tenable® network security

NIST Framework for Improving Critical Infrastructure Cybersecurity Technical Control Automation

Automating Cybersecurity Framework Technical Controls with Tenable SecurityCenter Continuous View™

February 22, 2016

(Revision 1)

Table of Contents

Introduction

This paper provides insight to how Tenable addresses the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (CSF), which calls for "a set of industry standards and best practices to help organizations manage cybersecurity risks."

Specifically, this paper describes how Tenable SecurityCenter Continuous View™ (SecurityCenter CV™) can be leveraged to help meet the guidelines and practices outlined in the CSF through automation of its technical controls. Organizations can use the CSF to take a risk-based approach to align their security processes with business requirements. Because the CSF is not intended to be a "one size fits all" approach, Tenable's solution is scalable across all organizational sizes and can be adapted for specific use across multiple industries.

What is the Cybersecurity Framework?

The Cybersecurity Framework was released in February 2014 as a result of Executive Order 13636, "Improving Critical Infrastructure Cybersecurity", which was signed on February 12, 2013. The CSF was created through collaboration between the United States government and the private sector, and places a focus on aligning business needs and priorities with cybersecurity and risk management. The CSF is comprised of three parts: the **Core**, the **Implementation Tiers**, and the **Profile**. The **Core** identifies cybersecurity activities and practices that share a commonality across critical infrastructure sectors. These activities and practices are grouped into five Functions: Identify, Protect, Detect, Respond, and Recover. The **Implementation Tiers** provide entities with context for managing cybersecurity risks and applying a plan to their specific organization. **Profiles** are used to match cybersecurity objectives to business requirements, risk tolerance, and resources.

Tenable's Solution

From a network security feature set, SecurityCenter CV is a robust solution that supports over 90% of the CSF's technical controls. SecurityCenter CV is also extremely powerful for communicating CSF conformance results to many different internal and external stakeholders.

SecurityCenter Continuous View is a comprehensive solution that provides continuous visibility and critical context, enabling decisive action. With advanced analytics, it gives you continuous assurance that your security program is working. Capabilities include:

- Information on which assets are connected to the network and how they are communicating
- Active monitoring of host activities and events, including who is accessing them and what is changing
- Identification of previously unknown resources, changes in behavior, and new application usage
- Near real-time metrics for continuous security and compliance
- Correlation of real-time activity with the state-based vulnerability
- Security assurance using Tenable exclusive Assurance Report Cards (ARCs) that measure effectiveness of security investments
- Highly customizable dashboards, reports, and workflows for rapid response
- Communication of consolidated metrics
- Trends across systems, services, and geographies
- Controls team member permissions by role
- Advanced analytics with actionable information and trending to prioritize events/alerts

The key features of SecurityCenter CV as they relate to automating the CSF technical controls are described in the following sections.

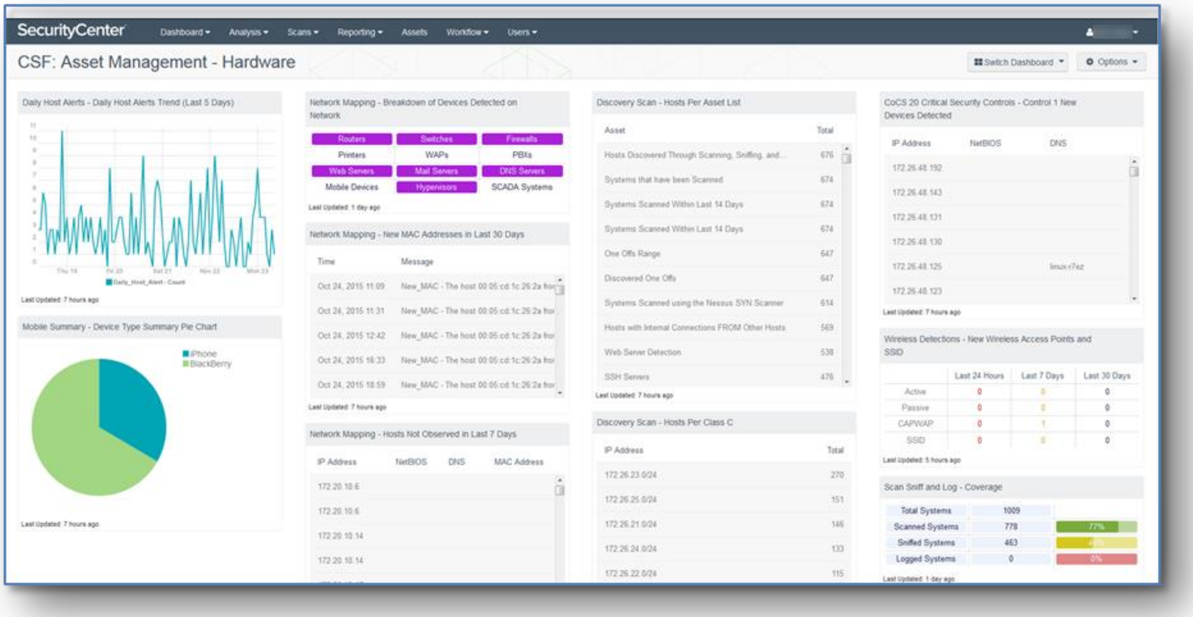
Automating Technical Controls

The CSF Core contains five Functions identified to improve security posture. These Functions are the “high level view” of numerous categories and subcategories that are more specific to drive particular outcomes. These categories and subcategories can be thought of as “controls” or “control objectives” used in other security and compliance frameworks. There are two control types: administrative and technical. Administrative controls are typically procedural and can be implemented and audited using manual processes, where technical controls benefit from the use of automated solutions because of the difficulty of performing manual audits for the control. For example, if we take a look at the “Risk Assessment” category within the Identify function, we will find examples of both administrative and technical controls:

- Administrative Control (ID.RM-1): “Risk management processes are established, managed, and agreed to by organizational stakeholders.” Establishing risk management processes requires people to develop, propose, and adopt procedures and is therefore an administrative control. In this example, control automation is not feasible because establishing, managing, and agreeing to risk management processes is an occasional activity.

- Technical Control (ID.RA-1): “Asset vulnerabilities are identified and documented.” Identifying and documenting vulnerability identification and documentation across all IT and ICS assets are huge, detailed tasks that must be frequently performed. These tasks cannot easily be performed manually, and automation is highly recommended. Technical controls account for about half of all of the controls listed in the CSF, and because they typically deal with huge amounts of fast moving data, automation for the technical controls is necessary for conforming to the CSF.

SecurityCenter CV supports over 90% of the CSF technical controls and builds them into an automated control foundation that helps organizations manage cyber risk and achieve their target security profile. For example, SecurityCenter CV’s asset discovery capabilities fulfill the Identify: Asset Management-1 control, which instructs that physical devices and systems within the organization are inventoried.



CSF: Asset Management - Hardware

Daily Host Alerts - Daily Host Alerts Trend (Last 5 Days)

Last Updated: 7 hours ago

Mobile Summary - Device Type Summary Pie Chart

Last Updated: 7 hours ago

Network Mapping - Breakdown of Devices Detected on Network

Last Updated: 1 day ago

Network Mapping - New MAC Addresses in Last 30 Days

Time	Message
Oct 24, 2015 11:09	New_MAC - The host 00:05:cd:1c:26:2a fro
Oct 24, 2015 11:31	New_MAC - The host 00:05:cd:1c:26:2a fro
Oct 24, 2015 12:42	New_MAC - The host 00:05:cd:1c:26:2a fro
Oct 24, 2015 16:33	New_MAC - The host 00:05:cd:1c:26:2a fro
Oct 24, 2015 18:59	New_MAC - The host 00:05:cd:1c:26:2a fro

Last Updated: 7 hours ago

Network Mapping - Hosts Not Observed in Last 7 Days

IP Address	NetBIOS	DNS	MAC Address
172.20.10.6			
172.20.10.6			
172.20.10.14			
172.20.10.14			

Discovery Scan - Hosts Per Asset List

Asset	Total
Hosts Discovered Through Scanning, Sniffing, and...	676
Systems that have been Scanned	674
Systems Scanned Within Last 14 Days	674
Systems Scanned Within Last 14 Days	674
One Offs Range	647
Discovered One Offs	647
Systems Scanned using the Nessus SYN Scanner	614
Hosts with Internal Connections FROM Other Hosts	569
Web Server Detection	538
SSH Servers	476

Last Updated: 7 hours ago

Discovery Scan - Hosts Per Class C

IP Address	Total
172.26.23.0/24	270
172.26.25.0/24	151
172.26.21.0/24	146
172.26.24.0/24	133
172.26.22.0/24	115

CoCS 20 Critical Security Controls - Control 1 New Devices Detected

IP Address	NetBIOS	DNS
172.26.48.192		
172.26.48.143		
172.26.48.131		
172.26.48.130		
172.26.48.125		linux-r7ez
172.26.48.123		

Last Updated: 7 hours ago

Wireless Detections - New Wireless Access Points and SSID

	Last 24 Hours	Last 7 Days	Last 30 Days
Active	0	0	0
Passive	0	0	0
CAPWAP	0	1	0
SSID	0	0	0

Last Updated: 5 hours ago

Scan Sniff and Log - Coverage

Total Systems	1009	
Scanned Systems	778	77%
Sniffed Systems	463	[illegible]
Logged Systems	0	0%

Last Updated: 1 day ago

SecurityCenter Continuous View Dashboard for CSF ID.AM-1: Asset Management – Hardware

Tenable and the Cybersecurity Framework Core Functions

Tenable SecurityCenter CV enables organizations to automate the CSF's technical controls by bringing active scanning and passive monitoring, configuration auditing, host event and data monitoring and analysis, reporting, and alerting together with risk classification, assessment, and mitigation in a scalable enterprise security system. Once an organization begins to use the CSF Core as a baseline for its cybersecurity and risk activities, SecurityCenter CV makes it easier to take the step towards developing a detailed Target Profile that is both achievable and manageable. Definitions of each function are quoted from the CSF, and several examples are explained below.

Identify: *The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business ne*eds. Examples of outcome Categories within this Function include: Asset *Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy*.

Using the Risk Assessment category as an example, there are three technical controls, all of which can be automated or supported with the use of SecurityCenter CV. Subcategory ID.RA-2 requires that "Threat and vulnerability information is received on a daily basis from information sharing forums and sources." SecurityCenter CV updates its vulnerability information and threat intelligence, provided by multiple third-parties, on a daily basis. The Risk Assessment category has two other subcategories that state "Asset vulnerabilities are identified and documented" and "Threats, both internal and external, are identified and documented." Both of these subcategories are also automated through active scanning, passive monitoring, and event analysis.

Protect: *The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.*

Using the Information Protection Processes and Procedures category as an example, SecurityCenter CV has numerous capabilities to automate the technical controls. Examples include:

- PR.IP-1: Baselines are created and maintained
- PR.IP-2: System development lifecycle to manage systems is implemented
- PR.IP-3: Configuration change control processes are in place

The CSF contains 22 technical subcategories for Protect, 19 of which are automated or supported by SecurityCenter CV. For example, SecurityCenter CV performs baseline audits, which allows organizations to scan systems based on a "standard image" by which to compare other systems, and can also alert when there are configuration changes made on endpoint devices and systems.

Detect: *The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.*

Using the Security Continuous Monitoring category as an example, SecurityCenter CV has numerous automated capabilities to fulfill these controls. Examples include:

- DE.CM-1: Network is monitored to detect potential cybersecurity events
- DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events
- DE.CM-4: Malicious code is detected
- DE.CM-5: Unauthorized mobile code is detected

The CSF contains 14 technical subcategories for Detect, 13 of which are automated or supported by SecurityCenter CV. For example, through active and agent scanning, continuous listening, and host data analysis, SecurityCenter CV can observe network and user activity, detect vulnerabilities and events, and alert and report on these as part of an overall cybersecurity plan.

Respond: *The Respond Function supports the ability to contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.*

Recover: *The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.*

The Respond and Recover Functions are comprised of categories and subcategories that are mostly administrative in nature, such as "Response plan is executed during or after an event," "Recovery plans incorporate lessons learned," and "Public relations are managed." SecurityCenter CV's capabilities are focused primarily on the CSF's technical controls, and although some exceptions exist, SecurityCenter CV does not provide full support for the administrative Respond and Recover Functions.

Asset-Centric Analysis

SecurityCenter CV organizes network assets into categories based on data from a combination of network scanning and auditing, imported agent data, passive network monitoring, host data, 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 assets can be easily identified, and vulnerability assessments on assets can be performed to determine and assess risk.

SecurityCenter Continuous View's dynamic asset list feature applies across the Identify Function of the CSF and automatically adds newly discovered assets to all applicable asset lists. SecurityCenter CV has the ability to parse the results from active scans, passive monitoring, and host event data to build dynamic lists of assets, and a single asset can be a member of multiple asset lists. For example, a dynamic rule can be created to generate a list of IP addresses that has ports 25 and 80 open. These rules can be very sophisticated and take into account addressing, open ports, specific vulnerability IDs, and discovered vulnerability content. SecurityCenter CV includes more than 200 dynamic asset list templates that you can use out of the box or that you can tailor for your specific requirements.

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

Grouping assets within SecurityCenter CV by attributes such as business service and/or data classification will allow you to tailor and assess controls based on risk. For example, to tailor the control ID.RA-1: Asset vulnerabilities are identified and documented, you could scan and report on high risk systems for vulnerabilities on a daily basis and scan and report on moderate risk systems weekly.

Concurrent and Continuous Monitoring

Strong security, as prescribed in the CSF, requires broad visibility of extended networks, including IT systems, industrial control systems (ICS), virtual infrastructure, cloud, and BYOD. This visibility cannot rely solely on point-in-time data acquisition; it requires continuous, real-time data. SecurityCenter CV acquires security data from across organizations, using sources such as network traffic, virtual systems, mobile device management, patch management, host activity and monitoring, as well as external sources of threat intelligence to feed an intelligent monitoring system. It analyzes this data to identify and prioritize anomalies and suspicious behavior so you can efficiently investigate and resolve them.

"Appendix A" breaks down the CSF Core into its functions, categories, and subcategories, and describes how SecurityCenter Continuous View can automate the vast majority of the CSF's Core technical controls.

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's Solution for the Cybersecurity Framework

Note: Tenable SecurityCenter Continuous View can help organizations automate more than 90% of the Cybersecurity Framework Core's technical controls. Specific categories and subcategories of the Core are listed in the table below, along with how SecurityCenter CV can be matched to each item. The examples below are not all-inclusive, and in many cases, SecurityCenter Continuous View can be used for more in-depth coverage of a specific subcategory.

Process	Name	How Tenable Can Help
ID	**Identify**	
ID.AM	**Asset Management**	
ID.AM-1	Physical devices and systems within the organization are inventoried	The combination of active and passive analysis of the network identifies and inventories physical systems active on the network. Using dynamic asset lists, SecurityCenter CV categorizes IT and ICS assets into groups by component type, hardware specifications, or physical location.
ID.AM-2	Software platforms and applications within the organization are inventoried	The combination of active and passive analysis of the network identifies and inventories individual software and applications, such as operating systems, web browsers, and office suites. SecurityCenter CV utilizes active scanning to audit a specified network segment for new software platforms and applications, and listens continuously to passively analyze network traffic from those platforms and applications at the packet layer. Using dynamic asset lists, SecurityCenter CV can also categorize assets into groups by component type, software specifications, or installed applications.
ID.AM-3	Organizational communication and data flows are mapped	SecurityCenter CV includes 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. SecurityCenter CV 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.
ID.AM-4	External information systems are catalogued	SecurityCenter CV uses asset discovery and system analysis to identify authorized cloud services or systems that were not configured to be part of the normal infrastructure. Interactions are primarily detected through passive traffic analysis or via logged events; however, some cloud applications and vulnerabilities are also detected through active scans.
ID.RA	**Risk Assessment**	
ID.RA-1	Asset vulnerabilities are identified and documented	SecurityCenter CV gathers both active and passive vulnerability data for all assets. Current vulnerabilities are documented through scan results, reports, and dashboards that can be shared with all levels within an organization.
ID.RA-2	Threat and vulnerability information is received from information sharing forums and sources	SecurityCenter CV receives security advisories, vulnerability information, and threat intelligence from multiple external sources on a daily basis. This ensures that recent and relevant vulnerability data is being referenced by SecurityCenter CV.

ID.RA-3	Threats, both internal and external, are identified and documented	SecurityCenter CV's management of log analysis, active vulnerability assessments, imported Nessus Agent data, and passive vulnerability detection discovers changes in the network that may indicate the presence of an internal or external threat. SecurityCenter CV identifies 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.
PR	**Protect**	
PR.AC	**Access Control**	
PR.AC-1	Identities and credentials are managed for authorized devices and users	SecurityCenter CV can test for the presence of accounts that should or should not be present on a system. The presence of an account can also be detected through passive network monitoring and host data analysis.
PR.AC-3	Remote access is managed	Tenable's solution can audit the security of remote access infrastructure. A wide variety of data from remote access devices can be monitored to discover intrusions, non-compliant activity, or other types of unauthorized access. For example, SecurityCenter CV can monitor the activity of remote employees who enter a network via VPN, network, or dial in connections. Nessus Agents gather configuration, vulnerability, and policy information even when devices leave the network, and SecurityCenter CV can determine in real-time if remote connections are encrypted in accordance with the site security policy. Tenable's solution includes the ability to discover when new hosts are added to the network, including laptops, phones, and other mobile devices. SecurityCenter CV is able to identify the device model and its operating system, and the "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 three months.
PR.AC-4	Access permissions are managed, incorporating the principles of least privilege and separation of duties	Tenable's solution enables testing of servers to ensure they are configured with the proper level of access control, including detecting configurations of servers that have not been locked down to a least level of privilege. For example, a running 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 SecurityCenter CV to ensure servers are configured to be secure by default.
PR.AC-5	Network integrity is protected, incorporating network segregation where appropriate	Multiple active scanners can be placed across an enterprise to perform remote network audits. This allows SecurityCenter CV users to audit parts of a network that may have excessive trust relationships with other parts. Events from any system(s) monitoring the boundaries of a network can be normalized and analyzed through SecurityCenter CV. The information collected by SecurityCenter CV 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, an event stating this would be noted. With SecurityCenter CV, 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 an IDS/IPS and with known "blacklisted" IP addresses, and a variety of other threat monitoring rules.
PR.DS	**Data Security**	
PR.DS-1	Data-at-rest is protected	Unencrypted sensitive data at rest can be detected by SecurityCenter CV in near real-time and identify breaches of information flow control policy. Static file audits have the ability to look into certain document types and discover if they contain sensitive data. SecurityCenter CV 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 alert if the user in question is not on the authorized list.
PR.DS-2	Data-in-transit is protected	Through continuous listening on a network, SecurityCenter CV analyzes data in motion and can detect unencrypted sensitive data, such as credit card numbers and Social Security numbers, as well as files traversing the network. SecurityCenter CV can determine in real-time if remote connections are encrypted in accordance with the site security policy. SecurityCenter CV can be used to look for any non-encrypted services on specific assets that are supposed to use SSH or SSL for administration. If server logs are being monitored, SecurityCenter CV can correlate network traffic with logins to see that only encrypted protocols are being used.
PR.DS-4	Adequate capacity to ensure availability is maintained	SecurityCenter CV monitors 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. SecurityCenter CV can also monitor system resource changes, detect event spikes, and identify high utilization events on servers and other devices, which can aid in ensuring performance and availability of services across the enterprise.
PR.DS-5	Protections against data leaks are implemented	SecurityCenter CV performs 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. SecurityCenter CV automatically analyzes any log for statistical significance, if it is evidence of a compromise or if there has been a compliance infraction.

		SecurityCenter CV also actively audits and passively monitors network activity. SecurityCenter CV unifies data from a wide variety of security devices to provide a correlated view of the enterprise security posture.
PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity	SecurityCenter CV processes events on file changes, from which you can obtain additional information on the file change made, when the change was made, which host the change was made on, and by which user. Active auditing can also be used to perform MD5 checksums of Linux and Unix servers to ensure that the file(s) being monitored have not been changed.
PR.IP	**Information Protection Processes and Procedures**	
PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained	Tenable SecurityCenter CV can help discover the baseline of a network footprint with data imported from Nessus Agents, active scanning, and continuous listening. If a baseline is already known, it can be loaded into SecurityCenter CV 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.
PR.IP-2	A System Development Life Cycle to manage systems is implemented	Between active scanning, passive monitoring, host data analysis, alerting, remote device management, and more, SecurityCenter CV possesses the ability to support the implementation of an effective System Development Life Cycle. SecurityCenter CV can help protect against vulnerabilities such as coding errors and the use of vulnerable libraries in order to assist the organization in securing its application development and lifecycle management.
PR.IP-3	Configuration change control processes are in place	SecurityCenter CV can be used to manage data collected from active scans, passive monitoring and host data analysis to continuously assess changes to servers, infrastructure devices, users, software, and more. SecurityCenter CV can also be used to provide independent verification of any patches or security issues in accordance with an established change management or security and configuration management plan.
PR.IP-7	Protection processes are continuously improved	SecurityCenter CV can be used to monitor a wide variety of security controls. Host data analysis, configuration audits, vulnerability remediation, and many other types of controls can be monitored and analyzed by Tenable’s solution, which allows for the continual improvement of an organization’s security and compliance processes.
PR.IP-12	A vulnerability management plan is developed and implemented	Tenable’s solution delivers continuous visibility into all known and previously unknown assets, making it possible to bring all assets under management to support a complete vulnerability management plan and program. SecurityCenter CV continuously collects information from a broad spectrum of unique sensors and capabilities, including active scanning and auditing, passive monitoring and listening, intelligent connectors, agent scanning, and host activity data to facilitate vulnerability management plans.

PR.MA	Maintenance	
PR.MA-1	Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	SecurityCenter CV can be used to monitor maintenance and patching processes. Although one primary focus is to integrate and monitor the effectiveness of the patch management system, SecurityCenter CV can be used to look for unauthorized patching from hackers, administrators hand-compiling "fixes" to security issues, and to look for unauthorized software and operating systems.
PR.MA-2	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	SecurityCenter CV can be used to perform a "before and after" configuration audit of systems undergoing maintenance. Remote maintenance of employee devices can be assisted through asset information that is reported to SecurityCenter CV from Nessus Agents. Host and network activity for the assets in question can be monitored with SecurityCenter CV, which can also determine in real-time if remote connections are authorized and encrypted in accordance with the organization's security policy.
PR.PT	**Protective Technology**	
PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	SecurityCenter CV 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. These logs can be easily accessed by designated personnel for review.
PR.PT-2	Removable media is protected and its use restricted according to policy	Tenable's solution 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 can be used to easily search and monitor USB activity across the enterprise.
PR.PT-3	Access to systems and assets is controlled, incorporating the principle of least functionality	Tenable's solution enables 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. SecurityCenter CV passively monitors network data flows and can be configured to monitor for access to a number of specific unencrypted data types (e.g., credit card data, patient health information, etc.) across specified network segments, as well as access to those assets.
PR.PT-4	Communications and control networks are protected	Tenable's solution can audit the security of remote access infrastructure for vulnerabilities. A wide variety of data from remote access devices and control networks can be monitored to discover intrusions or non-compliant activity. For example, SecurityCenter CV can determine in real-time if remote connections are encrypted in accordance with the site security policy. In addition, SecurityCenter CV can provide an inventory of wireless access points, events from wireless devices, and wireless vulnerabilities.

DE	Detect	
DE.AE	**Anomalies and Events**	
DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed	Tenable SecurityCenter CV can help discover the baseline of a network footprint and user activity through active and passive vulnerability and event analysis, as well as NetFlow and network protocol monitoring. If a baseline is already known, it can be loaded into SecurityCenter CV 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.
DE.AE-2	Detected events are analyzed to understand attack targets and methods	Tenable SecurityCenter CV 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. SecurityCenter CV has the ability to import syslog data from multiple sources in order to analyze data from past change-control events. It can also accept change logs and correlate these events with suspicious events and IDS attacks. Previous searches can be re-launched against the latest logs, and SecurityCenter CV can also provide detailed statistics on passively detected events across the network.
DE.AE-3	Event data are aggregated and correlated from multiple sources and sensors	SecurityCenter CV receives data from Tenable’s active scanners and passive monitors as well as through host data analysis. SecurityCenter CV provides event data from devices within the organization, remote devices outside of the organization, and many events such as network anomalies, unauthorized configuration changes, malware outbreaks, and more. 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 agent that is installed at the host generating logs.
DE.AE-4	Impact of events is determined	SecurityCenter CV allows for coordination and communication among multiple organizational entities and departments, such as information system owners, system administrators, information security staff, and risk management teams. Summary reports and detailed reports can be generated and sent to groups, reducing the time for response and increasing team involvement across an organization.
DE.CM	**Security Continuous Monitoring**	
DE.CM-1	The network is monitored to detect potential cybersecurity events	Tenable’s solution can be used to continuously monitor a wide variety of network activity and events. Host data analysis, configuration audits, software vulnerabilities, and many other types of data can be gathered by SecurityCenter CV, which analyzes, monitors, and reports on potential and actual cybersecurity events.
DE.CM-3	Personnel activity is monitored to detect potential cybersecurity events	Tenable’s solution 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 accounts. The presence of an account can also be detected through network and host data analysis.

		SecurityCenter CV can help identify malicious insiders, or identify what a particular individual has been doing. For example, active scanning can be used to audit servers to check that only authorized accounts exist. SecurityCenter CV can also produce lists of which accounts have had access to certain sensitive systems.
DE.CM-4	Malicious code is detected	SecurityCenter CV identifies malicious software and botneted systems with three very different methods. First, for Windows credentialed scans, Nessus examines the file checksum of every running process and supporting file against an industry index of the top 25 anti-virus vendors. Second, Nessus also leverages a high-quality botnet IP and DNS list to see if a scanned asset is part of a known botnet, communicating with a known botnet, or configured with botnet information such as a DNS server or web content used to propagate the botnet. Finally, Nessus offers a variety of specific local and credentialed checks that identify specific malware activity, such as modification of the LMHOSTS file on Windows platforms.
DE.CM-5	Unauthorized mobile code is detected	Tenable's solution performs a wide variety of audits for vulnerabilities in mobile code. Examples include, but are not limited to, Java, Flash, ActiveX, and PDF. SecurityCenter CV can also detect the presence of mobile code in transit across a network, and identify the systems involved in the transfer.
DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed	SecurityCenter CV can: • Passively monitor and actively scan for unauthorized network connections • Alert on unauthorized software configuration changes • Monitor for use of network resources by unauthorized or terminated personnel
DE.CM-8	Vulnerability scans are performed	Tenable was founded on the belief that it is crucial to audit and monitor systems in a manner as close to real-time as possible. The greater the gap between monitoring cycles, the more likely it is for vulnerabilities to be undetected. • Active vulnerability scans and audits can take just a few minutes. With SecurityCenter CV, multiple active scanners can be combined to perform load balanced network audits. • Credentialed 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. • SecurityCenter CV passively monitors all network traffic in real-time to find new hosts, new vulnerabilities, and new applications. It monitors the network for the same vulnerabilities detected by active scanning. In addition, SecurityCenter CV analyzes host data to passively detect and identify a variety of vulnerabilities.

DE.DP	Detection Processes	
DE.DP-3	Detection processes are tested	SecurityCenter CV can detect penetration tests and custom malware tests with the same level of accuracy as real malware and insider attack detection.
DE.DP-5	Detection processes are continuously improved	Host data analysis, configuration audits, vulnerability remediation, and many other types of controls can be monitored and analyzed by SecurityCenter CV, which allows for the continual improvement of an organization’s security and compliance processes.
RS	**Respond**	
RS.AN	**Analysis**	
RS.AN-1	Notifications from detection systems are investigated	SecurityCenter CV 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. SecurityCenter CV can also accept logs from Tripwire and correlate these events with suspicious activity and changes in file integrity.
RS.AN-3	Forensics are performed	Organizations that make use of SecurityCenter CV can quickly provide a global picture of system activity to those responding to an incident. SecurityCenter CV provides the ability to save all 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 evidence data.
RS.MI	**Mitigation**	
RS.MI-3	Newly identified vulnerabilities are mitigated or documented as accepted risks	Vulnerable devices and applications on an organization's network pose a great risk to the organization and could allow attackers to compromise the network. A robust vulnerability scanning and risk assessment process combined with a sound vulnerability management and remediation program can go far to protect an organization. SecurityCenter CV’s management of active vulnerability assessments and passive monitoring 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. Exploitable vulnerabilities that have been marked as accepted risks or recast to Informational within SecurityCenter CV can be noted.