compliance with internal and external mandates efficiently
- Continually assess your security and compliance posture through flexible reporting and consistent metrics

The key features of Tenable's products as they relate to compliance are referred to as "Tenable's Critical Cyber Controls for Secure Systems". They are:

Track Your Authorized Inventory of Hardware and Software

SecurityCenter Continuous View can organize network assets into categories through a combination of active network scanning, passive network monitoring, and integration with existing asset and network management data tools. SecurityCenter CV can discover when there has been a change to the assets it is monitoring, such as the addition of a new server or device. Unauthorized and unmanaged hardware assets can be easily identified, and vulnerability assessments can be performed on all assets to determine and assess risk.

Credentialed scans allow SecurityCenter CV 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 CV 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.

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 or mobile phones.

In addition, SecurityCenter CV's LCE component 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 CV can also help inventory and manage the security vulnerabilities and configurations of the systems controlling the physical devices.

Continuously Remove Vulnerabilities and Misconfigurations

To remove all vulnerabilities, you must implement a regular continuous network monitoring program. Procedures should include three areas:

- Applying software, hardware, and cloud service patches to remove vulnerabilities
- Applying configuration changes to limit malicious exploits
- Applying additional host or network-based security monitoring

Tenable recommends that you organize your technologies by business function and asset. Each asset should be assessed and patched on an agreed upon schedule with a repeatable process.

In addition to active scanning through Nessus, PVS delivers continuous network monitoring and profiling for an ongoing 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 and continuously determine host file-level information, which has tremendous forensics and situational awareness value. For large networks, the ability to passively determine all shared folder contents can facilitate identification of potentially sensitive data. PVS can send a record of each file that was shared over the network to the LCE, which enables forensic analysis of employee and malware activity.

A configuration audit is one where the auditors verify that servers and devices are configured according to an established standard or baseline 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 into Unix, Linux, or Windows servers without the use of an installed agent.

Thousands of organizations use Nessus and SecurityCenter to audit their networks. Using Tenable's solutions, you can ensure that IT assets including operating systems, applications, databases, and network devices are compliant with policies and standards. Tenable provides more than 500 audit policies for a wide range of assets and standards, including:

- Operating systems
- Databases
- Applications
- Network infrastructure
- Virtual infrastructure
- Sensitive content
- Anti-virus

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 has been configured in SecurityCenter, it 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.

Deploy a Secure Network

Network security should be a daily practice. For each asset, one or several mitigating technologies can be deployed to prevent or detect malicious activity. For example, host-based technologies include anti-virus, application white-listing, and system monitoring; network-based technologies include activity monitoring, intrusion prevention, and access control; auditing cloud-based technologies can be done with APIs, threat subscriptions, and network monitoring or endpoint system monitoring.

To assist with the deployment of a secure network, SecurityCenter Continuous View can perform the following forms of security event assessments and 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 identify successful attacks, reconnaissance activity, and theft of information

To support continuous network monitoring, Tenable ships SecurityCenter CV with logic that can map any number of normalized events to a "compliance" event. For example, a simple login failure may be benign, but when it occurs on a critical asset, it must be logged at a higher priority. SecurityCenter CV allows any organization to continuously implement their compliance monitoring policy. These events are also available for reporting and historical records that must be maintained in accordance with retention policies.

Give Users Access to Only What They Need

All users should have a demonstrated business need to access specific systems and data. Limit and control administrative privileges, avoid using default accounts, enforce strong password creation, and log all accesses. Tenable recommends that you implement multiple technologies to determine active user accounts, such as authentication logging and network protocol analysis.

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 solutions can also detect changes to network access control policies through the use of repeated network scans, passive network monitoring, and log analysis.

SecurityCenter CV's LCE component provides full log aggregation, storage, and search capabilities. 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. SecurityCenter CV unifies access data and provides a large number of filters to analyze user activity, and 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.

Search for Malware and Intruders

You must actively monitor your systems for anomaly detection and exploitation. It is frankly unrealistic to expect your systems to be 100% incident free. Attackers acquire new technologies every day; you have to stay one step ahead of them by proactively managing your systems with near real-time continuous scanning for viruses, malware, exploits, and inside threats. Each of the previous four controls make your search for malicious activity easier and create several audit trails to be used in a forensic analysis.

Nessus identifies malicious software and botnets 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 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 more than 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 yet another level of protection for an organization.

SecurityCenter Continuous View offers 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. SecurityCenter CV also works with logs from many anti-virus vendors, which makes it much easier to investigate how an outbreak or infection occurred.

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 through CIP-011 (CIP-014, Physical Security, is out of scope for this paper). Each CIP has the following focus areas, many of which relate to Bulk Electric System (BES) Cyber Systems:

- CIP-002 – BES Cyber System Categorization
- CIP-003 – Security Management Controls
- CIP-004 – Personnel and Training
- CIP-005 – Electronic Security Perimeter(s)
- CIP-006 – Physical Security of BES Cyber Systems
- CIP-007 – System Security Management
- CIP-008 – Incident Reporting and Response Planning
- CIP-009 – Recovery Plans for BES Cyber Systems
- CIP-010 – Configuration Change Management and Vulnerability Assessments
- CIP-011 – Information Protection

In November 2013, the Federal Energy Regulatory Commission (FERC) approved Version 5 of the NERC CIP standards, which provides a significant change from Version 3 of the CIP and completely bypasses the implementation of the proposed Version 4 of the CIP. A Transition Program will be used during the implementation of Version 5, which will be fully enforced beginning on April 1, 2016. Additional information about the Transition Program can be found on the official NERC website at http://www.nerc.com/pa/CI/Pages/Transition-Program-FAQs.aspx.

The last two CIP standards listed above are new to Version 5: CIP-010 (Configuration Change Management and Vulnerability Assessments) and CIP-011 (Information Protection) are included in the latest revision. The new standards consolidate requirements that were previously included in other CIP standards, including CIP-003, CIP-005, and CIP-007. Each new standard also specifies that a “Responsible Entity” is required to document processes involved with the implantation of each of the standards’ requirements.

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 the typical enterprise network faced.

This has generally changed now that many control systems have implemented Ethernet and TCP/IP networks and are using operating systems, databases, and web servers commonly found in a typical enterprise network. This happened 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 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 “BES Cyber Systems” and “Electronic Security Perimeters”. Tenable’s solutions can identify rogue systems within Electronic Security Perimeters, unauthorized communication with BES Cyber Systems, and help meet the monitoring requirements of the NERC standards.

System availability is the most critical security requirement in most electric SCADA and DCS systems. Many organizations are hesitant to use technology that may impact legitimate communication, even if the probability is small. Tenable’s passive analysis component of SecurityCenter Continuous View 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 uncredentialed and credentialed scans to discover basic services associated with SCADA and ICS devices and control systems, such as ICCP or Modbus, and can also identify many different types of control systems such as KingView or Ecava IntegraXor software. Nessus also finds vulnerabilities in these systems, and can highlight exploitable control system devices.

- Specific SCADA plugins are available through a partnership with Digital Bond. These plugins discover and scan SCADA devices for known and newly discovered vulnerabilities.

- SecurityCenter Continuous View's Passive Vulnerability Scanner (PVS) scans network traffic for potential problems. As control systems are managed over the network, PVS tracks these devices, ports, and applications. Passive scanning is invaluable for devices considered "unscannable" and offers coverage not available through active scanning technology alone.

With hundreds of Nessus and PVS plugins currently available that discover and assess the security posture of common SCADA applications, devices, and protocols, 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 A" for details on each of the requirements outlined by each CIP. In some cases, Tenable's solutions can help perform a required action such as continuous network monitoring. The data gathered from Tenable solutions 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 to assess the security posture of the operating system and applications such as historians, operator consoles, and communication services used by the leading vendors. Digital Bond has developed dozens of different Nessus and SecurityCenter audit files for major control system vendors 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. Please see http://www.digitalbond.com/tools/bandolier/downloads/ for additional information about Digital Bond's Bandolier Security Audit Files.

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", which was formed on the standards established by NIST Special Publication 800-53. 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 to secure 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 Continuous View can be used 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 B" for details on each step of the RG 5.71 plan and how Tenable's solutions can be used to help ensure the availability, integrity, and confidentiality of systems owned or operated by NRC licensees.

Conclusion

Tenable's solutions can help an organization focus on reducing the burden of proving compliance with security guidelines and regulations for the energy and nuclear facility sectors. If your organization is subject to these regulations, leveraging solutions from Tenable can greatly facilitate demonstrating and reporting compliance and enhancing your security posture with minimal resource commitment.

About Tenable Network Security

Tenable Network Security provides continuous network monitoring to identify vulnerabilities, reduce risk, and ensure compliance. Our family of products includes SecurityCenter Continuous View™, which provides the most comprehensive and integrated view of network health, and Nessus®, the global standard in detecting and assessing network data. Tenable is relied upon by many of the world's largest corporations, not-for-profit organizations and public sector agencies, including the entire U.S. Department of Defense. For more information, visit tenable.com.

Appendix A: Tenable Solutions for NERC CIP Audits

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

Process	Name	How Tenable Can Help
CIP-002	**BES Cyber System Categorization**	
Purpose	To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES.	For systems that support the reliable operation of power generation and delivery, a risk assessment must be performed that analyzes the impact of each system not being available. Once the criteria for discovering which devices are "high impact", "medium impact", and "low impact" is determined, the actual assessment must be performed.
R1	Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1, and Parts 1.1 and 1.2.	As part of the effort to identify critical systems, Tenable's SecurityCenter Continuous View can be used to discover which systems 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 PVS can ensure that all protocols, including many SCADA protocols, and all operational modes for a network are considered without any adverse impact. SecurityCenter Continuous View can also identify network parties that connect to a BES Cyber System over a routable IP protocol. The distinction is subtle, but this will ensure that unneeded auditing and documentation of non-critical systems and assets is avoided. With Tenable's solutions, 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 BES Cyber System list. This information must be submitted to and approved by a CIP Senior Manager or delegate. Having the right information can help the manager make the right decision.
CIP-003	**Security Management Controls**	
Purpose	To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in	A policy must be in place to cover CIP-004 through CIP-011. Although Tenable's solutions 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 BES Cyber Systems are being accessed on the network. This information can help determine an access control policy.

	the BES.	A critical aspect of the policy is that it must be able to be audited. Tenable's solutions are uniquely positioned to show both policy failures and policy compliance events in both system configurations and overall activities.
R1	Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies(…)	Technically, all that CIP-003 requires is that a CIP Senior Manager be in charge of the review and approval of security policies. However, with Tenable solutions, 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 solutions, such as SecurityCenter Continuous View, allow for a Senior Manager to track overall risk, threat events, and compliance events that are unique to their environment.
CIP-004	**Personnel and Training**	
Purpose	To minimize the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.	Data from Tenable's solutions can be used for any personnel awareness and training programs to provide real numbers about raw vulnerabilities, attacks, policy violations, and compliance status. Threat data on a bulk electric entity's system can be a powerful security awareness tool.
R1 – 1.1	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	Awareness and training programs can be augmented to encompass the features and capabilities of Tenable solutions that monitor a BES Cyber System. For example, access control training can include a discussion that the base configuration of a system, including its password policy, logging policy, and permissions, are all audited by Nessus and SecurityCenter Continuous View on an ongoing basis. Similarly, understanding that all access events are logged by proxies or firewalls and analyzed by the SecurityCenter Continuous View is also relevant.
R2 – 2.1-2.3	Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in CIP-004-5.1 Table R2 – Cyber Security Training Program.	All personnel who have access to BES Cyber Systems need to undergo annual training. Training is required to include proper use of BES Cyber Systems, a discussion of the access controls, how critical cyber security information should be handled, and how to recover a cybersecurity asset from a cybersecurity incident. Tenable's products can help identify when a particular user is attempting to circumvent their given authority. For example, SecurityCenter Continuous View's LCE component can look for login failures or access attempts in both COTS and custom applications. 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)	
Purpose	To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.	An Electronic Security Perimeter (ESP) is the boundary around all BES Cyber Systems. Typically, this is a list of all communication access points such as modems, firewalls, or routers. Tenable's solutions can help in the following areas that are necessary to comply with this requirement: • All BES Cyber Systems "inside" an ESP as defined by specific access points such as firewalls, routers, and modems need to be documented. All of Tenable's solutions can aid in discovering and reporting about what is connected to which side of a network. • All non-critical BES Cyber Systems "inside" an ESP also need to be documented and protected. With the use of SecurityCenter's dynamic asset groups, this information can readily be analyzed for documentation support. • All assets deployed to enforce or monitor asset control such as firewalls, routers, and authentication servers can be discovered, reported, and documented.
R1 – 1.1-1.5	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter.	This requirement focuses on access to a BES Cyber System from outside an Electronic Security Perimeter. Tenable's solutions can help in several ways: • Access must be denied by default. This can be audited through the use of compliance checks in Nessus. 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 SecurityCenter Continuous View for reporting and analysis. • Tenable's solutions can help produce quarterly reviews of access control policies, changes in access control, or user account privileges and generate lists of terminated user accounts. • Only specific ports and services are to be authorized for use through an ESP. This can be continuously monitored through log analysis by SecurityCenter Continuous View, including auditing with active scanning by Nessus and passive monitoring with PVS. • Testing that systems display an appropriate banner can also be conducted through Nessus auditing.
R2 – 2.1-2.3	Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts,	SecurityCenter Continuous View provides the capability to assist with remote access management through the use of passive monitoring and log correlation. SecurityCenter dashboards and reports can give administrators a view of which systems are available for remote access, which ports, protocols, and services they use, which systems are attempting to access the environment remotely, and volume trending and analytics that can help detect potential intrusions from unauthorized

	where technically feasible, in CIP-005-5 Table R2 – Interactive Remote Access Management.	sources. Protocol detection also helps determine where encryption is being used (or not used) for remote system access.
CIP-006	**Physical Security of BES Cyber Assets**	
Purpose	To manage physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.	A plan for securing physical access to BES Cyber Systems and access control points must exist. Using Tenable's solutions to help identify all assets located within an environment and their access control points can help ensure the proper physical security plan exists. For organizations that use IP networks to implement cameras, physical sensors, or other types of alarm and monitoring systems, Tenable's solutions can be used to "watch the watchers" and monitor that network for specific attacks and security issues.
R1 – 1.1-1.9	Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented physical security plans that collectively include all of the applicable requirement parts in CIP-006-5 Table R1 – Physical Security Plan.	Tenable's solutions do not specifically help deploy physical access controls, but they can help identify systems that need to be physically secured. SecurityCenter Continuous View's LCE component can also perform very customizable correlation such as observing a successful physical access event and then observing a suspicious electronic event. If SecurityCenter Continuous View 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 as intended. There is a requirement to test these systems once every two years.
R2 – 2.1-2.3	Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented visitor control programs that include each of the applicable requirement parts in CIP-006-5 Table R2 – Visitor Control Program.	Logs for physical access need to be retained for at least 90 days for successful access and denied events. SecurityCenter Continuous View's LCE can be used to accept logs from a variety of physical access control devices such as card, badge, or palm readers. NERC allows a variety of methods for logging physical events. For low-tech methods, such as a log book, there is not much to analyze with Tenable solutions. However, the logs from electronic access control systems can be analyzed through SecurityCenter Continuous View.
R3 – 3.1	Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in CIP-006-5 Table R3 – Maintenance and Testing Program.	All outages or lapses in access control enforcement also need to be documented. If SecurityCenter Continuous View's LCE component 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 during testing and maintenance phases or unexpected outages.

CIP-007	Systems Security Management	
Purpose	To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.	Tenable Network Security has transformed vulnerability management and system security management from a periodic and repetitive cycle to a comprehensive assessment of network security, with the ability to provide an integrated view into the network, strengthening organizations' security posture and minimizing their attack surface. Tenable's SecurityCenter Continuous View is the only continuous network monitoring solution, which provides the most comprehensive and integrated view of enterprise health.
R1	Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-5 Table R1 – Ports and Services.	Documentation of the need for all enabled ports and a listing of authorized open ("listening") ports must be maintained for each BES Cyber System with the principal of "least use". Through SecurityCenter Continuous View, 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 needs to be disabled. After this initial assessment, active scanning and passive monitoring 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.
R2	Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-5 Table R2 – Security Patch Management.	According to NERC, all available patches must be analyzed within 35 days of their availability. It does not say exactly when a patch is to be deployed, just that its applicability be determined. Some patches and upgrades cause security functionality to be removed or overwritten. All of Tenable's solutions can help detect this sort of change. Tenable's solutions can also help determine if such changes have introduced new vulnerabilities. Tenable's SecurityCenter Continuous View is an ideal solution to determine missing patches across all operating systems and network assets. With tens of thousands of active and passive vulnerability checks, Tenable's solutions are 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.
R3	Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-5 Table R3 – Malicious Code Prevention.	Although Tenable does not offer an anti-virus product, its solutions 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 can determine when a host is not running anti-virus software or when the software on an asset is out of date with its signatures. In addition to testing the viability of anti-virus software, Nessus can also test the base configuration of each operating system, and for patches that may prevent malicious code from being executed on a system.
R4	Each Responsible Entity shall implement, in a manner that	In general, Tenable's solutions can help monitor all BES Cyber Systems in the following manner:

	identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-5 Table R4 – Security Event Monitoring.	• Nessus can ensure that each system has logging enabled. • SecurityCenter Continuous View's LCE component can be configured to retain all logs for at least 90 days. • Through the use of SecurityCenter Continuous View, multiple users can analyze these logs for their specific asset groups when required. This ensures that system owners can perform the necessary analysis of security events. SecurityCenter Continuous View can also perform a wide variety of attack detection, attack verification, and general detection of "suspicious" events. These alerts can be sent by SecurityCenter Continuous View to specific business units or to system owners.
R5	Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-5 Table R5 – System Access Controls.	In addition to the requirements of CIP-005 R2, Tenable's solutions can also help meet the requirements of CIP-007 R5. These include (but are not limited to): • *Generating Audit Trails* – Nessus configuration audits can be used to ensure that audit trails of logins, failed logins, and logouts are enabled. SecurityCenter Continuous View's LCE component can also be used to collect those log events and analyze them for attacks, trends, and to also build reports. • *Securing Shared Accounts on BES Cyber Systems* – Nessus can be used to test for known default accounts that exist in BES Cyber Systems. • *Enforcement of Password Complexity* – Nessus can be used to test Windows, Linux, and Unix systems for a robust password policy. This can include password length, complexity, frequency of change, and testing for generic or default vendor passwords.
CIP-008	**Incident Reporting and Response Planning**	
Purpose	To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.	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. (http://www.nerc.com/pa/Stand/1200Cybersecurityurgent/IAW_SOP.pdf) 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 the reporting of malicious or suspicious events that have the ability to

		compromise the Electronic Security Perimeter of a BES Cyber System.
R1	Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications.	All of Tenable's solutions can be used to help deter attacks, minimize their attack surface, and also assist in detecting the attack and assessing the scope of the attack. Accurately knowing where an attacker has been able to achieve unauthorized access can help determine the correct incident response plan. The ability to combine vulnerability and security events into one product, such as SecurityCenter Continuous View, 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. All information about an incident needs to be maintained for three years. If SecurityCenter Continuous View's LCE component 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, SecurityCenter Continuous View can collect vulnerability and configuration data about the targets involved.
R2	Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing.	Tenable's SecurityCenter Continuous View can be used in the implementation and testing of any incident response plan through the use of its reporting, alerting, and workflow functions. Once an incident response plan has been implemented, using these functions allows an incident response team to test the speed and efficiency of the plan throughout multiple levels of an organization.
R3	Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.	Alerting and assigning workflow tickets through SecurityCenter Continuous View ensures that all interested parties are involved in incident response processes and procedures, and allows plan reviewers to identify and communicate any gaps that may exist in the plan so those gaps can be corrected for future tests and actual incidents.
CIP-009	**Recovery Plans for BES Cyber Systems**	
Purpose	To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.	All Tenable solutions can be used to help test and assess recovery plans, including the security and availability of backup technologies such as SANs and NASs. Increasingly, Tenable has been adding capabilities to Nessus and PVS to detect backup protocols, as well as vulnerabilities in specific backup and recovery applications such as Veritas.
R1	Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable	Tenable's solutions can help maintain more accurate recovery plans for BES Cyber Systems. For example, PVS can be used to discover which nodes communicate to BES Cyber Systems. This can help build realistic redundancy and recovery plans. Tenable's solutions can also be used to

	requirement parts in CIP-009-5 Table R1 – Recovery Plan Specifications.	keep these plans up to date with any known changes.
R2	Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, its documented recovery plan(s) to collectively include each of the applicable requirement parts in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.	Each recovery plan must be tested at least once every 15 months. Plans can be loosely grouped by specific profiles of unique BES Cyber Systems, and these assets can be determined effectively by Tenable's solutions. For example, PVS can be used to identify all nodes that speak specific SCADA protocols.
R3	Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable requirement parts in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.	Any changes to the recovery plans must be documented within 90 days of their discovery. Tenable's solutions can help support the addition of new BES Cyber Systems, changes to the profiles of these devices, and changes in access control that affect changes to the actual recovery plans themselves.
CIP-010	**Configuration Change Management and Vulnerability Assessments**	
Purpose	To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.	Using SecurityCenter Continuous View, organizations can achieve continuous monitoring of configurations and configuration change management from the integration of Nessus scans, real-time monitoring using Tenable's unique PVS, and the LCE. This combined solution helps organizations: • Detect system change events in real time and automatically perform a configuration audit on new or changed systems • Ensure that logging is configured correctly for Windows and Unix hosts • Audit the configuration of a web application's operating system, application, and SQL database SecurityCenter Continuous View also helps to identify and remove vulnerabilities and malware on hosts, devices, and applications. Defenses are optimized by gaining contextual insight into system activity by aggregating and correlating log data, and extracting actionable forensic analytics at the host/network level.
R1	Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-010-1 Table R1 – Configuration Change Management.	The change detection capabilities of Tenable's solutions can serve as a useful test of the change control policy implementation. For configuration management, Nessus and SecurityCenter 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.

R2	Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-010-1 Table R2 – Configuration Monitoring.	A key feature of Tenable's solutions is to detect and monitor change: • Successive network vulnerability scans conducted by Nessus and SecurityCenter always produce "change" lists of new hosts, applications, and vulnerabilities. • PVS detects new hosts in real time. SecurityCenter Continuous View's LCE component can analyze logs and 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. LCE can also examine software versions in logs for vulnerabilities.
R3	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-010-1 Table R3– Vulnerability Assessments.	Vulnerability assessments are required at least once every 15 calendar months. Tenable's solutions 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 scans can be controlled and analyzed with SecurityCenter. If scanning is not an option due to a potential system availability impact, PVS can be used to discover which ports are in use. • SecurityCenter Continuous View can be used throughout the year to perform vulnerability assessments in advance of the required annual audit. This can ensure a "good test" and can help identify any deviations prior to the annual test. • Tenable's solutions can help discover and enumerate all routers, firewalls and wireless access points. Although Tenable's solutions 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 continuous network monitoring with the PVS. • A vulnerability audit is required for the access points themselves. This can include a configuration review of system settings, an audit of missing patches, and password policy testing. A plan to mitigate or correct any vulnerabilities found during the audit is also required. SecurityCenter Continuous View can make recommendations to mitigate vulnerabilities and track when they are no longer an issue.
CIP-011	**Information Protection**	
Purpose	To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.	While Tenable's products can't write the information protection requirements to protect BES Cyber Systems, the continuous network monitoring supported by SecurityCenter Continuous View will help enforce those requirements through asset identification, passive monitoring between all systems within the environment, and log correlation that can be analyzed to detect unauthorized access. SecurityCenter Continuous View can monitor hosts, systems, and devices where BES Cyber System Information is held and alert when an unauthorized access attempt has been detected. These alerts can then be communicated to system administrators and other parties for review

		and incident response, where necessary.
R1	Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP- 011-1 Table R1 – Information 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 SecurityCenter 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, the local host auditing abilities of SecurityCenter and Nessus can be used to monitor for compliance. • If key systems with sensitive data are known, they can be easily monitored for intrusions, access attempts, and changes to their configuration. Both SecurityCenter and LCE can help monitor these systems. SecurityCenter can create on-the-fly asset groups that include systems with sensitive data. This assists in reporting, log analysis, and visualization of the security data about these systems. Comparisons between different asset groups that contain sensitive data can also be made.
R2	Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal.	Tenable products do not assist with removal, reuse, or destruction of actual data or hardware.

Appendix B: 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 the "Technical Security Controls" in Appendix B of RG 5.71.

Section	Name	How Tenable Can Help
A.3.1.3	Identification of Critical Digital Assets (CDAs)	Nessus and PVS can be used to actively and passively identify plant systems, equipment, communication systems, and networks. SecurityCenter 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 SecurityCenter Continuous View and its components, and the information gathered can be stored in SecurityCenter to review network activity and configurations. Tenable's 3D Tool also provides a visual overview of a network's layout based on data maintained by SecurityCenter, 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	SecurityCenter 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	SecurityCenter allows for the review and analysis of defense models, technical controls, and attack vectors. Active vulnerability scanning and passive monitoring through Nessus and PVS, as well as log analysis through SecurityCenter CV, 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. SecurityCenter CV provides near real-time updates found through network activity and system logs, and can be scheduled to perform active scans after plugin updates or change control windows. SecurityCenter CV ties all of this information together to provide a continually updated assessment of an organization's security, compliance, and risk posture while continuously monitoring for new changes and vulnerabilities across the network.
A.4.1.1	Periodic Assessment of Security Controls	Data gathered by SecurityCenter CV 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's solutions 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 Scans	Tenable's Nessus® is the world's most widely-deployed vulnerability, configuration, and compliance assessment product. Nessus prevents network attacks by reducing your attack surface – identifying the vulnerabilities and configuration issues that hackers could use to penetrate your network, whether your network is on-premises, in the cloud, or hybrid.

A.4.2	Change Control	SecurityCenter CV 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 solutions can help detect and measure violations to an established configuration management policy. SecurityCenter CV can be used to assess specific asset classes of servers or network devices with specific audits. Similarly, continuous network monitoring and 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 SecurityCenter CV, 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 generate a 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 SecurityCenter CV to assist with modifying security policies, procedures, and practices. Tenable's 3D Tool can assist in developing 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 solutions can also detect changes to network access control policies through the use of repeated network scans, passive network monitoring, and log analysis. SecurityCenter CV's LCE component provides full log aggregation, storage, and search capabilities. 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. SecurityCenter CV unifies access data and provides a large number of filters to analyze user activity, and 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's 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's active scanning and passive monitoring 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 SecurityCenter CV, sensitive data in motion and at rest can be detected in near real time to identify breaches of information flow control policy. SecurityCenter CV's LCE component can also be configured with a list of all valid

		user accounts that access a particular asset group. When logins occur (failed or successful), SecurityCenter CV can generate an 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. SecurityCenter CV provides the ability to associate an IP address with a user name, which aids in monitoring insiders to ensure separation of duties. SecurityCenter CV can manage multiple LCE components and provides powerful log search capabilities across multiple LCE instances. This facilitates an enterprise-wide search of a particular user's activity. SecurityCenter CV 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. SecurityCenter CV's LCE component will normalize all logs based on the user ID of the authenticated user. This allows quick, 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. SecurityCenter CV's LCE component 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 SecurityCenter CV can be used to monitor unsuccessful login attempts across the enterprise and determine a pattern of attack.
B.1.8	System Use Notification	Tenable's solutions can audit network devices to ensure a default warning banner message is displayed before users can log in.
B.1.9	Previous Logon Notification	Tenable's solutions can audit network devices to ensure a previous login notification setting is enabled.
B.1.16	"Open/Insecure" Protocol Restrictions	SecurityCenter Continuous View can be used to look for any non-encrypted services on specific assets that are supposed to use SSH or SSL for administration. SecurityCenter CV's LCE component 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. SecurityCenter CV can actively and passively 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 assets such as firewalls, routers, and modems need to be documented. Tenable's solutions 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	Tenable's solutions include the ability to discover when new hosts are added to the network including new laptops, PDAs, or cell phones. SecurityCenter CV's LCE

	Devices	Client 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 SecurityCenter CV and can be used to easily search and monitor USB activity across the enterprise.
B.2.2	Auditable Events	SecurityCenter CV's LCE component has the ability to store, compress, and search any log that is sent to it. 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. 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	SecurityCenter CV'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	SecurityCenter CV's LCE can be configured to alert administrators when a hard disk is nearing capacity. LCE Clients also report CPU, memory, and disk utilization. SecurityCenter CV also maintains a real-time status of all LCE servers and their clients.
B.2.5	Response to Audit Processing Failures	SecurityCenter CV's LCE can be configured to alert administrators when a hard disk is nearing capacity. LCE Clients also report CPU, memory, and disk utilization. SecurityCenter CV also maintains a real-time status of all LCE servers and their clients.
B.2.6	Audit Review, Analysis, and Reporting	SecurityCenter CV'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. LCE has the ability to import syslog data from multiple sources to analyze data from past change-control events. 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	SecurityCenter CV'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 SecurityCenter CV provides the ability to quickly summarize events across the entire enterprise.
B.2.8	Time Stamps	All events arriving at the SecurityCenter CV's LCE are uniquely time-stamped.
B.2.9	Protection of Audit Information	SecurityCenter CV 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 SecurityCenter CV's LCE raw log data is configurable on a "per-LCE" basis.
B.2.10	Nonrepudiation	SecurityCenter CV'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 SecurityCenter CV. All search results are saved in a compressed format along with a checksum so that they can be used as forensic evidence. 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	SecurityCenter CV's LCE provides 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 LCE that may be searched from the SecurityCenter console. This option includes a script to monitor disk use and generate an alert if resources reach a configurable threshold.