



# CIS Controls Assessment Specification

---

Last Revised: July 18, 2025



## Table of Contents

|  |          |
|--|----------|
| <b>CIS Controls Assessment Specification</b>   | <b>6</b> |
| <b>Basic Controls</b>  | <b>9</b> |
| CIS Control 1: Inventory and Control of Hardware Assets  | 10       |
| 1.4: Maintain Detailed Asset Inventory   | 14       |
| 1.6: Address Unauthorized Assets   | 22       |
| CIS Control 2: Inventory and Control of Software Assets  | 26       |
| 2.1: Maintain Inventory of Authorized Software   | 30       |
| 2.2: Ensure Software is Supported by Vendor  | 32       |
| 2.6: Address Unapproved Software   | 37       |
| CIS Control 3: Continuous Vulnerability Management   | 40       |
| Preface on Sub-Controls 3.4 and 3.5  | 44       |
| 3.4: Deploy Automated Operating System Patch Management Tools  | 45       |
| 3.5: Deploy Automated Software Patch Management Tools  | 48       |
| CIS Control 4: Controlled Use of Administrative Privileges   | 50       |
| Preface on Sub-Controls 4.2 and 4.3  | 53       |
| 4.2: Change Default Passwords  | 57       |
| 4.3: Ensure the Use of Dedicated Administrative Accounts   | 60       |
| CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers | 62       |
| Preface on Sub-Control 5.1   | 65       |
| 5.1: Establish Secure Configurations   | 67       |
| CIS Control 6: Maintenance, Monitoring and Analysis of Audit Logs  | 69       |
| Preface on Sub-Control 6.2   | 70       |



|  |           |
|--|-----------|
| 6.2: Activate Audit Logging .....  | 71        |
| <b>Foundational Controls .....</b>   | <b>73</b> |
| CIS Control 7: Email and Web Browser Protections .....   | 74        |
| Preface on Sub-Controls 7.1 and 7.7 .....  | 76        |
| 7.1: Ensure Use of Only Fully Supported Browsers and Email Clients .....                                 | 78        |
| 7.7: Use of DNS Filtering Services .....   | 82        |
| CIS Control 8: Malware Defenses .....  | 84        |
| Preface on Sub-Controls 8.2, 8.4, and 8.5 .....  | 86        |
| 8.2: Ensure Anti-Malware Software and Signatures Are Updated .....                                       | 89        |
| 8.4: Configure Anti-Malware Scanning of Removable Media .....  | 92        |
| 8.5: Configure Devices to Not Auto-Run Content .....   | 94        |
| CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services .....                    | 96        |
| Preface on Sub-Control 9.4 .....   | 98        |
| 9.4: Apply Host-Based Firewalls or Port-Filtering .....  | 102       |
| CIS Control 10: Data Recovery Capabilities .....   | 104       |
| 10.1: Ensure Regular Automated Backups .....   | 107       |
| 10.2: Perform Complete System Backups .....  | 110       |
| 10.4: Protect Backups .....  | 112       |
| 10.5: Ensure All Backups Have at Least One Offline Backup Destination .....                              | 114       |
| CIS Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches ..... | 116       |
| Preface on Sub-Control 11.4 .....  | 119       |
| 11.4: Install the Latest Stable Version of Any Security-Related Updates on All Network Devices .....     | 120       |
| CIS Control 12: Boundary Defense .....   | 122       |



|  |            |
|--|------------|
| Preface on Sub-Controls 12.1 and 12.4 .....  | 125        |
| 12.1: Maintain an Inventory of Network Boundaries .....                              | 126        |
| 12.4: Deny Communication Over Unauthorized Ports .....                               | 128        |
| CIS Control 13: Data Protection .....  | 130        |
| Preface on Sub-Controls 13.1 and 13.2 .....  | 133        |
| Preface on Sub-Control 13.6 .....  | 136        |
| 13.1: Maintain an Inventory of Sensitive Information .....                           | 137        |
| 13.2: Remove Sensitive Data or Systems Not Regularly Accessed by Organization .....  | 139        |
| 13.6: Encrypt Mobile Device Data .....   | 141        |
| CIS Control 14: Controlled Access Based on the Need to Know .....                    | 143        |
| 14.6: Protect Information Through Access Control Lists .....                         | 145        |
| CIS Control 15: Wireless Access Control .....  | 147        |
| 15.7: Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data ..... | 149        |
| CIS Control 16: Account Monitoring and Control .....                                 | 151        |
| Preface on Sub-Controls 16.8, 16.9, and 16.11 .....                                  | 154        |
| 16.8: Disable Any Unassociated Accounts .....  | 158        |
| 16.9: Disable Dormant Accounts .....   | 160        |
| 16.11: Lock Workstation Sessions After Inactivity .....                              | 162        |
| <b>Organizational Controls .....</b>   | <b>164</b> |
| CIS Control 17: Implement a Security Awareness and Training Program .....            | 166        |
| CIS Control 18: Application Software Security .....                                  | 168        |
| CIS Control 19: Incident Response and Management .....                               | 169        |
| CIS Control 20: Penetration Tests and Red Team Exercises .....                       | 171        |
| <b>Tenable Security Center CAS Dashboard .....</b>                                   | <b>174</b> |





|  |            |
|--|------------|
| <b>Appendix .....</b>                            | <b>180</b> |
| Audit File Scan Tutorial .....                   | 181        |
| CIS CAS Audit Requirements .....                 | 182        |
| Create a New Repository + Scan Zone .....        | 183        |
| Create a New Audit File + Policy .....           | 185        |
| Create a Scan .....                              | 186        |
| Run Scan + See the Results .....                 | 188        |
| CAS Implementation Group 1 Audit Questions ..... | 189        |



---

## CIS Controls Assessment Specification

---

The Center for Internet Security (CIS) and Tenable partnered together to create a guide to help customers understand how to implement the CIS Controls. Starting with the SANS Top 20 Controls published several years ago, Tenable has continuously helped our customers leverage Tenable Security Center to understand their security posture using these controls. CIS Controls version 7.1 introduced the concept of Implementation Groups (IGs), which are self-assessed categories for organizations based on specific cybersecurity attributes. The security community has assessed the Controls and identified these 20 controls to be reasonable for an organization to implement. Other standards such as Cybersecurity Maturity Model Certification (CMMC) and Cyber Security Framework (CSF) also have a tiered approach to deployment. By grouping the controls into three categories, the implementation is easier to understand and integrate into security operations.

This guide is focused on Implementation Groups 1 (IG1); however, many of the controls have requirements for input that come from active or passive network scanning. As Tenable is a Cyber Exposure and Vulnerability Management company, any guidance provided will best serve the organization with Tenable Security Center Continuous View deployed using active and passive scanning. For controls that Tenable is not able to directly assist with, suggestions on how to use Tenable products will be provided to aid in the successful completion of the control.



## Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

## Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

## Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises



The 20 CIS Controls are broken down into three categories: Basic, Foundational, and Organizational. The [Basic Controls](#) (first six controls) are commonly referred to as the “cyber hygiene” controls. These controls focus on basic security guidelines; for example, Configuration Management, Vulnerability Assessment, and Continuous Monitoring. The next group, [Foundational Controls](#) (7 - 16), enable an organization to build a framework for a good security program. The last category, [Organizational Controls](#) (final four controls) provide more guidance with respect to people and process.

Tenable assists organizations in taking charge of their cybersecurity program with five steps to successful cybersecurity. These five steps are Discover, Assess, Analyze, Fix, and Measure. For IG1 organizations, these five steps align closely with efforts across the Basic and Foundational categories. With Cyber Hygiene being the focus of the first six controls, these actions align closely with the Discover step. Starting with controls 1 & 2, organizations begin to discover hardware and software assets. The remaining steps Assess, Analyze, Fix and Measure are seen throughout the remaining controls. Controls 3, 4, 5, 8, and 11 are all key aspects to Tenable’s core ability to help assess risk. For the other categories, Tenable can often aid in the understanding of configuration problems or situational context based on discovered vulnerabilities.

By combining Tenable's Five Steps To Cybersecurity Success and the CIS Controls into a unified process, an organization can more easily secure their network. Using the CIS Control Assessment Specification (CAS) as a detailed guide, the security team can easily align their efforts in vulnerability management to meet the CIS Control requirements. Using the inputs and measures found in the CAS, the security team can operationalize the controls and use Tenable Security Center as the source of truth for many controls, and for other controls the data within Tenable Security Center will add value.

This guide provides a section for each CIS Control, and sub-sections for each Sub-Control. Examples of queries and dashboard use cases are provided. The security team can follow the CAS and this guide for a more successful deployment of the CIS Controls.



---

## Basic Controls

---

- [CIS Control 1: Inventory and Control of Hardware Assets](#)
- [CIS Control 2: Inventory and Control of Software Assets](#)
- [CIS Control 3: Continuous Vulnerability Management](#)
- [CIS Control 4: Controlled Use of Administrative Privileges](#)
- [CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers](#)
- [CIS Control 6: Maintenance, Monitoring and Analysis of Audit Logs](#)



---

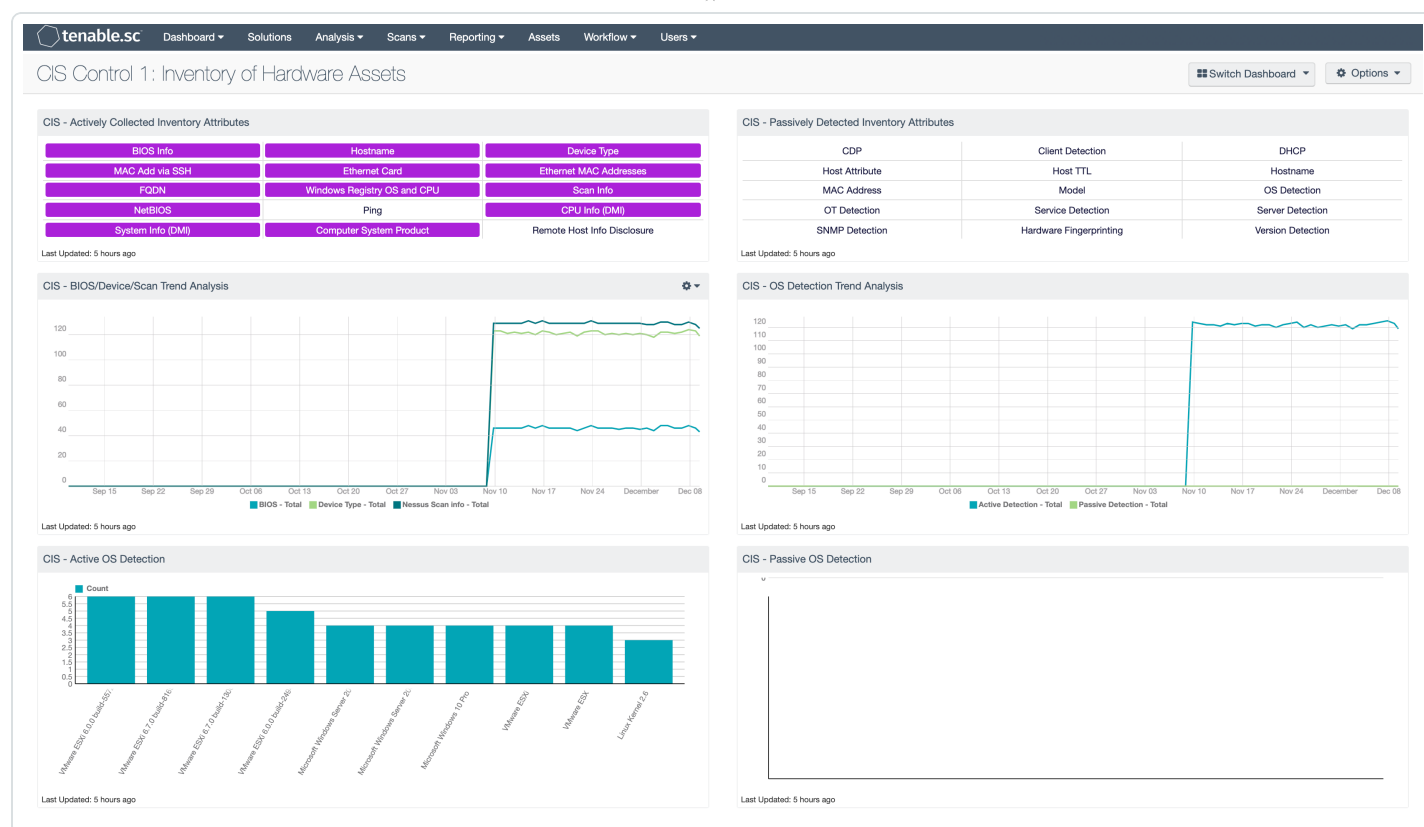
## CIS Control 1: Inventory and Control of Hardware Assets

---

Control 1 helps the CIS to actively manage (inventory, track, and correct) all hardware devices on the network. This ensures only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

*“Attackers, who can be located anywhere in the world, are continuously scanning the address space of target organizations, waiting for new and possibly unprotected systems to be attached to the network. They are particularly interested in devices which come and go off of the enterprise’s network such as laptops or Bring-Your-Own-Device (BYOD) which might be out of synchronization with security updates or might already be compromised. Attacks can take advantage of new hardware that is installed on the network one evening but not configured and patched with appropriate security updates until the following day. Even devices that are not visible from the Internet can be used by attackers who have already gained internal access and are hunting for internal pivot points or victims. Additional systems that connect to the enterprise’s network (e.g., demonstration systems, temporary test systems, guest networks) should also be managed carefully and/or isolated in order to prevent adversarial access from affecting the security of enterprise operations.”*

Any journey begins with single step, and the journey of implementing the CIS Controls begins with inventory of hardware assets. A hardware asset is any device that operates at the Datalink layer (Layer 2) or the Network layer (Layer 3). These devices, whether they are connected to the network or not, can store or provide access to sensitive data. Therefore, their risk must be identified. By discovering assets within the organization, the CISO can begin to establish an inventory and can then begin assessing and mitigating associated risks to the asset. To accomplish this, though, our first priority is to discover the assets. The CIS Control 1 Dashboard provides information to assist in identifying assets collected during a vulnerability scan.



For more information about the CIS Control 1 dashboard, see [CIS Control 1: Inventory of Hardware Assets](#).

The Discover step helps organizations identify and map every asset across any computing environment. In this phase, Tenable Security Center Continuous View allows the CISO to detect assets through active scanning, passive network analysis, and event log discovery. By utilizing these three methods of discovery, the CISO can build a more complete list of hardware assets and begin to understand a clearer picture of risk on the network.

The CAS provides guidance on how to assess the organization's progress in this journey. This guide illustrates how the CISO can effectively measure progress. Shown below are the CIS Control 1 IG levels and requirements.



## CIS Control 1: Inventory and Control of Hardware Assets

| Sub-Control | Asset Type | Security Function | Control Title   | Control Descriptions  | Implementation Groups |   |   |
|-------------|------------|-------------------|---|---|-----------------------|---|---|
|             |            |                   |   |   | 1                     | 2 | 3 |
| 1.1         | Devices    | Identify          | Utilize an Active Discovery Tool                            | Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.   |                       |   |   |
| 1.2         | Devices    | Identify          | Use a Passive Asset Discovery Tool                          | Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory.  |                       |   |   |
| 1.3         | Devices    | Identify          | Use DHCP Logging to Update Asset Inventory                  | Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory.  |                       |   |   |
| 1.4         | Devices    | Identify          | Maintain Detailed Asset Inventory                           | Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all assets, whether connected to the organization's network or not.   |                       |   |   |
| 1.5         | Devices    | Identify          | Maintain Asset Inventory Information                        | Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.                                     |                       |   |   |
| 1.6         | Devices    | Respond           | Address Unauthorized Assets                                 | Ensure that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner.  |                       |   |   |
| 1.7         | Devices    | Protect           | Deploy Port Level Access Control                            | Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network. |                       |   |   |
| 1.8         | Devices    | Protect           | Utilize Client Certificates to Authenticate Hardware Assets | Use client certificates to authenticate hardware assets connecting to the organization's trusted network.   |                       |   |   |

As shown above, the IG1 organization is required to implement Sub-Controls 1.4 - **Maintain Detailed Asset Inventory** and 1.6 - **Address Unauthorized Assets**. Some useful methods to collect data to meet these requirements include:

Active Scanning and passive Scanning, specifically:

- ICMP/TCP/SYN/ACK identification
- OS fingerprinting
- Passive scanning/listening for talkers
- Pulling data from switches and routers regarding connected devices





All devices that have an IP address (whether they are wired/wireless and/or physical/virtual) are to be included in the asset inventory.



## 1.4: Maintain Detailed Asset Inventory

Sub-control 1.4 states that an accurate and up-to-date inventory of all technology assets with the potential to store or process information must be maintained. This inventory shall include all assets, whether or not they are connected to the organization's network.

| Asset Type | Security Function | Implementation Groups |
|------------|-------------------|-----------------------|
| Devices    | Identify          | 1, 2, 3               |

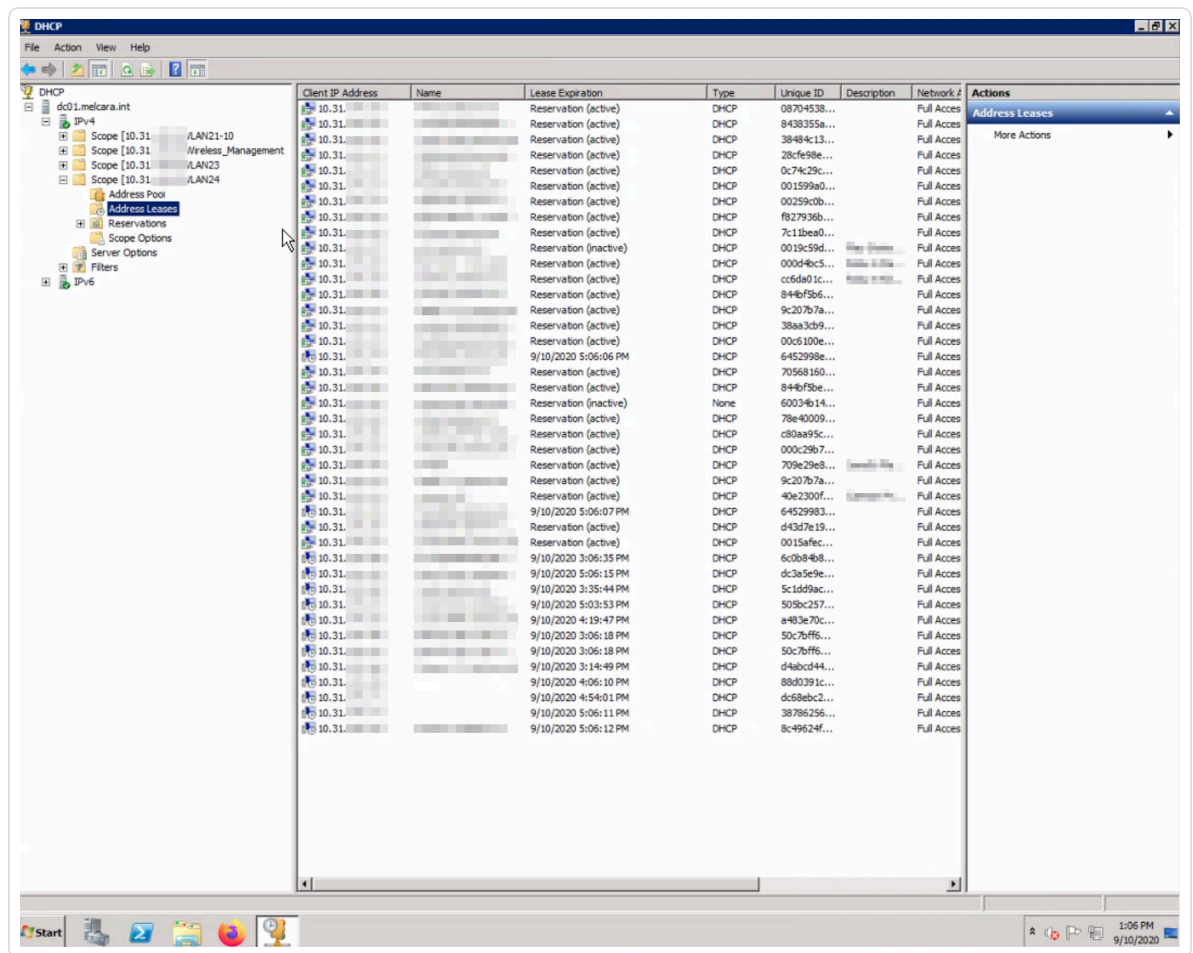
### Dependencies

- None

### Inputs

1. **Endpoint Inventory (I1):** The organization's current inventory list (aka the "to be checked" list).
  - a. This list is a static list of the number of assets the organization currently has or believes they have. For example, the organization should be aware of the number of laptops, desktops, servers, routers, switches, wireless Access Points, or other devices that are capable of obtaining an IP address. Use the count, or number of these devices for this input. The CISO is the resource who has a complete list of devices.
    - i. If the organization does not have a list of devices for this input, they can created a list of assets by utilizing DHCP logs, or other similar resources which track assets. In the example image below, a Windows DHCP Server's Address Leases are reviewed for assets on the network that are configured to receive a dynamic IP

address.



| Client IP Address | Name | Lease Expiration       | Type | Unique ID   | Description | Network Interface | Actions        |
|-------------------|------|------------------------|------|-------------|-------------|-------------------|----------------|
| 10.31.1.1         |      | Reservation (active)   | DHCP | 08704538... |             | Full Access       | Address Leases |
| 10.31.1.2         |      | Reservation (active)   | DHCP | 8438355a... |             | Full Access       | More Actions   |
| 10.31.1.3         |      | Reservation (active)   | DHCP | 38484c13... |             | Full Access       |                |
| 10.31.1.4         |      | Reservation (active)   | DHCP | 28cfe98e... |             | Full Access       |                |
| 10.31.1.5         |      | Reservation (active)   | DHCP | 0c74c29c... |             | Full Access       |                |
| 10.31.1.6         |      | Reservation (active)   | DHCP | 001599a0... |             | Full Access       |                |
| 10.31.1.7         |      | Reservation (active)   | DHCP | 00259c0b... |             | Full Access       |                |
| 10.31.1.8         |      | Reservation (active)   | DHCP | f827936b... |             | Full Access       |                |
| 10.31.1.9         |      | Reservation (active)   | DHCP | 7c11bea0... |             | Full Access       |                |
| 10.31.1.10        |      | Reservation (inactive) | DHCP | 0019c59d... |             | Full Access       |                |
| 10.31.1.11        |      | Reservation (active)   | DHCP | 000d4bc5... |             | Full Access       |                |
| 10.31.1.12        |      | Reservation (active)   | DHCP | cc6da01c... |             | Full Access       |                |
| 10.31.1.13        |      | Reservation (active)   | DHCP | 844bf5b6... |             | Full Access       |                |
| 10.31.1.14        |      | Reservation (active)   | DHCP | 9c207b7a... |             | Full Access       |                |
| 10.31.1.15        |      | Reservation (active)   | DHCP | 38aa3cd9... |             | Full Access       |                |
| 10.31.1.16        |      | Reservation (active)   | DHCP | 00c5100e... |             | Full Access       |                |
| 10.31.1.17        |      | 9/10/2020 5:06:06 PM   | DHCP | 6452998e... |             | Full Access       |                |
| 10.31.1.18        |      | Reservation (active)   | DHCP | 70568160... |             | Full Access       |                |
| 10.31.1.19        |      | Reservation (active)   | DHCP | 844bf5b6... |             | Full Access       |                |
| 10.31.1.20        |      | Reservation (inactive) | None | 60034b14... |             | Full Access       |                |
| 10.31.1.21        |      | Reservation (active)   | DHCP | 79e40009... |             | Full Access       |                |
| 10.31.1.22        |      | Reservation (active)   | DHCP | c80aa95c... |             | Full Access       |                |
| 10.31.1.23        |      | Reservation (active)   | DHCP | 000c29b7... |             | Full Access       |                |
| 10.31.1.24        |      | Reservation (active)   | DHCP | 709e29e8... |             | Full Access       |                |
| 10.31.1.25        |      | Reservation (active)   | DHCP | 9c207b7a... |             | Full Access       |                |
| 10.31.1.26        |      | Reservation (active)   | DHCP | 40e2300f... |             | Full Access       |                |
| 10.31.1.27        |      | 9/10/2020 5:06:07 PM   | DHCP | 64529983... |             | Full Access       |                |
| 10.31.1.28        |      | Reservation (active)   | DHCP | d43d7e19... |             | Full Access       |                |
| 10.31.1.29        |      | Reservation (active)   | DHCP | 0015afee... |             | Full Access       |                |
| 10.31.1.30        |      | 9/10/2020 3:06:35 PM   | DHCP | 6c0b84b0... |             | Full Access       |                |
| 10.31.1.31        |      | 9/10/2020 5:06:15 PM   | DHCP | dc3a5e9e... |             | Full Access       |                |
| 10.31.1.32        |      | 9/10/2020 3:35:44 PM   | DHCP | 5c1d99ac... |             | Full Access       |                |
| 10.31.1.33        |      | 9/10/2020 5:03:53 PM   | DHCP | 508bc257... |             | Full Access       |                |
| 10.31.1.34        |      | 9/10/2020 4:19:47 PM   | DHCP | a483e70c... |             | Full Access       |                |
| 10.31.1.35        |      | 9/10/2020 3:06:18 PM   | DHCP | 50c7bffe... |             | Full Access       |                |
| 10.31.1.36        |      | 9/10/2020 3:06:18 PM   | DHCP | 50c7bffe... |             | Full Access       |                |
| 10.31.1.37        |      | 9/10/2020 3:14:49 PM   | DHCP | d4abed44... |             | Full Access       |                |
| 10.31.1.38        |      | 9/10/2020 4:06:10 PM   | DHCP | 88d0391c... |             | Full Access       |                |
| 10.31.1.39        |      | 9/10/2020 4:54:01 PM   | DHCP | dc58ebc2... |             | Full Access       |                |
| 10.31.1.40        |      | 9/10/2020 5:06:11 PM   | DHCP | 38786256... |             | Full Access       |                |
| 10.31.1.41        |      | 9/10/2020 5:06:12 PM   | DHCP | 8c49624f... |             | Full Access       |                |

2. **"Ground Truth" Inventory (I2):** A list to compare with input 1 (I1). This list is enhanced by manual verification. However, a tool-generated or aggregated list can also be substituted. This list should be an aggregation of the devices detected over a period of time, but preferably not from a single scan. Scans should be conducted frequently. For example, a scan using plugin 10180 has very little effect on network performance, and can be conducted daily.
  - a. Tenable Security Center uses Nessus as the active discovery tool, and stores the collected data in a cumulative database. The database is considered cumulative because all data collected on the assets using active, passive, and event scanning methods are stored in a single repository for analysis.
3. **Procedural Write-up for Adding or Removing Assets to or from the Inventory:** an input only for manual review. This is a required physical document detailing the procedure for adding or removing assets in the inventory.

Assumptions



- Devices belonging to the organization, but not connected to the organization's network, require manual discovery in order to be included in the "Ground Truth" inventory.
- Audit File: Questions regarding connected devices.

## Operations

- If I1 is not provided, this sub-control is measured at a 0 (complete fail).
- If I2 is not provided, no true accuracy measurement can be made for this sub-control. However, I2 can be obtained from the CIS Sub-Control 1 on the CAS Control 1 (IG1) Dashboard available within Tenable Security Center. The Tenable Security Center component provides a summary of devices found on the network, as identified by Nessus. The following screenshots show the captured plugin output and the filters used within the component to capture the required data.

### Data

Data Type

Vulnerability

Type

Count

Source\*

Cumulative

#### Filters

|                    |             |
|--------------------|-------------|
| Plugin ID          | = 10180     |
| Vulnerability Text | Contains up |

+ Add Filter

### Rules

|         |         |                    |
|---------|---------|--------------------|
| Default | Display | Query Value: Hosts |
|---------|---------|--------------------|

+ Add Rule

Submit

Cancel



## Plugin Output

```
The remote host is up
The remote host replied to an ICMP echo packet
```

### CIS Sub-Control 1

|                 | Ground Truth (Active) | Dead (Inactive) |
|-----------------|-----------------------|-----------------|
| Sub-Control 1.4 | 3476                  | N/A             |
| Sub-Control 1.6 | N/A                   | 49252           |

Last Updated: Less than a minute ago

- An inverse search with this filter can be used to identify devices that are considered dead. The previous filter reports only on hosts that are alive and responsive. Altering the vulnerability text to "dead" displays a count of unresponsive devices.

## Plugin Output

```
The remote host (129.244.104.131) is considered as dead - not scanning
The remote host ('129.244.104.131') is on the local network and failed to reply
to an ARP who-is query.
```



### Data

Data Type

Vulnerability ▾

Type

Count ▾

Source\*

Cumulative ▾

Filters

Plugin ID

= 10180

Vulnerability Text

Contains dead

+ Add Filter

### Rules

Default

Display

Query Value: Hosts

+ Add Rule

Submit

Cancel

- Drill down into this component to view additional information on each scanned device. Often times, this can provide information about the type of device associated with the IPv4 address. This could include MAC Address and NetBIOS Information.
- This, or any data contained within a component can be easily exported to a spreadsheet for further analysis and processing:

- a. Click on the blue arrow in the top right corner of the component.
- b. On the Vulnerability Analysis page, click **Options**.
- c. Choose the method by which you want to export the data.

Optionally, you can also send the entire dashboard to a report:

- a. On the Dashboards page, click **Options**.
  - b. Select **Send to Report**.
- Calculate the intersection of I1 and I2. You can then see items that appear in one inventory but not the other.



Many of the tasks associated with this control are manual. However, active and passive discovery tools are available to assist you. In addition, using active and passive discovery tools to detect and inventory assets can help organizations meet the other Sub-Control CAS IG2 and IG3 requirements for Control 1. Tenable Security Center allows organizations at all IG's to collect unique information about each asset scanned via an active scanning tool. Using Nessus, Tenable Security Center initially port scans each asset and collects any open ports grabbing service banners where applicable. Next, when scanned with credentials, Nessus logs in to the system and collects a multitude of system configuration data. While Tenable Security Center is known for vulnerability data collected, it also collects a wide range of asset identification attributes such as MAC address, and CPU GUIDs. CIS Control 1 (Inventory of Hardware Assets Dashboard) contains actively collected attributes for further analysis by the operations teams. For more information, see <https://www.tenable.com/sc-dashboards/cis-control-1-inventory-of-hardware-assets>.

Tenable Security Center Continuous View includes Tenable Network Monitor. Using Tenable Network Monitor, Tenable Security Center can discover assets on the network using a Switch Port Analyzer (SPAN) port. SPAN ports are also commonly referred to as Mirrored ports. These ports provide copies of traffic to a Network Interface Card (NIC) for analysis.

Tenable Network Monitor is a network discovery and vulnerability analysis software solution that delivers continuous network listening, profiling, and monitoring in a non-intrusive manner. Tenable Network Monitor monitors network traffic at the packet layer to determine topology, services, and vulnerabilities. It is tightly integrated with Tenable Security Center and Log Correlation Engine (LCE) to centralize both event analysis and vulnerability management for a complete view of your security and compliance posture.

## Measures

| Measure   | Definition   |
|---|--|
| M1 = List of items in the intersection of Input 1 and Input 2. M1 is derived from the <b>Operations</b> section of this document. | A list of items that are either: in I2 but not in I1, or items that are in I1 but not in I2. The creation of this list is a manual task that requires reviewing all the assets from each of those lists. |
| M2 = Count of items in M1   | A count of the total number of items identified in M1.   |



|  |   |
|--|---|
| M3 = List of items in Input 2          | A list of found items that are unknown to the organization. This list contains items that have been scanned that are considered unknown/rogue to the organization. This measure is aided by Tenable Security Center Continuous View using Nessus. |
| M4 = Count of items in M3              | A count of the total number of items in M3.   |
| M5 = List of items in I1 and not in I2 | A list of devices that the organization believes they have, but that have not been found on the network.  |
| M6 = Count of items in M5              | A count of the total number of items in M5.   |
| M7 = List of items in I2 and not in I1 | A list of items that were identified from scanning but that are unknown to the organization.  |
| M8 = Count of items in M7              | A count of the total number of items in M7.   |

## Metrics

### Accuracy Score

| Metric  | Calculation  |
|---|--|
| The percentage of the "Ground Truth" inventory that is accounted for in the organization's current asset inventory. | $M2 / M4$<br><br>M2 is a count of the items from the intersection of I1 and I2.<br><br>M4 is the count of the items that have been identified. |

### Procedure Review

After the accuracy score is calculated, there must be a manual review/rating of the inventory procedures. This includes adding and removing assets and the time allowable or expected for the acquisition or disposal of assets.





Reconcile I1 with any new devices that have been identified that should be part of the asset inventory. In many cases, devices can be added to an organization over time and not be properly accounted for. Once the list of assets is updated to reflect an accurate count, this input can be used as a definitive resource in other Sub-Controls.



## 1.6: Address Unauthorized Assets

Sub-control 1.6 states that you must ensure unauthorized assets are either removed from the network, quarantined, or the inventory is updated in a timely manner.

| Asset Type | Security Function | Implementation Groups |
|------------|-------------------|-----------------------|
| Devices    | Respond           | 1, 2, 3               |

### Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory

### Inputs

1. **Unauthorized Assets:** A list of discovered assets not currently present in the asset inventory. This can be pulled from sub-control 1.4, Measure M3. This is a list of any found asset that was not previously known to the organization. The information from M3 must be brought into this sub-control as Input 1.
2. **Endpoint Inventory:** The current hardware inventory. This can be pulled from I2 sub-control 1.4, Inventory I1. This is a complete and accurate inventory of all the devices within the organization.
3. **Definition of "Timely":** An organizationally defined time frame for the term "timely". The CIS recommends a turnaround of 24 hours or less.
4. **(Optional) Disposition of Items:** Measurement results are more useful if the status (removed, added to inventory, quarantined, etc.) is provided and verified. This is not, however, required. Verification can be easily achieved with continued use of active and passive scanning techniques which determine if a device is still on the network. Assets/devices that are removed from the network can be validated as removed by a subsequent scan at a specified time period.

### Operations

If the optional disposition list is provided, the checks would be tailored to those dispositions. For the following, assume no disposition list is available:



1. At the time frame specified by I3, for each unauthorized asset (I1), check to see if the asset is present in the updated asset inventory (I2). This can be easily achieved by conducting follow-up scans to determine if devices are still present, or re-appear on the network.
2. For those I1 items that are not in I2, scan the network to determine if the item is still reachable on the network.

## Assumptions

If the item is not reachable, it may be reasonable to assume it has been removed from the network.

## Measures

| Measure                                 | Definition   |
|---|--|
| M1 = List of items not in the inventory | M1 can be copied from sub-control 1.4, Measure M7. A list of items that were identified from scanning but that are unknown to the organization. This is also the number of items from Input 1 NOT passing either Operation 1 or Operation 2.   |
| M2 = Count of items in M1               | A count of the total number of items in M1. This can also be copied from sub-control 1.4, Measure M8.  |
| M3 = List of items not reachable        | <p>A list of items that are considered unreachable. This can be curated by using a Tenable Security Center component that displays a list of assets/devices by Class C address space that are unreachable. The component works by utilizing the output of plugin 10180 to ping the remote host. The plugin output of "is considered dead" uses a timeframe of the last 7 days to determine which assets/devices have been removed from the network over the last 7 days. This timeframe can be changed to what the organization deems appropriate. This component accepts custom values. .</p> <p>This measure is aided by Tenable Security Center Continuous View using Nessus. The following screenshots show the captured plugin output and the filters used within the component to capture the required data.</p> |



|   |   |
|---|---|
|   | <div><p><b>Plugin Output</b></p><pre>The remote host (129.244.104.131) is considered as dead - not scanning The remote host ('129.244.104.131') is on the local network and failed to reply to an ARP who-is query.</pre></div> <div><p>Data</p><p>Data Type: Vulnerability</p><p>Type: Count</p><p>Source: Cumulative</p><p>Filters</p><p>Plugin ID: = 10180</p><p>Vulnerability Text: Contains dead</p><p>+ Add Filter</p><p>Rules</p><p>Default: Display Query Value: Hosts</p><p>+ Add Rule</p><p>Submit Cancel</p></div> |
| M4 = Count of items in M3                                       | A count of the total number of items in M3. You can manually add the count, or use the "Ground Truth" component to determine if the number of assets and devices has increased or decreased.  |
| M5 = List of items not in the inventory or that are unreachable | A list of items that are considered missing from the inventory or that are unreachable. The inventory must first be reconciled, at which point you can determine which items are rogue and should be removed.   |
| M6 = Count of items in M5                                       | A count of the total number of items in M5.   |
| M7 = List of items in the inventory                             | A list of items that are in the current inventory. This can be derived from sub-control 1.4, Input 1.   |
| M8 = Count of items in M7                                       | A count of the total number of items in M7.   |

## Metrics

### Unauthorized Asset Remediation



| Metric  | Calculation  |
|---|--|
| The ratio of unaccounted for, unauthorized assets as compared to the total number of assets in the asset inventory. | <p>If the value of M6 is 0, there are no unauthorized assets that remain unaccounted for.</p> <p>In this case, the value of the metric is 1. Otherwise, the value is:</p> $(M8 - M6) / M8$ |



## CIS Control 2: Inventory and Control of Software Assets

The focus of this control is to actively manage (inventory, track, and correct) software installed on systems within the organization. A fundamental aspect of risk management is discovering risk by tracking software present on information systems. Ensuring only authorized software is used by the organization will increase the effectiveness of risk management efforts. Being able to quickly identify unauthorized and unmanaged software can prevent security breaches and increase the productivity of users.

The CIS states this control is critical:

*“Attackers continuously scan target organizations looking for vulnerable versions of software that can be remotely exploited. Some attackers also distribute hostile web pages, document files, media files, and other content via their own web pages or otherwise trustworthy third-party sites. When unsuspecting victims access this content with a vulnerable browser or other client-side program, attackers compromise their machines, often installing backdoor programs and bots that give the attacker long-term control of the system. Some sophisticated attackers may use zero-day exploits, which take advantage of previously unknown vulnerabilities for which no patch has yet been released by the software vendor. Without proper knowledge or control of the software deployed in an organization, defenders cannot properly secure their assets.*

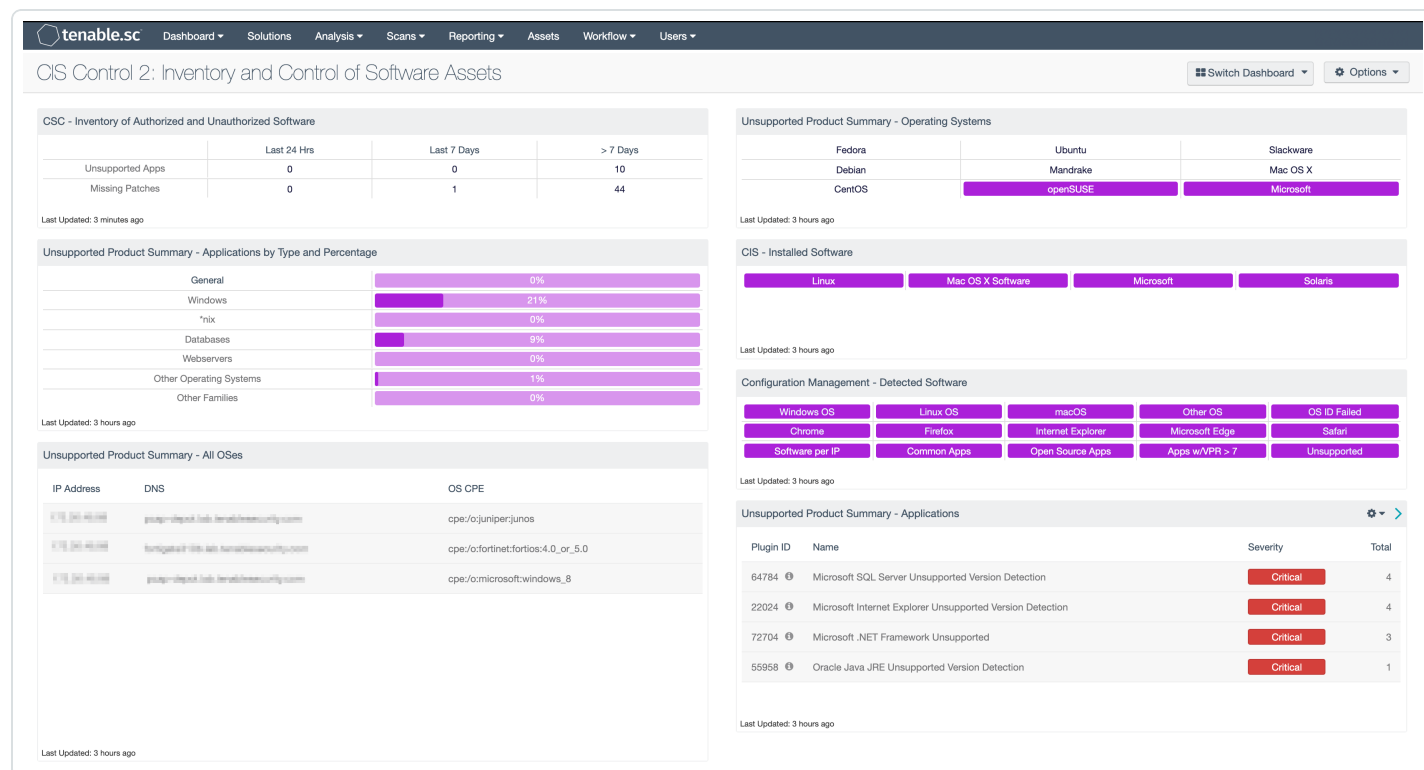
*Poorly controlled machines are more likely to be either running software that is unneeded for business purposes (introducing potential security flaws), or running malware introduced by an attacker after a system is compromised. Once a single machine has been exploited, attackers often use the compromised system as a staging point for collecting sensitive information from the compromised system and from other accessible systems connected to it. In addition, compromised machines are used as a launching point for movement throughout the network and partnering networks. In this way, attackers may quickly turn one compromised machine into many. Organizations that do not have complete software inventories are unable to find systems running vulnerable or malicious software to mitigate problems or root out attackers.*

*Managed control of all software also plays a critical role in planning and executing system backup, incident response, and recovery.”*

The journey of implementing the CIS Controls continues with inventory of software assets. Software assets are any application or program used by the organization, including operating systems. By



discovering software assets, the CIS0 can begin to establish an inventory and can then begin assessing and mitigating the associated risks. Tenable Security Center allows the CIS0 to use active and passive methods to collect the software inventories. The CIS Control 2 Dashboard provides information to assist in identifying unwanted or potentially dangerous applications, therefore enabling an efficient vulnerability management program.



For more information about the CIS Control 2 dashboard, see [CIS Control 2: Inventory and Control of Software Assets](#).

In the discovery phase Tenable Security Center Continuous View provides the CIS0 with the ability to detect assets through active scanning and passive network analysis. Utilizing these methods, the CIS0 is already transitioning from the IG1 to IG2, and is building a more complete list of software assets, and is able to better understand the current risk in the network. The CAS provides guidance on how to assess the organization's progress in this journey. Shown below is the CIS Control 1 IG levels and requirements.



## CIS Control 2: Inventory and Control of Software Assets

| Sub-Control | Asset Type   | Security Function | Control Title  | Control Descriptions  | Implementation Groups |   |   |
|-------------|--------------|-------------------|--|---|-----------------------|---|---|
|             |              |                   |  |   | 1                     | 2 | 3 |
| 2.1         | Applications | Identify          | Maintain Inventory of Authorized Software                | Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.  |                       |   |   |
| 2.2         | Applications | Identify          | Ensure Software Is Supported by Vendor                   | Ensure that only software applications or operating systems currently supported and receiving vendor updates are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system. |                       |   |   |
| 2.3         | Applications | Identify          | Utilize Software Inventory Tools                         | Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems.   |                       |   |   |
| 2.4         | Applications | Identify          | Track Software Inventory Information                     | The software inventory system should track the name, version, publisher, and install date for all software, including operating systems authorized by the organization.   |                       |   |   |
| 2.5         | Applications | Identify          | Integrate Software and Hardware Asset Inventories        | The software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.   |                       |   |   |
| 2.6         | Applications | Respond           | Address Unapproved Software                              | Ensure that unauthorized software is either removed or the inventory is updated in a timely manner.   |                       |   |   |
| 2.7         | Applications | Protect           | Utilize Application Whitelisting                         | Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.   |                       |   |   |
| 2.8         | Applications | Protect           | Implement Application Whitelisting of Libraries          | The organization's application whitelisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc.) are allowed to load into a system process.  |                       |   |   |
| 2.9         | Applications | Protect           | Implement Application Whitelisting of Scripts            | The organization's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.ps1, *.py, macros, etc.) are allowed to run on a system.   |                       |   |   |
| 2.10        | Applications | Protect           | Physically or Logically Segregate High Risk Applications | Physically or logically segregated systems should be used to isolate and run software that is required for business operations but incurs higher risk for the organization.   |                       |   |   |

As shown above, the IG1 organization is required to implement Sub-Controls 2.1 - **Maintain Inventory of Authorized Software**, 2.2 - **Ensure Software is Supported by Vendor**, and 2.6 - **Address Unapproved Software**. Some useful methods to collect data to meet these requirements include:

Active Scanning and passive Scanning, specifically:





- Identify installed/detected software/applications
- Identify software/applications that are installed on hosts
- Identify patching/version information on detected software/applications



## 2.1: Maintain Inventory of Authorized Software

Sub-control 2.1 states that an up-to-date list of all authorized software required in the enterprise for any business purpose on any business system must be maintained.

| Asset Type   | Security Function | Implementation Groups |
|--------------|-------------------|-----------------------|
| Applications | Identify          | 1, 2, 3               |

### Dependencies

- None

### Inputs

1. **Authorized Software List:** The authorized software list that contains a timestamp indicating both the last updated and last verified values. The organization should have a list of all approved applications. Reviewers should identify organizational artifacts such as a “Gold” image that is used to provision servers and/or desktops/laptops, purchase orders, and license agreements to create a master list of approved software.
2. **Definition of “Up-to-Date”:** An organizationally defined time frame for the term “up-to-date”. This time frame includes remediating issues, such as removing unapproved software or patching unsupported/out-of-date software. The CIS recommends this be at least monthly.

### Operations

1. Test for the presence of the list. This is a TRUE/FALSE value (M1).
2. (Optional) If specific attributes of the software are deemed required, test for those (vendor, product name, version, business case, etc.)
  - a. We highly recommended that software versions be checked when evaluating installed software. Reviewing software versions information ensures all software components are patched and up to date. Patching remains a critical concern for organizations to protect themselves.



3. Compare the timestamp of I1 against the current date to determine if the most recent update/verification is within the timeframe specified by I2. This is a TRUE/FALSE value (M2).

## Measures

- M1:
  - TRUE if the authorized software list is present and in the proper format.
  - FALSE if the authorized software list is not present or is in the incorrect format.
- M2:
  - TRUE if the most recent update/verification is within the “up-to-date” threshold
  - FALSE if the most recent update/verification is not within the “up-to-date” threshold

## Metrics

### Update Quality

| Metric  | Calculation |
|---|-------------|
| Is the authorized software list present and up-to-date? | M1 AND M2   |



## 2.2: Ensure Software is Supported by Vendor

Sub-control 2.2 states that you must ensure that only software applications or operating systems currently supported and receiving vendor updates are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.

| Asset Type   | Security Function | Implementation Groups |
|--------------|-------------------|-----------------------|
| Applications | Identify          | 1, 2, 3               |

### Dependencies

- Sub-control 2.1: Maintain Inventory of Authorized Software

### Inputs

1. **Authorized Software List:** An authorized software list with a notation of "supported" or "unsupported" for each entry (sub-control 2.1). This can be pulled from sub-control 2.1, I1, however, each piece of software must then be marked as "supported" or "unsupported".
2. **Authoritative Source of Information:** Access to an authoritative source of information indicating supported/unsupported details per product.
  - a. There are many active and passive scanning options for the identification of applications and identification of unsupported applications. For example, selected Plugin Families along with a Vulnerability Text of 'unsupported' can be used to identify detected unsupported applications and operating systems.



**Filters**

Plugin Family

= ▼

Q

☒ X

Search

☒ Select All

☒ CentOS Local Security Checks

☒ Cloud Services [Passive]

☒ Data Leakage [Passive]

☒ AIX Local Security Checks

☒ Amazon Linux Local Security Checks

☒ CGI [Passive]

☒ CGI abuses

Plugin Name

Contains unsupported

- b. There are also hundreds of plugins available that provide detailed information on unsupported applications. For example, plugin 33850 Unix Operating System Unsupported Version Detection returns the following plugin output when triggered:

**Plugin Output**

```
AIX 6.1 support ended on 2017-04-30.  
Upgrade to AIX 7.1 / 7.2.  
  
For more information, see : http://www-01.ibm.com/software/support/aix/lifecycle/index.html
```

- c. Common Platform Enumeration (CPE) Strings can also be used, and are a common method for the identification of specific applications. For example, if Apache Tomcat is an authorized application, you can use the CPE string to retrieve information for that specific application. As shown below, Apache Tomcat is displayed in the fourth row of CPE strings.



## Plugin Output

```
The remote operating system matched the following CPE :  
  
cpe:/o:microsoft:windows_server_2008:r2:sp1:x64-datacenter  
  
Following application CPE's matched on the remote system :  
  
cpe:/a:7-zip:7-zip:9.20.0.0  
cpe:/a:adobe:flash_player:32.0.0.387  
cpe:/a:apache:http_server:  
cpe:/a:apache:tomcat:  
cpe:/a:google:chrome:83.0.4103.106  
cpe:/a:microsoft:.net_framework:2.0.50727  
cpe:/a:microsoft:.net_framework:3.0 -> Microsoft .NET Framework 3.0  
cpe:/a:microsoft:.net_framework:3.5 -> Microsoft .net Framework 3.5  
cpe:/a:microsoft:.net_framework:4.7.1  
cpe:/a:microsoft:ie:11.0.9600.18860  
cpe:/a:microsoft:remote_desktop_connection:6.3.9600.16415  
cpe:/a:microsoft:silverlight:5.1.50907.0  
cpe:/a:microsoft:sql_server:10.50.6220.0  
cpe:/a:microsoft:sql_server:2008:sp3  
cpe:/a:oracle:jre:1.8.0:update144  
cpe:/a:oracle:jre:1.8.0_144  
cpe:/a:vmware:vcenter_converter:5.1.0  
cpe:/a:vmware:vcenter_orchestrator:5.5.3  
cpe:/a:vmware:vcenter_server:vmware_vcenter_5.5  
cpe:/a:vmware:vmware_tools:10.0.0.50046  
cpe:/a:vmware:vsphere_client:  
x-cpe:/a:microsoft:laps:6.2.0.0
```

d. Nessus displays installed software during Authenticated Scans if the following plugins are enabled:

- For Linux: **Nessus Plugin ID 22869** Software Enumeration (SSH)
- For Windows: **Nessus Plugin ID 20811** Microsoft Windows Installed Software Enumeration (credentialed check)
- For MacOS: **Nessus Plugin ID 83991** List Installed Mac OS X Software

## Operations



1. For each entry in I1, perform a lookup in I2 to verify:
  - a. Using the organizations list of known approved software I1, compare the list of software that has been found to exist within the organization I2 using active and passive detection and the methods outlined above for each of the following operations.
2. For each entry in I1 labeled “supported”, perform a lookup in I2.
  - a. From these lookups, note the list of authorized software labeled “supported” but that is actually not supported based on the authoritative source lookup.
3. For each entry in I1 labeled “unsupported”, perform a lookup in I2.
  - a. From these lookups, note the list of authorized software labeled “unsupported” but that is actually supported based on the authoritative source lookup.

## Measures

| Measure   | Definition  |
|---|---|
| M1 = List of items in the authorized software list that are unsupported               | A combination of Operation 1 and those initially marked as unsupported in I1, resulting in a complete list of unsupported applications. |
| M2 = Count of items in M1   | A count of the total number of items in M1.   |
| M3 = List of authorized software  | A full list of the applications the organization is authorized to have.   |
| M4 = Count of items in M3   | A count of the total number of items in M3.   |
| M5 = List of items in the authorized software list that are mislabeled as supported   | A list of applications that the organization believes to be supported, but are actually found to be unsupported.                        |
| M6 = Count of items in M5   | A count of the total number of items in M5.   |
| M7 = List of items in the authorized software list that are mislabeled as unsupported | A list of applications that are believed to be unsupported but that are actually supported.   |
| M8 = Count of items in M7   | A count of the total number of items in M7.   |



## Metrics

### Percentage of Unsupported Software in Use

| Metric   | Calculation      |
|--|------------------|
| The percentage of authorized software in use is that is unsupported. | $(M4 - M2) / M4$ |

### Rate of False Positives

| Metric   | Calculation      |
|--|------------------|
| The percentage of software listed as supported that is actually unsupported. | $(M4 - M5) / M4$ |

### Percentage of Unsupported Software in Use

| Metric   | Calculation      |
|--|------------------|
| The percentage of software listed as unsupported that is actually supported. | $(M4 - M8) / M4$ |





## 2.6: Address Unapproved Software

Sub-control 2.6 states that you must ensure that unauthorized software is either removed or the inventory is updated in a timely manner.

| Asset Type   | Security Function | Implementation Groups |
|--------------|-------------------|-----------------------|
| Applications | Respond           | 1, 2, 3               |

### Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 2.1: Maintain Inventory of Authorized Software

### Inputs

1. **Authorized Software List:** The previous list of authorized software (sub-control 2.1, I1).
2. **Definition of "Resolved":** An organizationally defined allowable time frame for the resolution of discovered unauthorized software. The CIS recommends this occur at least monthly.
3. **Software-Capable Endpoints:** The list of endpoints to be checked (sub-control 1.4). This should include all the organizations devices.
4. **Authorized Software List:** The updated authorized software list, following the time frame defined in I2.
5. **"Scanning Threshold":** The time period between scan 1 and scan 2.

### Assumptions

- For I4, the authorized software list may have been updated after a manual review of unauthorized software based on user requests, etc.
- For I5, the scanning threshold time period is greater than the resolution time frame defined in I2.

### Operations



1. For each endpoint in I3, scan the installed software present on that endpoint.
  - a. Perform an active credentialed scan against each device on the network. There are two plugins when conducting credentialed scans that enumerate installed software on the host.
    - i. For Linux: **Nessus Plugin ID 22869** Software Enumeration (SSH)
    - ii. For Windows: **Nessus Plugin ID 20811** Microsoft Windows Installed Software Enumeration (credentialed check)
2. Compare the installed software list for each endpoint (M1) to the authorized software list (I1) to generate the unauthorized software list for that endpoint (M2). This list is the software that is found/identified on any host that the organization does not have a license to use, or policy prohibits its installation. For example, the application and protocol analyzer Wireshark may be considered free to use, but organization policy may not authorize its installation.
3. Wait the defined “scanning threshold” period (I5) and re-scan the endpoints specified by I3.
4. For each piece of software listed in M2, determine if scan from Operation 3 still shows that software as present.
5. For those that are still present, check I4 to determine if the software is now present on the updated authorized software list. Software that remains installed on the machine, but that does not appear on the updated authorized software list, is added to the unaddressed software list for that endpoint (M3).

## Measures

| Measure  | Definition   |
|--|--|
| M1 = Installed software on a given endpoint  | A list of all installed software/applications. This is derived from the scan defined in Operation 1.   |
| M2 = Unauthorized software installed on a given endpoint.                              | A list of unauthorized software/applications. This is derived from comparing M1 to I1.   |
| M3 = Unaddressed software installed on a given endpoint, identified by follow-up scan. | A list of any unauthorized software/applications still present on the endpoint after a follow-up scan (Operation 3) at a specified interval. |



|                           |   |
|---------------------------|---|
| M4 = Count of items in M2 | A count of the total number of items in M2. |
| M5 = Count of items in M3 | A count of the total number of items in M3. |

## Metrics

### Unauthorized Software (Per Endpoint)

| Metric  | Calculation      |
|---|------------------|
| Ensure unauthorized software installations are addressed. | $(M4 - M5) / M4$ |

### Unauthorized Software (Organizational)

The organizational metric is calculated by averaging the results of the **Per Endpoint** metric above.



---

## CIS Control 3: Continuous Vulnerability Management

---

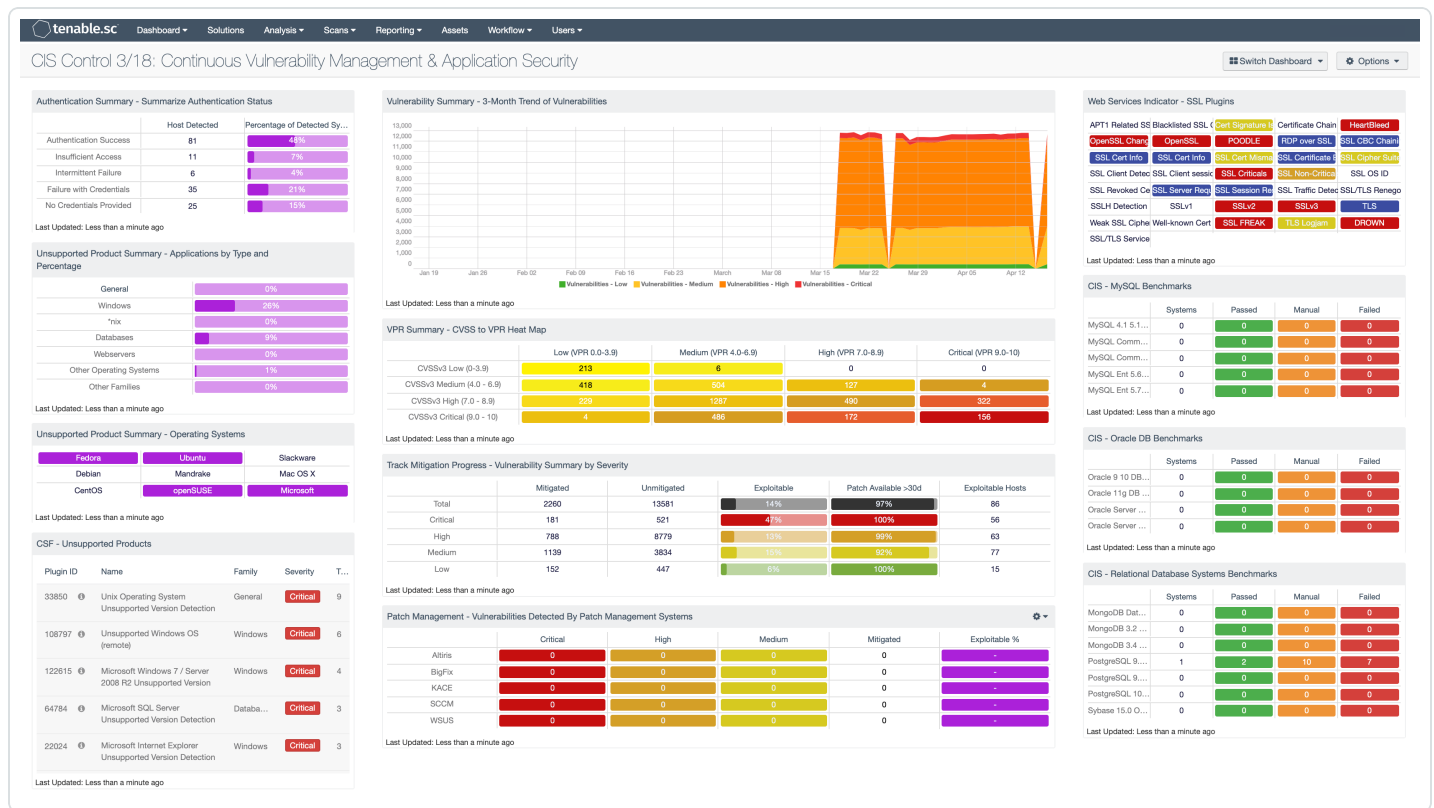
The focus of this control is to have an established vulnerability management program that is configured to conduct regular, comprehensive, credentialed scans across the organization. The most effective vulnerability scanning programs not only identify vulnerabilities, but also evaluate and report on a number of other critical concerns such as:

- Security configurations of systems
- Misconfigurations
- Unauthorized changes
- Patch levels of systems

Vulnerability assessment tools should follow industry recognized vulnerability, configuration, and platform classification schemes such as:

- Vulnerability Priority Rating (VPR)
- Common Vulnerabilities and Exposures (CVE)
- Common Configuration Enumeration (CCE)
- Open Vulnerability and Assessment Language (OVAL)
- Common Platform Enumeration (CPE)
- Common Vulnerability Scoring System (CVSS)
- Extensible Configuration Checklist Description Format (XCCDF)

In addition, identified concerns should be reconciled/mitigated in a timely manner, using follow up vulnerability scanning as validation. For CIS Control 3, Tenable products allow organizations to effectively address, report, and follow up on these industry standards via active, credentialed scanning, across all three Implementation Groups. A number of dashboards, reports, and Assurance Report Cards (ARC) are readily available to provide organizations with real time continuous vulnerability monitoring and reporting, such as the CIS Control 3/18 Continuous Vulnerability Management and Application Security Dashboard.



For more information about the CIS Control 3 dashboard, see [CIS Control 3/18: Continuous Vulnerability Management & Application Security](#).

The CIS states this Control is critical:

*“Cyber defenders must operate in a constant stream of new information: software updates, patches, security advisories, threat bulletins, etc. Understanding and managing vulnerabilities has become a continuous activity, requiring significant time, attention, and resources. Attackers have access to the same information and can take advantage of gaps between the appearance of new knowledge and remediation. For example, when researchers report new vulnerabilities, a race starts among all parties, including: attackers (to “weaponize,” deploy an attack, exploit), vendors (to develop, deploy patches or signatures and updates), and defenders (to assess risk, regression-test patches, install).*

*Organizations that do not scan for vulnerabilities and proactively address discovered flaws face a significant likelihood of having their computer systems compromised. Defenders face particular challenges in scaling remediation across an entire enterprise, and prioritizing actions with conflicting priorities, and sometimes uncertain side effects.”*



The journey of implementing the CIS Controls continues with continuous vulnerability management. Credentialed Active Scanning and monitoring with products such as Nessus, Tenable Vulnerability Management, and Tenable Security Center allows organizations to continuously acquire, assess, and take action on new vulnerability information in order to identify and remediate risks. Thereby, the organizations can reduce the window of opportunity for attackers. Tenable Security Center provides an on-premise solution for organizations to better understand vulnerability management. By facilitating the interactions with patch management solutions, which is required by sub control 3.4 & 3.5, Tenable Security Center allows all 3 IG levels to better understand risk and mitigate threats.

The CAS provides guidance on how to assess the organization's progress in this journey. This guide illustrates how the CISO can effectively measure cybersecurity success. Shown below are the CIS Control 3 IG levels and requirements.

### CIS Control 3: Continuous Vulnerability Management

| Sub-Control | Asset Type   | Security Function | Control Title  | Control Descriptions   | Implementation Groups |   |   |
|-------------|--------------|-------------------|--|--|-----------------------|---|---|
|             |              |                   |  |  | 1                     | 2 | 3 |
| 3.1         | Applications | Detect            | Run Automated Vulnerability Scanning Tools               | Utilize an up-to-date Security Content Automation Protocol (SCAP) compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems. |                       |   |   |
| 3.2         | Applications | Detect            | Perform Authenticated Vulnerability Scanning             | Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested.   |                       |   |   |
| 3.3         | Users        | Protect           | Protect Dedicated Assessment Accounts                    | Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.  |                       |   |   |
| 3.4         | Applications | Protect           | Deploy Automated Operating System Patch Management Tools | Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.   |                       |   |   |
| 3.5         | Applications | Protect           | Deploy Automated Software Patch Management Tools         | Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.  |                       |   |   |
| 3.6         | Applications | Respond           | Compare Back-to-Back Vulnerability Scans                 | Regularly compare the results from consecutive vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.   |                       |   |   |
| 3.7         | Applications | Respond           | Utilize a Risk-Rating Process                            | Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities.   |                       |   |   |



As shown above, the IG1 organization is required to implement Sub-Controls 3.4 - **Deploy Automated Operating Systems Patch Management Tools**, and 3.5 - **Deploy Automated Software Patch Management Tools**. Some useful methods to collect data to meet these requirements include:

Credentialed Active Scanning, specifically:

- Identify operating systems/software/applications that are installed on hosts
- Identify patching/version information on detected operating systems/software/applications



---

## Preface on Sub-Controls 3.4 and 3.5

---

Sub-Controls 3.4 and 3.5 provide advice and guidance to organizations on deploying operating systems and application/software patch management tools. Sub-Controls 3.4 and 3.5 have inputs and processes that dive deep into calculating a score around patching by combining the number of patches that have been installed to the number of patches not installed per endpoint. This helps to manually score each endpoint while considering the fact that counting of every single previously applied patch to the number of missing patches is a time consuming endeavor for any organization.

The ultimate goal of these sub-controls is to have a score (or ratio) of zero (The number of patches applied to each end point is the same as the number of patches that are available from the vendor for the OS or Software, i.e., there are no missing patches). Automated patch management tools can help organizations ensure that critical security concerns are patched as soon as a fix is available. However, there will always be patches that require manual updates. Completely relying on automated patch management as the only option results in poor patch management practice. This leads us to question: how do we make it better?

Tenable products are able to query a variety of patch management solutions and verify whether or not patches are installed on managed systems. Additionally, Nessus can also report on unmanaged hosts, hosts that have fallen out of management, or hosts that aren't functioning properly. Implementing a comprehensive patch management policy can provide organizations with a consistent, repeatable process that can keep systems up to date. If all systems are up to date, there is little to no "manual" scoring requirements as all ratios would be zero. Any systems out of patching compliance would be easily identified. The effort to capture and calculate the Inputs, Operations, and Measurements of the following sub-controls would greatly be reduced.

At the same time, we must also consider that if an organization has specific separate devices, such as database servers, web servers, mail servers, etc., each server type may have a different subset of applications installed. Or, in some cases, those applications may be combined onto a single server. Organizations must also be able to identify what software is appropriate for each endpoint device, removing inappropriate software in addition to patching.





## 3.4: Deploy Automated Operating System Patch Management Tools

Sub-control 3.4 states that you must deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.

| Asset Type   | Security Function | Implementation Groups |
|--------------|-------------------|-----------------------|
| Applications | Protect           | 1, 2, 3               |

### Dependencies

- Sub-control 5.1: Establish Secure Configurations

### Inputs

1. **Required OS auto-update configuration:** This could vary by organization, by product, by security tool, etc. This could be 1 setting or multiple settings. You must also determine if partial settings are creditable, the potential weighting of settings, dependencies, etc.
2. **List of required updates:** This could be pulled from the vendor's website, or could be an organization's selected subset of updates.
  - Optional Field: If time metrics are desired, this list also needs to show the date when each update was released by the vendor.
  - Continuous vulnerability scanning and integration with patch management systems can often lessen the burden on organizations to visit vendor sites and pull lists of updates. Tenable Security Center Continuous View supports a wide variety of patch management solutions including SCCM, WSUS, HCL BigFix, Dell KACE K1000, and Symantec Altiris.
3. **List of endpoints to be checked:** Ideally, this includes all assets. While some hardware devices exist that rarely receive patches, all endpoints should be monitored on a regular basis. The list of endpoints can be pulled from the "Ground Truth" devices of Sub-Control 1.4, because this list includes all known devices on the network as identified by continuous scanning.



4. **Optional: Time metrics:** The allowable time frame for installation of an update after its release. CIS recommends this be at least 30 days.

## Operations

1. For each endpoint in I3, compare that endpoint's auto-update configuration to that provided in I1. Then, generate a score based on the logic provided by I1 (M1).
2. For each endpoint in I3, retrieve a list of installed OS updates (M2) and compare that endpoint's installed updates to the required updates provided by I2. The list of matching updates is M3.
3. (Optional) If timing metrics are desired, for each endpoint, also determine the elapsed time between the update release date provided in I2 and the install date for each of the corresponding updates on the endpoint. This information could be added as another field attached to each update entry in M3.

## Measures

| Measure                              | Definition   |
|--------------------------------------|--|
| M1 = Auto-update configuration score | The endpoint-specific auto-update configuration score as determined by Operation 1.  |
| M2 = List of installed updates       | An endpoint-specific list of installed updates as determined by Operation 2.   |
| M3 = List of required updates        | An endpoint-specific list of required updates that are installed, as determined in Operation 2. This is a full list of updates that are installed for each endpoint. |
| M4 = Number of required updates      | The number of required OS updates per I2. This is a count of any updates that are required to be installed.  |
| M5 = Count of items in M3            | A count of the total number of items in M3.  |

## Metrics



## Update Effectiveness (Per Endpoint)

| Metric  | Calculation   |
|---|---|
| For a given endpoint, the calculated ratio of installed OS updates compared to the total number of OS updates required. | If $M4 = 0$ , this indicates the endpoint requires no OS updates. Otherwise, this metric is calculated as $M5 / M4$ |

## Update Effectiveness (Organizational)

The organizational metric is calculated by averaging the results of the **Per Endpoint** metric above.



## 3.5: Deploy Automated Software Patch Management Tools

Sub-control 3.5 states that you must deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.

| Asset Type   | Security Function | Implementation Groups |
|--------------|-------------------|-----------------------|
| Applications | Protect           | 1, 2, 3               |

### Dependencies

- Sub-control 2.1: Maintain Inventory of Authorized Software

### Inputs

- **Authorized Software List:** An authorized software list (ASL; sub-control 2.1) and information on the current authorized version.
- **Authoritative Source of Information:** Access to an authoritative source of information indicating version details by product.
- **List of Approved Exceptions:** A list of approved exceptions that notes any reasons that an authorized software package does not match the latest version.

### Operations

1. For each software in I1, list the software products that do not match the latest version as described by I2.
2. For each endpoint, obtain the current software load (the list of installed software). This information can be retrieved from sub-control 2.1.
3. For each endpoint, list the installed software that does not match the current authorized version from I1.
4. For each software product listed in Operation 3, list any that exist in the approved exceptions list (I3).

### Measures



| Measure  | Definition   |
|--|--|
| M1 = List of authorized software products at wrong version | A list of authorized software products installed on the endpoint that are not at the latest version.                               |
| M2 = Count of items in M1                                  | A count of the total number of items in M1.  |
| M3 = List of all authorized software products              | A list of all authorized software products installed on the endpoint.  |
| M4 = Count of items in M3                                  | A count of the total number of items in M3.  |
| M5 = List of authorized software with exceptions           | A list of authorized software products installed on the endpoint that are not at the latest version, but have approved exceptions. |
| M6 = Count of items in M5                                  | A count of the total number of items in M5.  |

## Metrics

### Update Effectiveness (Per Endpoint)

| Metric   | Calculation  |
|--|--|
| For a given endpoint, the ratio of installed software updates compared to the total number of required software updates. | If $M2 == 0$ , this indicates the endpoint requires no software updates. If $(M2 - M5) == 0$ , this indicates the endpoint requires software updates, but the out-of-date software has an approved exception. Otherwise, this metric is calculated as $(M2 - M5) / M4$ |

### Update Effectiveness (Organizational)

The organizational metric is calculated by averaging the results of the **Per Endpoint** metric above.



## CIS Control 4: Controlled Use of Administrative Privileges

The focus of this control is to ensure that all users with administrative level access use a dedicated or secondary account for any elevated activity. This administrator account should not be used for any other purpose, and should not be used for email, web-browsing, or similar activity.

The CIS states this Control is critical:

*“The misuse of administrative privileges is a primary method for attackers to spread inside a target enterprise. Two very common attacker techniques take advantage of uncontrolled administrative privileges. In the first, a workstation user running as a privileged user is fooled into opening a malicious email attachment, downloading and opening a file from a malicious website, or simply surfing to a website hosting attacker content that can automatically exploit browsers. The file or exploit contains executable code that runs on the victim’s machine either automatically or by tricking the user into executing the attacker’s content. If the victim user’s account has administrative privileges, the attacker can take over the victim’s machine completely and install keystroke loggers, sniffers, and remote control software to find administrative passwords and other sensitive data. Similar attacks occur with email. An administrator inadvertently opens an email that contains an infected attachment and this is used to obtain a pivot point within the network that is used to attack other systems.*

*The second common technique used by attackers is elevation of privileges by guessing or cracking a password for an administrative user to gain access to a target machine. If administrative privileges are loosely and widely distributed, or identical to passwords used on less critical systems, the attacker has a much easier time gaining full control of systems, because there are many more accounts that can act as avenues for the attacker to compromise administrative privileges.”*

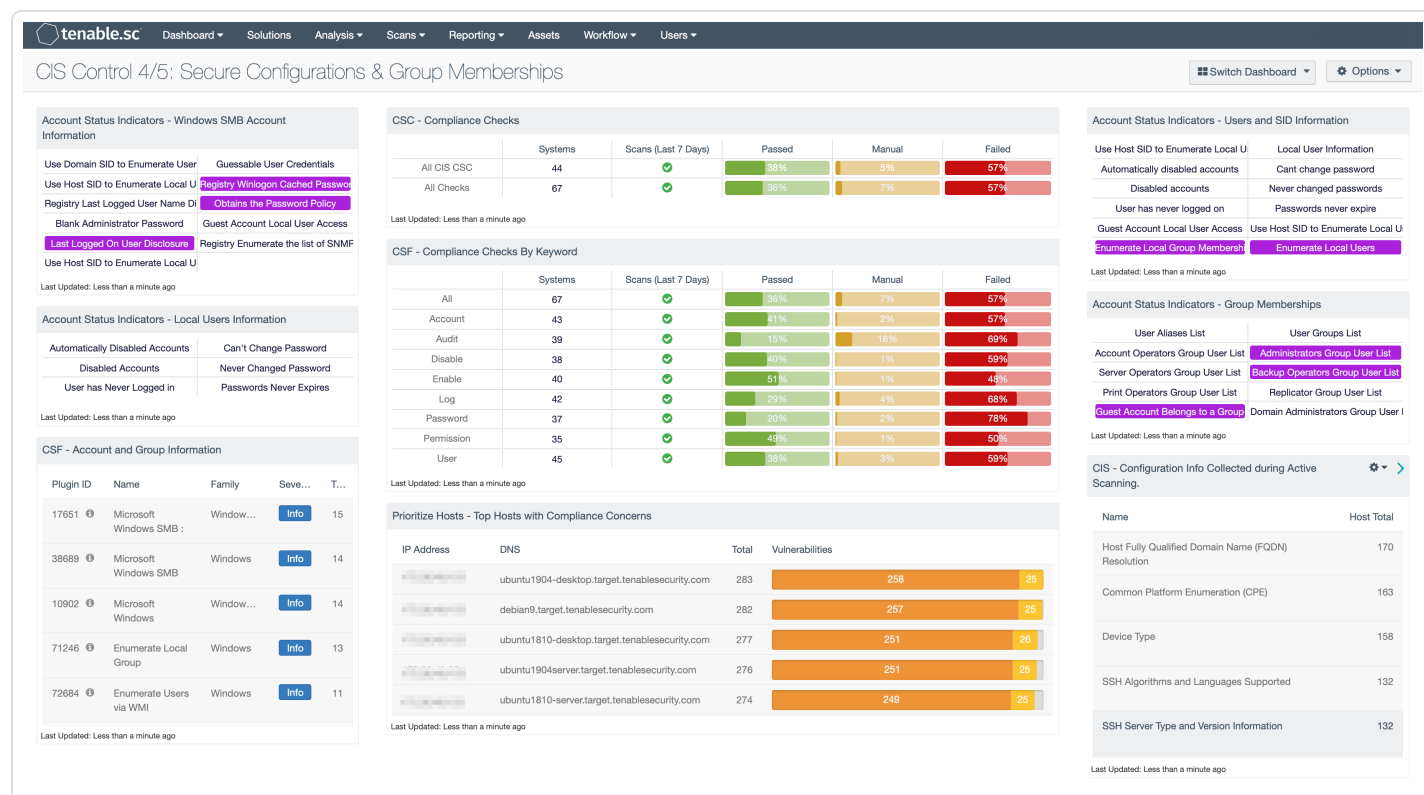
The journey of implementing the CIS Controls continues with controlled use of administrative privileges. Organizations are directed to verify that users with high-privileged accounts are not using privileged accounts for non-administrative activities such as web surfing and email. The two specific sub-controls that are part of Implementation Group 1 (IG1) are:

- [4.2: Change Default Passwords](#)
- [4.3: Ensure the Use of Dedicated Administrative Accounts](#)



For CIS Control 4, Tenable products allow security operations teams to use Tenable Security Center Continuous View to analyze group membership in local and domain groups. In addition to plugins that help monitor for group membership, there are also plugins that track the processes, services, and other related indicators of elevated privileges.

A vital step in vulnerability management is assessing the configuration of systems within the network. The CIS Control 4/5 Secure Configurations and Group Memberships Dashboard provides useful information to assist organizations with this control.



For more information about the CIS Control 3 dashboard, see [CIS Control 4/5: Secure Configurations & Group Memberships](#).

NIST also provides helpful information directly related to this CIS Control under the [NIST Digital Identity Guidelines](#).

The CAS provides guidance on how to assess the organization's progress in this journey. This guide illustrates how the CISO can effectively measure progress through the vulnerability management program. Shown below are the CIS Control 4 IG levels and requirements:



## CIS Control 4: Controlled Use of Administrative Privileges

| Sub-Control | Asset Type | Security Function | Control Title   | Control Descriptions  | Implementation Groups |   |   |
|-------------|------------|-------------------|---|---|-----------------------|---|---|
|             |            |                   |   |   | 1                     | 2 | 3 |
| 4.1         | Users      | Detect            | Maintain Inventory of Administrative Accounts                 | Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.   |                       |   |   |
| 4.2         | Users      | Protect           | Change Default Passwords                                      | Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.  |                       |   |   |
| 4.3         | Users      | Protect           | Ensure the Use of Dedicated Administrative Accounts           | Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not Internet browsing, email, or similar activities.  |                       |   |   |
| 4.4         | Users      | Protect           | Use Unique Passwords  | Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.  |                       |   |   |
| 4.5         | Users      | Protect           | Use Multi-Factor Authentication for All Administrative Access | Use multi-factor authentication and encrypted channels for all administrative account access.   |                       |   |   |
| 4.6         | Users      | Protect           | Use Dedicated Workstations For All Administrative Tasks       | Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading email, composing documents, or browsing the Internet. |                       |   |   |
| 4.7         | Users      | Protect           | Limit Access to Scripting Tools                               | Limit access to scripting tools (such as Microsoft® PowerShell and Python) to only administrative or development users with the need to access those capabilities.  |                       |   |   |
| 4.8         | Users      | Detect            | Log and Alert on Changes to Administrative Group Membership   | Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.  |                       |   |   |
| 4.9         | Users      | Detect            | Log and Alert on Unsuccessful Administrative Account Login    | Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.   |                       |   |   |





---

## Preface on Sub-Controls 4.2 and 4.3

---

The two metrics for sub-control 4.2 are:

- What percentage of credentials have been changed from the default value?
- What percentage of collected password policies comply with the organization's password policies?

Sub-control 4.3 specifically checks that each user has a separate Administrator account to perform those functions. While there is no method for determining if each user is assigned a separate Administrator level account, the methods of enumerating user accounts for sub-control 4.2 help organizations to meet the requirements of sub-control 4.3.

Sub-control 4.2 has inputs and processes that dive deep into calculating a score around the number of default account credentials per endpoint. Steps include manually creating a database of known default passwords, hashing these passwords, and comparing them to hashes on each endpoint for each account. Then, you can calculate a score for each endpoint. Manually locating a trusted database of default credentials, creating hashed passwords, and comparing them to existing password hashes is a time consuming endeavor for any organization.

The ultimate goal of these sub-controls is to have a score (or ratio) of zero (The number of default accounts on each end point is zero, there are no default credentials). Active and passive scanning with Tenable products allow the organization to query a variety of systems. Organizations can verify whether or not default credentials exist and are installed on managed systems. Additionally, active scanning can provide organizations with a consistent, repeatable process that can be used to identify credentials that have fallen out of policy guidelines (password complexity and password age). If all endpoints meet defined password guidelines, there is little to no "manual" scoring requirements as part of sub-control 4.2 as all ratios would be zero. Any systems found with default credentials, or credentials out of policy compliance, would be easily identified. The effort to capture and calculate the Inputs, Operations, and Measurements of the following sub-control would greatly be reduced, reducing overall cost and workload.

Helpful plugins for this subcontrol are:

- Nessus plugin 10860 SMB Use Host SID to Enumerate Local Users
- 95928 Linux User List Enumeration
- 95929 macOS and Mac OS X User List Enumeration



Nessus uses these plugins to enumerate all the users on a Windows, Linux, or MacOS endpoint, providing the following plugin output. Follow the guidance if you need to alter the ID range.

## Plugin Output

```
- Administrator (id 500, Administrator account)
- Guest (id 501, Guest account)
- datatel (id 1001)
- library (id 1002)
```

Note that, in addition to the Administrator, Guest, and Kerberos accounts, Nessus has enumerated local users with IDs between 1000 and 1200. To use a different range, edit the scan policy and change the 'Enumerate Local Users: Start UID' and/or 'End UID' preferences under 'Assessment->Windows' and re-run the scan. Only UIDs between 1 and 2147483647 are allowed for this range.



## Plugin Output

-----[ User Accounts ]-----

User : administrator  
Home folder : /home/administrator  
Start script : /bin/bash  
Groups : lpadmin  
cdrom  
smbashare  
sudo  
administrator  
plugdev  
dip  
adm

User : sshd  
Home folder : /var/run/sshd  
Start script : /usr/sbin/nologin  
Groups : nogroup

-----[ System Accounts ]-----

User : root  
Home folder : /root  
Start script : /bin/bash  
Groups : root

User : daemon  
Home folder : /usr/sbin  
Start script : /usr/sbin/nologin  
Groups : daemon



## Plugin Output

```
-----[ User Accounts ]-----
```

```
User   : admin
Groups : _appserveradm,
         _appserverusr,
         _lpadmin,
         admin
```

```
User   : daemon
```

```
User   : nobody
```

```
User   : root
Groups : admin,
         certusers,
         daemon,
         kmem,
         operator,
         procmod,
         procvview,
         staff,
         sys,
         tty,
         wheel
```

```
User   : test1
```

```
User   : test2
```

Additional plugins to validate password policies are:

- 10900/10914 Microsoft Windows - User Information: Passwords Never Expire
- 10898 Microsoft Windows - User Information: Never Changed Password
- 83303 Unix/Linux - Local Users Information: Passwords Never Expire

Additionally, Nessus has compliance checks for password length, and min/max password age for Linux, Solaris, HP-UX, Mac OS X. Windows systems can be audited against password history, and forced logoff.



## 4.2: Change Default Passwords

Sub-control 3.5 states that before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.

| Asset Type | Security Function | Implementation Groups |
|------------|-------------------|-----------------------|
| Users      | Protect           | 1, 2, 3               |

### Dependencies

- Sub-control 2.4: Track Software Inventory Information

### Inputs

1. **Inventory of Endpoints:** The organization's inventory of endpoints which utilize credentials, either at the OS level or at the application software level. Ideally, this includes software inventory from sub-control 2.4.
2. **Authoritative Source of Default Passwords:** An authoritative source of known default passwords. Tenable has thousands of checks for known default passwords. Active and passive scanning can identify and report on the use/existence of default credentials.
3. **Password Policy Configuration:** The organization's defined password policy configuration.

### Operations

1. For each endpoint in I1, enumerate the available logins, including hashed credentials (M1). For each endpoint that was previously identified, create a list of user ids.
2. For each endpoint in I1, generate password hashes for all relevant default passwords provided in I2 in accordance with the corresponding hashing procedures for the appropriate OS, application, etc. (including any applicable salting). The organization must identify a trusted resource that can provide a list of default passwords for each device on the organizations network.
3. For each login, compare the password hash for that login to the default password hashes generated in the previous operation. Create a list containing any logins that have hashes that match default password hashes, including the endpoint to which the login corresponds and



the default password and hash that matched (M3).

4. For each endpoint, collect the applied password policy configuration (M5).
5. For each endpoint, compare the password policy configuration to the organizationally defined password policy recommendations (including password length, complexity requirements, etc.). Create a list of endpoint password policies that adhere to the organizational policy (M7) and a list of endpoint password policies that deviate from the organizational policy (M9). Note where the deviations occur.

## Measures

| Measure  | Definition   |
|--|--|
| M1 = List of logins for credentialed accounts                  | A list of available logins for endpoints which utilized credentialed accounts. This can be derived from Operation 1.               |
| M2 = Count of items in M1                                      | A count of the total number of items identified in M1.   |
| M3 = List of logins with a hash matching a default hash        | A list of enumerated logins with a password hash that matches a known default password hash. This can be derived from Operation 3. |
| M4 = Count of items in M3                                      | A count of the total number of items in M3.  |
| M5 = List of collected endpoint password policy configurations | A list of the collected endpoint password policy configurations. This can be derived from Operation 4.                             |
| M6 = Count of items in M5                                      | A count of the total number of items in M5.  |
| M7 = List of matching password policy configurations           | A list of collected password policy configurations that match organizationally defined recommendations.                            |
| M8 = Count of items in M7                                      | A count of the total number of items in M7.  |
| M9 = List of unatching password policy configurations          | A list of collected password policy configurations that do not match organizationally defined recommendations.                     |

## Metrics



## Default Password Usage

| Metric   | Calculation      |
|--|------------------|
| The percentage of credentials that have been changed from the default value. | $(M2 - M4) / M2$ |

## Password Policy Compliance

| Metric   | Calculation  |
|--|--|
| The percentage of collected password policies that comply with the organization's password policies. | If $M6 = 0$ , then no endpoint password policy configurations were collected. Otherwise, the value of this metric is $M8 / M6$ |



## 4.3: Ensure the Use of Dedicated Administrative Accounts

Sub-control 4.3 states that you must ensure all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not Internet browsing, email, or similar activities.

| Asset Type | Security Function | Implementation Groups |
|------------|-------------------|-----------------------|
| Users      | Protect           | 1, 2, 3               |

### Dependencies

- None

### Inputs

1. **The list of users defined as Administrators:** All users who are Administrators.
2. **The list of user accounts for the users defined in Input 1:** A list of all user accounts for I1.
3. **The list of users NOT defined as Administrators:** All users who are not administrators.
4. **The list of user accounts for the users defined in Input 3:** A list of all user accounts for I3.
5. **The list of all user accounts.:** A list of all user accounts.
6. **The list of all Administrative user accounts:** A list of all Administrative user accounts.
7. **The list of non-Administrative user accounts:** Aa list of user accounts that do not have administrator access.

### Operations

1. For each user defined in I1, collect the Administrative user account for that user from I6 and the non-Administrative user account from I7.
2. For each user defined in I3, collect any Administrative user account for that user from I6 and the non-Administrative user account from I7.

### Measures





| Measure                             | Definition                                       |
|-------------------------------------|--|
| M1 = List of Admin users            | A list of all administrative users.              |
| M2 = Count of items in M1           | A count of the total number of items in M1.      |
| M3 = List of users from Operation 1 | A list of all users identified from Operation 1. |
| M4 = Count of items in M3           | A count of the total number of items in M3.      |
| M5 = List of users from Operation 2 | A list of all users identified from Operation 2. |
| M6 = Count of items in M5           | A count of the total number of items in M5.      |

## Metrics

### Administrative User Accounts

| Metric  | Calculation   |
|---|---|
| Determines whether those users identified as Administrative-level have at least one Administrative-level and one non-Administrative level user account. | The mapping performed by Operation 1 must show that, for each Administrative-level user, at least 1 Administrative-level user account and at least 1 non-Administrative-level user account are available. Otherwise, this metric is a <b>FAIL</b> |

### Unauthorized User Accounts

| Metric   | Calculation  |
|--|--|
| Illustrates any non-Administrative-level users that have been assigned an Administrative-level user account. | If <b>M6 &gt; 0</b> , then <b>FAIL</b> ; otherwise <b>PASS</b> |



---

## CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

---

The focus of this control is to maintain documented security configuration standards for all authorized operating systems and software. Organizations must establish a baseline security configuration, implement a configuration management and change control process, and actively be able to report on the security configuration of all endpoint devices such as:

- Mobile devices
- Laptops
- Servers
- Workstations

The CIS states this Control is critical:

*“As delivered by manufacturers and resellers, the default configurations for operating systems and applications are normally geared towards ease-of-deployment and ease-of-use – not security. Basic controls, open services and ports, default accounts or passwords, older (vulnerable) protocols, and pre-installation of unneeded software can be exploitable in their default state.*

*Developing configuration settings with good security properties is a complex task beyond the ability of individual users, requiring analysis of potentially hundreds or thousands of options in order to make good choices (the Procedures and Tools section below provides resources for secure configurations). Even if a strong initial configuration is developed and installed, it must be continually managed to avoid security “decay” as software is updated or patched, new security vulnerabilities are reported, and configurations are “tweaked” to allow the installation of new software or support new operational requirements. If not, attackers will find opportunities to exploit both network accessible services and client software.”*

The journey of implementing the CIS Controls continues with the Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers. Organizations are directed to develop strong, secure baseline configurations for each deployed software system. Organizations are also directed to maintain documented security configuration standards for all authorized oper-



ating systems and software. The specific sub-controls that are part of Implementation Group 1 (IG1) are:

- [5.1: Establish Secure Configurations](#)

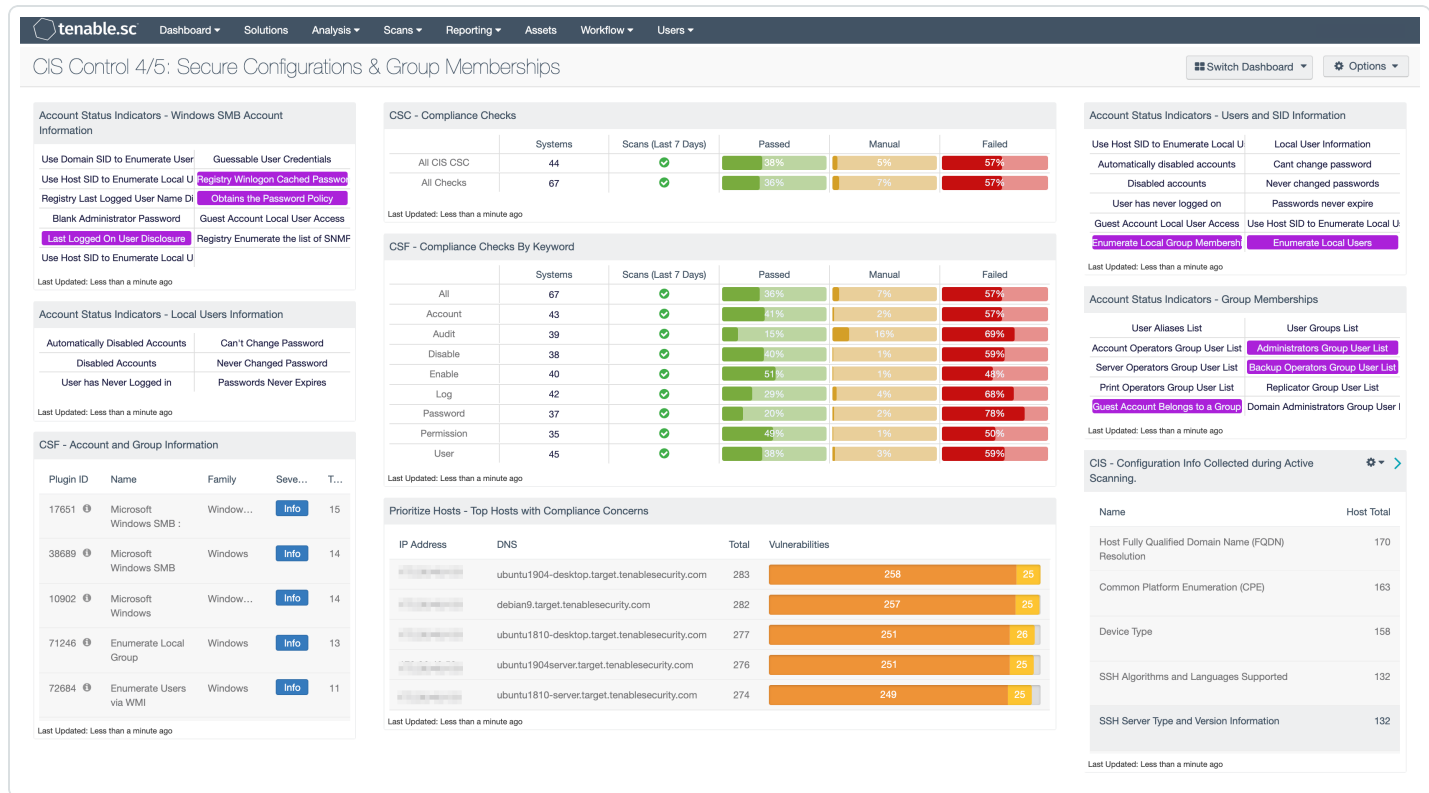
Oftentimes organizations struggle to get started. Small organizations purchase devices that arrive pre-configured or pre-loaded with an operating system and applications. Large organizations typically struggle with large numbers of devices which become harder to manage over time. Creating a secure baseline is challenging at best, and involves a great deal of resources and expertise. Why recreate the wheel developing a secure baseline? CIS and NIST have developed publicly available security benchmarks, security guides, and checklists that have been thoroughly vetted. Excellent resources include:

- [The CIS Benchmarks™ Program](#)
- [The NIST National Checklist Program](#)

Organizations can save a great deal of time and effort by starting with these publicly available resources, then augmenting or adjusting these baselines to satisfy local policies and requirements. Because these resources are trusted industry standards, any deviations should be documented to facilitate later reviews or audits. For example, complex enterprises may find that a single security baseline configuration is impractical. Many organizations may find they need to support different configurations, such as those for web servers, database servers, etc,. If this is the case, the number of baseline variations should be kept to a minimum and should be well documented.

For CIS Control 5, Tenable products allow security operations teams to use Tenable Security Center Continuous View to analyze endpoint operating systems and software configurations. Using the CIS Benchmarks and Tenable Security Center, the organization can verify that established configuration policies are followed.

A vital step in vulnerability management is assessing the configuration of systems within the network. The CIS Control 4/5 Secure Configurations and Group Memberships Dashboard provides useful information to assist organizations with this control.



- 64 -



---

## Preface on Sub-Control 5.1

---

The single metric for sub-control 5.1 Implementation Group 1 (IG1) is:

- The percentage of the total OS/Software in an enterprise for which security configuration standards are documented and maintained

Specifically, Sub-Control 5.1 checks that the organization maintains documented security configuration standards for all authorized operating systems and software. A passing score on this sub-control is achieved when the organization states that they have established and documented security configuration standards for each endpoint. This is a relatively simple and straightforward check.

Just as with previous sub-controls, the goal of this sub-control is to have a score (or ratio) of zero (all endpoints have documented security standards). However, organizations have an opportunity to easily jump ahead to IG2 or IG3. Active and passive scanning with Tenable products provide the organization with the ability to query a variety of systems. Organizations can verify whether or not endpoints meet established security best practices. Additionally, active scanning can provide organizations with a consistent, repeatable process that can be used to identify endpoints that no longer meet compliance. If all endpoints pass these checks, there are little to no “manual” scoring requirements as part of most of the other sub-control 5.x items in CIS Control 5.

Many products are available that can perform vulnerability scans of endpoint devices and detect missing patches. However, a lack of vulnerabilities does not mean endpoint devices are compliant with any particular standard. By using Nessus and Tenable Security Center, information is aggregated for an entire network or asset class allowing security and risk to be analyzed globally. This allows organizations to spot trends in non-compliant systems and adjust controls to fix these on a larger scale. Nessus can log into Unix and Windows servers, Cisco devices, SCADA systems, IBM iSeries servers, databases, and more, to determine if they have been configured in accordance with the local site security policy. For example:

- Windows endpoints: Nessus can test for any setting that can be configured as a “policy” under the Microsoft Windows framework. There are several hundred registry settings that can be audited. The permissions of files, directories, and objects can also be analyzed.
- Unix endpoints: Nessus can broadly be used to test for file permissions, file contents, running processes, and user access control for a variety of Unix-based systems. Currently, checks are available to audit Solaris, Red Hat, AIX, HP-UX, SUSE, Gentoo, and FreeBSD derivatives of Unix.



When using Nessus for compliance scanning, each of the audit file types has a corresponding plugin ID. In Tenable Security Center, however, the audit file plugin ID is not used. In Tenable Security Center when you install an audit file, a new plugin is created for each check with a plugin number greater than ID 1000000. To retain the audit file type, there is a cross reference called "auditFile". You can view the auditFile value in the Reference Information section of the Vulnerability Detail List tool.

When searching using the Cross Reference field, the XREF TYPE and XREF ID are separated by a pipe (|) character. If the filter should search for more than one XREF TYPE and ID combination, then separate the two phrases with a comma, as shown below.

## Reference Information

**800-171:** 3.1.11

**800-53:** AC-12

**CN-L3:** 7.1.2.2(d)

**CN-L3:** 7.1.3.7(b)

**CSCv6:** 16.4

**HIPAA:** 164.312(a)(2)(iii)

**ITSG-33:** AC-12

**LEVEL:** 1S

**NIAv2:** NS49

**PCI-DSSv3.1:** 12.3.8

**PCI-DSSv3.1:** 8.1.8

**PCI-DSSv3.2:** 12.3.8

**PCI-DSSv3.2:** 8.1.8

**Cross References:** auditFile:cisco, LEVEL:1S, 800-171:3.1.11, 800-53:AC-12, CN-L3:7.1.2.2(d),7.1.3.7(b), **CSCv6:16.4**, HIPAA:164.312(a)(2)(iii), ITSG-33:AC-12, NIAv2:NS49, PCI-DSSv3.1:12.3.8,8.1.8, PCI-DSSv3.2:12.3.8,8.1.8



## 5.1: Establish Secure Configurations

Sub-control 5.1 states that you must maintain documented security configuration standards for all authorized operating systems and software.

| Asset Type   | Security Function | Implementation Groups |
|--------------|-------------------|-----------------------|
| Applications | Protect           | 1, 2, 3               |

### Dependencies

- Sub-control 2.1: Maintain Inventory of Authorized Software

### Inputs

1. **Authorized Software List:** The list of authorized software. This can be pulled from sub-control 2.1.
2. **Security Configuration Standards:** The list of enterprise security configuration standards.

### Assumptions

- Documentation of secure configuration standards should include any approved deviations/exceptions from industry-standard security baselines such as CIS benchmarks, DISA Security Technical Implementation Guides (STIGs), or U.S. government configuration baselines (USGCB).

### Operations

1. Perform a calculation to compute the intersection (M1) of I1 and I2.

### Measures

| Measure  | Definition   |
|--|--|
| M1 = List of authorized software with security configuration standards | A list of all the software/applications the organization has, including operating systems, that have associated enterprise security configuration standards. |



|   |   |
|---|---|
| M2 = Count of items in M1   | A count of the total number of items in M1.   |
| M3 = List of authorized software with security configuration standards    | A list of all the software/applications the organization has, including operating systems, that do not have associated enterprise security configuration standards. |
| M4 = Count of items in M3   | A count of the total number of items in M3.   |
| M5 = List of security configuration standards without associated software | A list of all the enterprise security configuration standards that do not have installed applications/software or operating systems within the organization.        |
| M6 = Count of items in M5   | A count of the total number of items in M5.   |
| M7 = List of authorized software  | A list of authorized applications/software and operating systems.   |
| M8 = Count of items in M7   | A count of the total number of items in M7.   |

## Metrics

### Security Configuration Standards Coverage

| Metric   | Calculation            |
|--|------------------------|
| The percentage of the total OS/Software in an enterprise that have security configuration standards documented and maintained. | $\frac{(M8 - M4)}{M8}$ |





---

## CIS Control 6: Maintenance, Monitoring and Analysis of Audit Logs

---

The focus of this control is to collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

The CIS states this Control is critical:

*“Deficiencies in security logging and analysis allow attackers to hide their location, malicious software, and activities on victim machines. Even if the victims know that their systems have been compromised, without protected and complete logging records they are blind to the details of the attack and to subsequent actions taken by the attackers. Without solid audit logs, an attack may go unnoticed indefinitely and the particular damages done may be irreversible. Sometimes logging records are the only evidence of a successful attack. Many organizations keep audit records for compliance purposes, but attackers rely on the fact that such organizations rarely look at the audit logs, and they do not know that their systems have been compromised.*

*Because of poor or nonexistent log analysis processes, attackers sometimes control victim machines for months or years without anyone in the target organization knowing, even though the evidence of the attack has been recorded in unexamined log files.”*

The journey of implementing the CIS Controls continues with the Maintenance, Monitoring and Analysis of Audit Logs. Organizations are directed to ensure that local logging has been enabled on all systems and networking devices. The specific sub-controls that are part of Implementation Group 1 (IG1) are:

- [6.2: Activate Audit Logging](#)



---

## Preface on Sub-Control 6.2

---

The single metric for sub-control 6.2 Implementation Group 1 (IG1) is:

- Ensure that local logging has been enabled on all systems and networking devices.

Specifically, Sub-Control 6.2 checks that the organization maintains an event logging policy, and that endpoints are appropriately configured. A passing score on this sub-control is achieved by the organization stating that they have an established, documented logging policy for each endpoint, and that each endpoint has been checked and validated as appropriately configured. As with previous sub-controls, the goal of this sub-control is to have a score (or ratio) of zero (all endpoints have documented security standards).

Using Tenable Security Center, organizations are able to verify configuration settings on a wide variety of systems. In Control 5, we discussed how to establish baseline configuration settings. Using the CIS Benchmarks and the corresponding audit file, organizations can use Tenable Security Center to verify that logging is enabled. This illustrates the connection between controls 5 & 6. Listed below are two examples, however a majority of the CIS Benchmarks and Tenable Audit files have recommendations for establishing a baseline along with detail on how to configure & audit the settings.

- CIS Microsoft Windows Server 2008 R2 Benchmark v3.2.0
  - <https://workbench.cisecurity.org/files/2696>
  - CIS\_MS\_Windows\_Server\_2008\_R2\_MS\_Level\_1\_v3.2.0.audit
  - 9.3.10 Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes'
- CIS Benchmark for Cisco IOS 16 Benchmark v1.0.0
  - <https://workbench.cisecurity.org/files/2657>
  - CIS\_Cisco\_IOS\_16\_v1.0.0\_Level\_1.audit
  - 2.2.1 Set 'logging on'



## 6.2: Activate Audit Logging

Sub-control 6.2 states that you must ensure that local logging has been enabled on all systems and networking devices.

| Asset Type | Security Function | Implementation Groups |
|------------|-------------------|-----------------------|
| Network    | Detect            | 1, 2, 3               |

### Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 5.1: Establish Secure Configurations

### Inputs

1. **Endpoint Inventory:** The list of endpoints from the endpoint inventory
2. **Event Logging Inventory:** The list of events that should be logged (aka an event logging policy).

### Assumptions

- There could potentially be numerous events that should be logged.
- A checklist verifying the logging policy can be examined per endpoint.

### Operations

1. For each endpoint, determine if the configured event logging policy matches the policy defined by I2. Note the appropriately and inappropriately configured endpoints.

### Measures

| Measure                   | Definition                                  |
|---------------------------|---|
| M1 = List of Endpoints    | A list of all endpoints.                    |
| M2 = Count of items in M1 | A count of the total number of items in M1. |



|  |  |
|--|--|
| M3 = List of appropriately configured end-points   | A list of all appropriately configured end-points.   |
| M4 = Count of items in M3                          | A count of the total number of items in M3.          |
| M5 = List of inappropriately configured end-points | A list of all inappropriately configured end-points. |
| M6 = Count of items in M5                          | A count of the total number of items in M5.          |

## Metrics

### Logging Policy Coverage

| Metric   | Calculation |
|--|-------------|
| The ratio of endpoints implementing the prescribed event logging policy compared to the total number of endpoints. | $(M4 / M6)$ |



---

## Foundational Controls

---

- [CIS Control 7: Email and Web Browser Protections](#)
- [CIS Control 8: Malware Defenses](#)
- [CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services](#)
- [CIS Control 10: Data Recovery Capabilities](#)
- [CIS Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches](#)
- [CIS Control 12: Boundary Defense](#)
- [CIS Control 13: Data Protection](#)
- [CIS Control 14: Controlled Access Based on the Need to Know](#)
- [CIS Control 15: Wireless Access Control](#)
- [CIS Control 16: Account Monitoring and Control](#)



---

## CIS Control 7: Email and Web Browser Protections

---

The focus of this control is to minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems.

The CIS states this Control is critical:

*“Web browsers and email clients are very common points of entry and attack because of their technical complexity, flexibility, and their direct interaction with users and with other systems and websites. Content can be crafted to entice or spoof users into taking actions that greatly increase risk and allow introduction of malicious code, loss of valuable data, and other attacks. Since these applications are the main means that users interact with untrusted environments, these are potential targets for both code exploitation and social engineering.”*

The journey of implementing the CIS Controls with CIS Control 7 moves from Basic to Foundational controls, and begins with Email and Web Browser Protections. Organizations are directed to ensure that only fully supported web browsers and email clients are used. Ideally, only the latest version of these fully supported web browsers and email clients should be used. Organizations are also directed to use Domain Name System (DNS) filtering services to assist in the identification and blocking of malicious domains. The specific sub-controls that are part of Implementation Group 1 (IG1) are:

- 7.1 Ensure Use of Only Fully Supported Browsers and Email Clients Software
- 7.7: Use of DNS Filtering Services



## CIS Control 7: Email and Web Browser Protections

| Sub-Control | Asset Type   | Security Function | Control Title   | Control Descriptions  | Implementation Groups |   |   |
|-------------|--------------|-------------------|---|---|-----------------------|---|---|
|             |              |                   |   |   | 1                     | 2 | 3 |
| 7.1         | Applications | Protect           | Ensure Use of Only Fully Supported Browsers and Email Clients       | Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.   |                       |   |   |
| 7.2         | Applications | Protect           | Disable Unnecessary or Unauthorized Browser or Email Client Plugins | Uninstall or disable any unauthorized browser or email client plugins or add-on applications.   |                       |   |   |
| 7.3         | Applications | Protect           | Limit Use of Scripting Languages in Web Browsers and Email Clients  | Ensure that only authorized scripting languages are able to run in all web browsers and email clients.  |                       |   |   |
| 7.4         | Network      | Protect           | Maintain and Enforce Network-Based URL Filters                      | Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.                           |                       |   |   |
| 7.5         | Network      | Protect           | Subscribe to URL-Categorization Service                             | Subscribe to URL-categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default.   |                       |   |   |
| 7.6         | Network      | Detect            | Log All URL Requests  | Log all URL requests from each of the organization's systems, whether on-site or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.  |                       |   |   |
| 7.7         | Network      | Protect           | Use of DNS Filtering Services                                       | Use Domain Name System (DNS) filtering services to help block access to known malicious domains.  |                       |   |   |
| 7.8         | Network      | Protect           | Implement DMARC and Enable Receiver-Side Verification               | To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards. |                       |   |   |
| 7.9         | Network      | Protect           | Block Unnecessary File Types  | Block all email attachments entering the organization's email gateway if the file types are unnecessary for the organization's business.  |                       |   |   |
| 7.10        | Network      | Protect           | Sandbox All Email Attachments                                       | Use sandboxing to analyze and block inbound email attachments with malicious behavior.  |                       |   |   |



## Preface on Sub-Controls 7.1 and 7.7

The CIS recommends that content filters, popup blockers, and blocking of known malicious domains be employed to reduce the number of threats available to web browsers and email clients. In addition, spam filtering, restricting the types of files that can be sent/received (blocking attachments that are not required), and email encryption add additional layers of security.

For CIS Control 7, Tenable products allow security operations teams to use Tenable Security Center Continuous View to analyze endpoint browser and email client configurations. Using a variety of active and passive plugins paired with Tenable Security Center, the organization can verify established configuration policies are followed. Tenable Security Center provides an on-premise solution for organizations to better understand vulnerability management. As an example, Tenable Network Monitor can passively detect and enumerate web browsers that are being utilized, as well as any potential vulnerabilities present in the versions detected. Active credentialed scanning by Nessus can provide detailed information on web browsers that are installed via the same methods of software enumeration described in CIS Control 2. Analysts can easily produce tables and matrices utilizing this information, such as the sample matrix below, which presents Chrome vulnerabilities. Many other browser clients such as Firefox, Internet Explorer, and Safari, are part of the **Browser Vulnerabilities Dashboard** located in the Tenable.sc feed.

Browser Vulnerabilities - Chrome

All Vulnerabilities

Critical Vulns

Exploitable Vulns

|             |            |             |
|-------------|------------|-------------|
| Adobe       | Flash      | Java        |
| Quicktime   | Shockwave  | Silverlight |
| Account     | Bypass     | Credentials |
| Corruption  | CSRF       | Disclosure  |
| DoS         | Escalation | Execution   |
| Injection   | Jacking    | MitM        |
| Overflow    | Password   | Script      |
| Spoofing    | Theft      | Toolbar     |
| Unsupported | Validation | XSS         |

Last Updated: 1 hour ago

Browser Vulnerabilities - Firefox

All Vulnerabilities

Critical Vulns

Exploitable Vulns

|             |            |             |
|-------------|------------|-------------|
| Adobe       | Flash      | Java        |
| Quicktime   | Shockwave  | Silverlight |
| Account     | Bypass     | Credentials |
| Corruption  | CSRF       | Disclosure  |
| DoS         | Escalation | Execution   |
| Injection   | Jacking    | MitM        |
| Overflow    | Password   | Script      |
| Spoofing    | Theft      | Toolbar     |
| Unsupported | Validation | XSS         |

Last Updated: 1 hour ago

Browser Vulnerabilities - Internet Explorer

All Vulnerabilities

Critical Vulns

Exploitable Vulns

|             |            |             |
|-------------|------------|-------------|
| Adobe       | Flash      | Java        |
| Quicktime   | Shockwave  | Silverlight |
| Account     | Bypass     | Credentials |
| Corruption  | CSRF       | Disclosure  |
| DoS         | Escalation | Execution   |
| Injection   | Jacking    | MitM        |
| Overflow    | Password   | Script      |
| Spoofing    | Theft      | Toolbar     |
| Unsupported | Validation | XSS         |

Last Updated: 1 hour ago

Browser Vulnerabilities - Safari

All Vulnerabilities

Critical Vulns

Exploitable Vulns

|             |            |             |
|-------------|------------|-------------|
| Adobe       | Flash      | Java        |
| Quicktime   | Shockwave  | Silverlight |
| Account     | Bypass     | Credentials |
| Corruption  | CSRF       | Disclosure  |
| DoS         | Escalation | Execution   |
| Injection   | Jacking    | MitM        |
| Overflow    | Password   | Script      |
| Spoofing    | Theft      | Toolbar     |
| Unsupported | Validation | XSS         |

Last Updated: 1 hour ago

Browser Vulnerabilities - Opera

All Vulnerabilities

Critical Vulns

Exploitable Vulns

|             |            |             |
|-------------|------------|-------------|
| Adobe       | Flash      | Java        |
| Quicktime   | Shockwave  | Silverlight |
| Account     | Bypass     | Credentials |
| Corruption  | CSRF       | Disclosure  |
| DoS         | Escalation | Execution   |
| Injection   | Jacking    | MitM        |
| Overflow    | Password   | Script      |
| Spoofing    | Theft      | Toolbar     |
| Unsupported | Validation | XSS         |

Last Updated: 1 hour ago

Browser Vulnerabilities - Summary by Browser

|                   | Vulnerabilities | Systems | % with Criticals | % with Exploits |
|-------------------|-----------------|---------|------------------|-----------------|
| Chrome            | 9402            | 1178    | 5%               | 50%             |
| Firefox           | 16695           | 1163    | 67%              | 67%             |
| Internet Explorer | 8252            | 1419    | 1%               | 35%             |
| Safari            | 65              | 18      | 17%              | 17%             |
| Opera             | 0               | 0       | 0%               | 0%              |

Last Updated: 1 hour ago

Browser Vulnerabilities - Summary by Keyword

|         | Vulnerabilities | Systems | % with Criticals | % with Exploits |
|---------|-----------------|---------|------------------|-----------------|
| Browser | 5730            | 4130    | 0%               | 0%              |
| Toolbar | 0               | 0       | 0%               | 0%              |
| Java    | 15617           | 1322    | 20%              | 57%             |
| XSS     | 86              | 70      | 0%               | 19%             |

Last Updated: 1 hour ago





For more information about the browser vulnerabilities dashboard, see [Browser Vulnerabilities Dashboard](#).

In most environments that use the Microsoft Office system, Outlook is often already the default program for email, contacts, and calendaring. Compliance checks exist to ensure that group policies are set which make Outlook the default program for email. Installed web browsers and email clients which were enumerated in Control 2, can easily be searched for vulnerabilities using vulnerability text filters within the **Analysis** tab of Tenable Security Center.

Just as with previous sub-controls, the goal of this sub-control is to have a score (or ratio) of zero (all endpoints having up to date/supported web browsers and email clients).



## 7.1: Ensure Use of Only Fully Supported Browsers and Email Clients

Sub-control 7.1 states that you must ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.

| Asset Type  | Security Function | Implementation Groups |
|-------------|-------------------|-----------------------|
| Application | Protect           | 1, 2, 3               |

### Dependencies

- Sub-control 2.1: Maintain Inventory of Authorized Software

### Inputs

1. **Software Inventory:** From the authorized software list (ASL: sub-control 2.1), the inventory of web browser and email client software. Each entry should have a notation indicating whether the software is “supported” or “unsupported”.
2. **Authoritative source of information:** Access to an authoritative source of information indicating supported/unsupported details by product.

### Operations

1. For each entry in I1, perform a lookup in I2 to verify.
2. For each entry in I1 labeled “supported”, perform a lookup in I2. From these lookups, note the list of authorized software labeled “supported” but are actually not supported based on the authoritative source lookup.
3. For each entry in I1 labeled “unsupported”, perform a lookup in I2. From these lookups, note the list of authorized software labeled “unsupported” but are actually supported based on the authoritative source lookup.
4. (Optional) Organizations can utilize Tenable Security Center to identify specific details about applications utilizing the same techniques that were previously used in sub-control 2. For



example, If we wanted to identify endpoints which had Firefox installed, we would filter on pluginID = 20811, with a Vulnerability Text = Firefox and we would get results similar to the screenshot below, which shows results for all the hosts which have Firefox installed.

## Plugin Output

The following software are installed on the remote host :

```
Windows Driver Package - Lexmark International Printer (01/28/2016 2.2.0.0)
[version 01/28/2016 2.2.0.0]
FMAudit Onsite [version 3.7.13.9069]
Mozilla Firefox 45.0.1 (x86 en-US) [version 45.0.1]
Mozilla Maintenance Service [version 45.0.1]
Microsoft Visual C++ 2005 Redistributable (x64) [version 8.0.56336] [installed
on 2019/08/22]
Microsoft .NET Framework 4.7.2 [version 4.7.03062] [installed on 2019/05/15]
Canon PRO-1 v1-1 series Printer Driver
VMware Tools [version 10.0.0.3000743] [installed on 2017/01/25]
Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219 [version
```

If we wanted to drill down into these results further, and specifically identify Firefox vulnerabilities, we could simply use a filter of Vulnerability Text = Firefox and set either No Severity, or chose a specific Severity to filter on as shown in the example below.

### Vulnerability Analysis

#### Filters

**\* Vulnerability Text**  
Contains firefox

**\* Address**  
All

**\* Plugin ID**  
All

**\* Plugin Name**  
All

**\* Severity**  
All

Apply All

Revert All

Select Filters

Load Query

Vulnerability Summary

Severity

☐ Select All

☐ Info

☐ Low

☐ Medium

☐ High

☒ Critical

Apply

Clear

Jump to Vulnerability Detail List

Total Results: 9619

| Plugin ID | Name  | Family                        | Severity | VPR | Total |
|-----------|---|-------------------------------|----------|-----|-------|
| 136404    | Mozilla Firefox < 76.0  | Windows                       | Critical | 9.9 | 767   |
| 134706    | Adobe Reader <= 2015.006.30510 / 2017.011.30158 / 2020.006.20034 Multiple Vulnerabilities (APSB20-13) | Windows                       | Critical | 7.4 | 716   |
| 130913    | Security Updates for Microsoft Office Products (November 2019)  | Windows : Microsoft Bulletins | Critical | 6.7 | 504   |
| 62758     | Microsoft XML Parser (MSXML) and XML Core Services Unsupported  | Windows                       | Critical |     | 492   |
| 126072    | Mozilla Firefox < 67.0.4  | Windows                       | Critical | 9.9 | 488   |
| 134942    | Microsoft Windows Type 1 Font Parsing Remote Code Execution Vulnerability (ADV200006)                 | Windows                       | Critical |     | 475   |
| 133673    | Adobe Reader <= 2015.006.30508 / 2019.021.20061 Multiple Vulnerabilities (APSB20-05)                  | Windows                       | Critical | 6.7 | 431   |
|           |   | Windows                       | Critical | 8.1 | 418   |
|           | / 2017.011.30152 / 2019.021.20056 Multiple Vulnerabilities (APSB19-55)                                | Windows                       | Critical | 9.2 | 375   |
|           | Application Detection   | Windows                       | Critical |     | 367   |
|           | / 2017.011.30148 / 2019.012.20040 Multiple Vulnerabilities (APSB19-49)                                | Windows                       | Critical | 8.9 | 339   |
|           | / 2017.011.30143 / 2019.012.20035 Multiple Vulnerabilities (APSB19-41)                                | Windows                       | Critical | 9.0 | 310   |
|           | / 2017.011.30138 / 2019.010.20099 Multiple Vulnerabilities (APSB19-18)                                | Windows                       | Critical | 6.7 | 294   |
|           | Control Unauthenticated RCE   | Windows                       | Critical | 5.9 | 294   |

## Measures



| Measure   | Definition  |
|---|---|
| M1 = List of unsupported items in I1  | A combination of Operation 1 results and the software initially marked as unsupported in I1. This can be pulled from the list of applications/software in sub-control 2.1 that are identified as email or web browsers. |
| M2 = Count of items in M1   | A count of the total number of items in M1.   |
| M3 = List of authorized web browser/email client software                           | An organizational list of supported/authorized web browsers/email clients.  |
| M4 = Count of items in M3   | A count of the total number of items in M3.   |
| M5 = List of items from I1 labeled as "supported" that are not actually supported   | A list of items from I1 labeled as "supported" but that are not actually supported. This can be pulled from sub-control 2.1.  |
| M6 = Count of items in M5   | A count of the total number of items in M5.   |
| M7 = List of items from Input 1 labeled as "unsupported" but are actually supported | A list of items from I1 labeled as "unsupported" but that are actually supported. This can be pulled from sub-control 2.1.  |
| M8 = Count of items in M7   | A count of the total number of items in M7.   |

## Metrics

### Percentage of Unsupported Web Browser/Email Client Software in Use

| Metric | Calculation |
|--------|-------------|
|--------|-------------|



The calculation of this metric is determined by the ratio of unsupported web browser/email client software to the total authorized web browser/email client software in use.

$$\frac{(M4 - M2)}{M4}$$

#### Rate of False Positives

| Metric   | Calculation            |
|--|------------------------|
| The calculation of this metric is determined by the ratio of web browser-/email client software labeled "supported" but found to be unsupported, to the total authorized web browser/email client software in use. | $\frac{(M4 - M6)}{M4}$ |

#### Rate of False Negatives

| Metric   | Calculation            |
|--|------------------------|
| The calculation of this metric is determined by the ratio of web browser-/email client software labeled "unsupported" but found to be supported, to the total authorized web browser/email client software in use. | $\frac{(M4 - M8)}{M4}$ |



## 7.7: Use of DNS Filtering Services

Sub-control 7.7 states that you must use Domain Name System (DNS) filtering services to help block access to known malicious domains.

| Asset Type | Security Function | Implementation Groups |
|------------|-------------------|-----------------------|
| Network    | Protect           | 1, 2, 3               |

### Dependencies

- Sub-control 1.5: Maintain Asset Inventory Information

### Inputs

1. **Endpoint Inventory:** The list of endpoints to be audited. This can pulled sub-control 1.5.
2. **Accepted DNS services:** The list of accepted DNS filtering services, such as Quad-9.

### Operations

1. For each endpoint in I1, collect its DNS configuration setting. Note appropriately and inappropriately configured endpoints.

### Measures

| Measure   | Definition   |
|---|--|
| M1 = List of audited endpoints                    | A list of endpoints to be audited.                   |
| M2 = Count of items in M1                         | A count of the total number of items in M1.          |
| M3 = List of appropriately configured endpoints   | A list of endpoints that are configured correctly.   |
| M4 = Count of items in M3                         | A count of the total number of items in M3.          |
| M5 = List of inappropriately configured endpoints | A list of endpoints that are configured incorrectly. |
| M6 = Count of items in M5                         | A count of the total number of items in M5.          |



## Metrics

### DNS Filtering Coverage

| Metric   | Calculation |
|--|-------------|
| The ratio of endpoints configured to use accepted DNS filtering service compared to the total number of endpoints which utilize DNS. | $M4 / M2$   |

### Traffic Analysis

**Note:** A second measurement could utilize traffic analysis to determine if any traffic is not being sent through the prescribed DNS services.



---

## CIS Control 8: Malware Defenses

---

The focus of this control is to control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

The CIS states this Control is critical:

*“Malicious software is an integral and dangerous aspect of Internet threats, as it is designed to attack your systems, devices, and your data. It is fast-moving, fast-changing, and enters through any number of points like end-user devices, email attachments, web pages, cloud services, user actions, and removable media. Modern malware is designed to avoid defenses, and attack or disable them. Malware defenses must be able to operate in this dynamic environment through large-scale automation, rapid updating, and integration with processes like incident response. They must also be deployed at multiple possible points of attack to detect, stop the movement of, or control the execution of malicious software. Enterprise endpoint security suites provide administrative features to verify that all defenses are active and current on every managed system.”*

The journey of implementing the Foundational CIS Controls continues with CIS Control 8 Malware Defenses. Organizations are directed to ensure that the scanning engine and signature database are updated on a regular basis for all anti-malware software. Ideally, only the latest version should be used. Organizations are also directed to configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected. Finally, as part of the IG1 set of controls, organizations are advised to configure devices to not auto-run content from removable media. The specific sub-controls that are part of Implementation Group 1 (IG1) are:

- 8.2 Ensure Anti-Malware Software and Signatures are Updated
- 8.4 Configure Anti-Malware Scanning of Removable Media
- 8.5 Configure Devices to Not Auto-Run Content





## CIS Control 8: Malware Defenses

| Sub-Control | Asset Type | Security Function | Control Title  | Control Descriptions  | Implementation Groups |   |   |
|-------------|------------|-------------------|--|---|-----------------------|---|---|
|             |            |                   |  |   | 1                     | 2 | 3 |
| 8.1         | Devices    | Protect           | Utilize Centrally Managed Anti-Malware Software                                      | Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.   |                       |   |   |
| 8.2         | Devices    | Protect           | Ensure Anti-Malware Software and Signatures Are Updated                              | Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.   |                       |   |   |
| 8.3         | Devices    | Detect            | Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies | Enable anti-exploitation features such as Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables. |                       |   |   |
| 8.4         | Devices    | Detect            | Configure Anti-Malware Scanning of Removable Media                                   | Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.  |                       |   |   |
| 8.5         | Devices    | Protect           | Configure Devices to Not Auto-Run Content  | Configure devices to not auto-run content from removable media.   |                       |   |   |
| 8.6         | Devices    | Detect            | Centralize Anti-Malware Logging  | Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.  |                       |   |   |
| 8.7         | Network    | Detect            | Enable DNS Query Logging   | Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains.   |                       |   |   |
| 8.8         | Devices    | Detect            | Enable Command-Line Audit Logging  | Enable command-line audit logging for command shells, such as Microsoft PowerShell and Bash.  |                       |   |   |



---

## Preface on Sub-Controls 8.2, 8.4, and 8.5

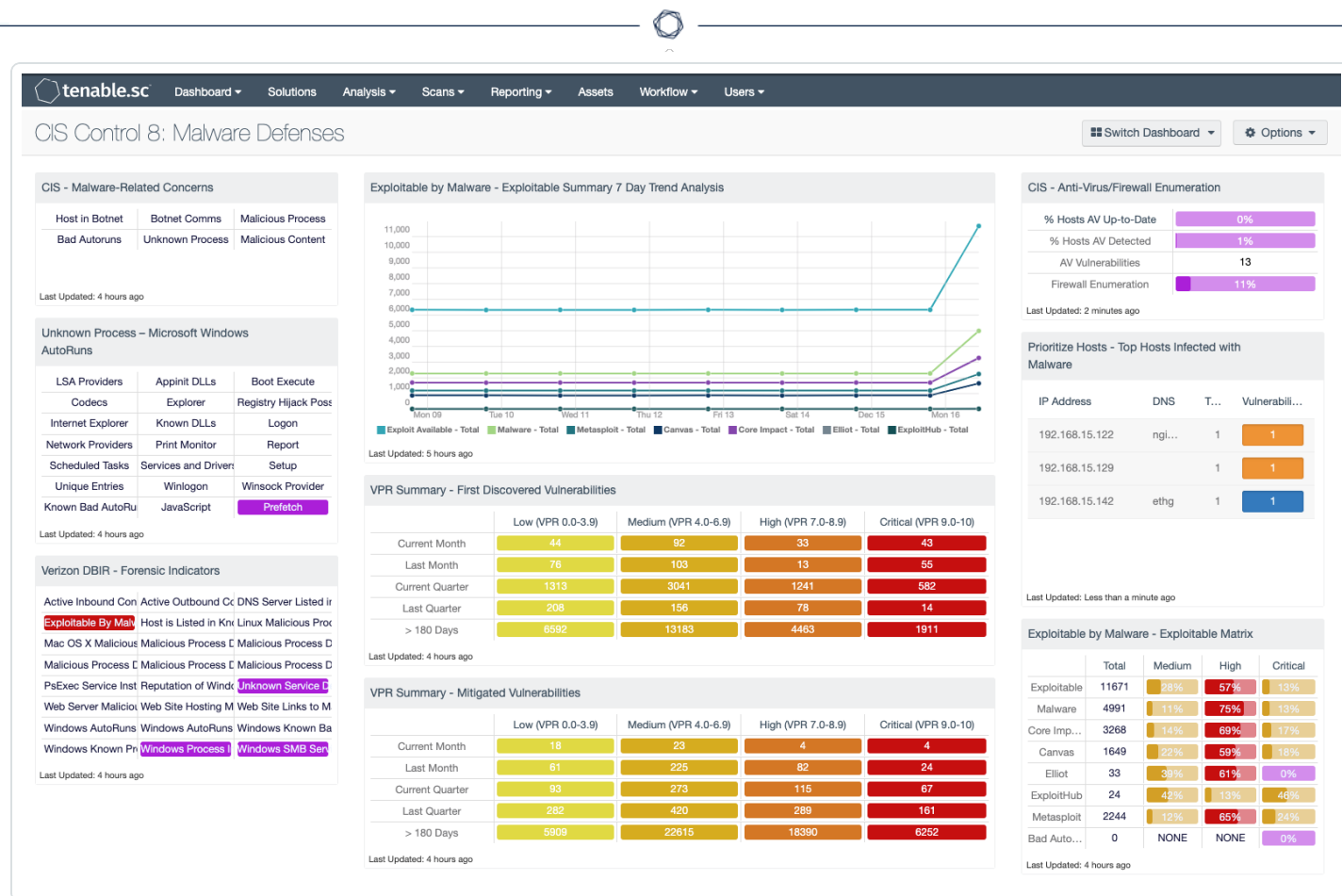
---

Malicious software, commonly known as malware, is any software that can attack your systems or data. The majority of malware is designed to be fast moving, and is typically identified by general terms such as worms, viruses, trojans, adware, rootkits, and spyware. Malware can be something simple and annoying, like adware, or can be a complex application that steals data, deletes documents, or installs unwanted software without the user's knowledge.

For CIS Control 8, Tenable products allow the security operations teams to use Tenable Security Center Continuous View to analyze endpoints for malicious file detection. As an example, Nessus detects potentially unwanted files on a remote host utilizing the built in malicious file detection ability. Using a credentialed Nessus scan, hash files are compared against known malware signatures cataloged by major antivirus vendors. A report then shows which anti-virus vendor considers the file to be malicious. Security teams may find this information, along with data derived from the following plugins, useful in detecting malicious applications:

- [88963](#) Malicious File Detection
- [59275](#) Malicious Process Detection
- [59641](#) Unwanted Software Detection

Additionally, Tenable Security Center has the CIS Control 8: Malware Defenses dashboard, which contains components that provide information and report on enforcing anti-virus (AV) deployments, disabling Auto Run, and automating AV scans. In this dashboard, Tenable Security Center shows all systems with Auto Run settings enabled, the AV status, and many other parameters described throughout all sub controls. Using Tenable Security Center, customers from all IG's can effectively track and report on sub controls 8.1, 8.2, and 8.5.



For more information about the CIS Control 8 dashboard, see [CIS Control 8: Malware Defenses](#).

Solely relying on software enumeration does not always indicate that an antivirus solution is installed. Not having a functioning antivirus application installed on endpoints could pose a danger to the organization. Tenable has a number of plugins that check for antivirus solutions:

- [24232](#) BitDefender Check
- [20284](#) Kaspersky Anti-Virus Check
- [12107](#) McAfee Anti Virus Check
- And more

Additionally, plugin [16193](#) Antivirus Software Check aggregates the results from other plugins if multiple applications are installed. Plugin 16193 also reports hosts that do not have an antivirus solution installed. Output from the plugin shows anti-malware products, versions of the signature files, and information regarding if the signatures are out of date. This helps organizations meet sub-control 8.2.



## Plugin Output

Forefront\_Endpoint\_Protection :

A Microsoft anti-malware product is installed on the remote host :

|                               |   |
|-------------------------------|---|
| Product name                  | : Microsoft Security Client                   |
| Path                          | : c:\Program Files\Microsoft Security Client\ |
| Version                       | : 4.10.0209.0                                 |
| Engine version                | : 1.1.16100.4                                 |
| Antivirus signature version   | : 1.297.600.0                                 |
| Antispyware signature version | : 1.297.600.0                                 |

The antivirus signatures are out of date. The last known updated version from the vendor is : 1.305.1053.0

The antispyware signatures are out of date. The last known updated version from the vendor is : 1.305.1053.0



## 8.2: Ensure Anti-Malware Software and Signatures Are Updated

Sub-control 8.2 states that you must ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.

| Asset Type | Security Function | Implementation Groups |
|------------|-------------------|-----------------------|
| Devices    | Protect           | 1, 2, 3               |

### Dependencies

- Sub-control 1.4: Integrate Software and Hardware Asset Inventories
- Sub-control 2.1: Maintain Inventory of Authorized Software
- Sub-control 2.4: Track Software Inventory Information

### Inputs

1. **Endpoint Inventory:** The endpoint inventory. Update the record for each endpoint to indicate whether that endpoint can support anti-malware software or not (sub-control 1.4).
2. **Anti-malware software version information:** A list of acceptable versions for the scanning engines and the signature databases for any anti-malware products in use on endpoints in I1. This version information needs to be updated frequently to reflect current version information and age off outdated versions. Reference the ASL per sub-control 2.1. and ideally leverage the software inventory in sub-control 2.4)
3. **Software update time limit:** The maximum time allowed for anti-malware software updates to be applied to endpoints.

### Assumptions

- Some endpoints, such as network devices, may not support anti-malware software. Whether an endpoint supports anti-malware software is provided as part of I1. Devices that cannot support anti-malware software are removed from the list of endpoints to be checked during Operation 1, and these devices are not counted in the metric below.

### Operations



1. Refine the endpoint inventory (I1) to only contain endpoints that can support anti-malware software. This reduced list of endpoints becomes M1.
2. For each endpoint in M1, generate a list of those endpoints that have an acceptable version of anti-malware software installed and enabled (both scanning engine and signature database) according to the information provided in I2 (M2). Then, generate a list of those endpoints that do not have an acceptable version of anti-malware software installed and enabled (M3).
3. For each endpoint in M1, generate a list of those endpoints that have been updated within the time frame specified by I3 (M4), and a list of those endpoints that have not been updated within that time-frame (M5).

## Measures

| Measure   | Definition  |
|---|---|
| M1 = List of endpoints capable of supporting anti-malware software  | A list of all endpoints that have anti-malware software installed.  |
| M2 = List of endpoints with an acceptable version of anti-malware software installed and enabled (version compliant list)                 | A list of endpoints that have supported versions of anti-malware (and definitions) that are installed and current.        |
| M3 = List of endpoints that do not have an acceptable version of anti-malware software installed and enabled (version non-compliant list) | A list of endpoints that do not have supported versions of anti-malware (and definitions) that are installed and current. |
| M4 = List of endpoints that have had their anti-malware software updated within the specified time-frame (time compliant list)            | A list of endpoints that have had their anti-malware software updated within the specified time-frame.                    |
| M5 = List of endpoints that have not had their anti-malware software updated within the specified time-frame (time compliant list)        | A list of endpoints that have not had their anti-malware software updated within the specified time-frame.                |
| M6 = Count of items in M1   | A count of the total number of items in M1.   |
| M7 = Count of items in M2   | A count of the total number of items in M2.   |



|                            |   |
|----------------------------|---|
| M8 = Count of items in M3  | A count of the total number of items in M3. |
| M9 = Count of items in M4  | A count of the total number of items in M4. |
| M10 = Count of items in M5 | A count of the total number of items in M5. |

## Metrics

### Coverage

| Metric  | Calculation |
|---|-------------|
| The ratio of anti-malware software version compliant endpoints compared to the total number of endpoints capable of supporting anti-malware software. | $M7 / M9$   |

### Freshness

| Metric  | Calculation |
|---|-------------|
| The ratio of endpoints whose anti-malware software has been updated within the specified timeframe. | $M9 / M6$   |

**Note:** Comparing the coverage metric to the freshness metric can serve as a useful check – for instance, if the coverage metric tends to be high, while the freshness metric is low, that would suggest that I2 might not have been updated recently enough (that is, outdated versions are being considered acceptable).



## 8.4: Configure Anti-Malware Scanning of Removable Media

Sub-control 8.4 states that you must configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.

| Asset Type | Security Function | Implementation Groups |
|------------|-------------------|-----------------------|
| Devices    | Detect            | 1, 2, 3               |

### Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 5.1: Establish Secure Configurations

### Inputs

1. **Endpoint Inventory:** The endpoint inventory with an entry for each endpoint indicating whether or not that endpoint can support anti-malware software or not.
2. **Desired anti-malware configuration:** The desired configuration to automatically scan removable media when inserted/connected.

### Assumptions

- Some endpoints, such as network devices, may not support anti-malware software. Whether an endpoint supports anti-malware software is provided as part of I1. Devices that cannot support anti-malware software are removed from the list of endpoints to be checked during Operation 1, and these devices are not counted in the metric below.

### Operations

1. Refine the endpoint inventory (I1) to only contain endpoints that can support anti-malware software endpoint inventory. This reduced list of endpoints becomes M1.
2. Of the set of endpoints that can support anti-malware software (M1), generate a list of those endpoints that actually have anti-malware software installed, enabled, and adhere to the configuration specified in I2 (M2). Then, generate a list of the endpoints that do not adhere to the





specified configuration (M3). Note: Endpoints in M1 that do not have anti-malware installed and enabled, are considered non-compliant and added to M3.

## Measures

| Measure   | Definition   |
|---|--|
| M1 = List of endpoints capable of supporting anti-malware software  | A list of all endpoints that have anti-malware software installed.   |
| M2 = List of endpoints with an acceptable version of anti-malware software installed, enabled, and properly configured to scan removable media (compliant list) | A list of endpoints that have supported versions of anti-malware that are installed, enabled, and properly configured to scan removable media. |
| M3 = List of endpoints not adhering to the specified configuration (non-compliant list)   | A list of endpoints that do not adhere to the specified configuration.   |
| M4 = Count of items in M1   | A count of the total number of items in M1.  |
| M5 = Count of items in M2   | A count of the total number of items in M2.  |
| M6 = Count of items in M3   | A count of the total number of items in M3.  |

## Metrics

### Coverage

| Metric   | Calculation |
|--|-------------|
| The ratio of endpoints that are compliant with the desired anti-malware configuration compared to the total number of endpoints capable of supporting anti-malware software. | $M5 / M4$   |



## 8.5: Configure Devices to Not Auto-Run Content

Sub-control 8.5 states that you must configure devices to not auto-run content from removable media.

| Asset Type | Security Function | Implementation Groups |
|------------|-------------------|-----------------------|
| Devices    | Protect           | 1, 2, 3               |

### Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 5.1: Establish Secure Configurations

### Inputs

1. **Endpoint Inventory:** The endpoint inventory.
2. **Desired configuration(s) to disable auto-run:** The desired configuration to use to disable auto-running content. There may be multiple configurations targeted at different types of endpoints (for instance, a different configuration might be provided for each type of operating system used on the endpoints in the provided inventory). If the endpoints are capable of performing multiple types of auto-run behavior (i.e., auto-run vs. auto-play), appropriate configurations should be provided for each type.

### Operations

1. For each endpoint in I1, compare the endpoint's configuration to the appropriate configuration from I2. Generate a list of endpoints that adhere to the specified configuration (M1) and a list of the endpoints that do not adhere to the specified configuration (M2).

### Assumptions

- Endpoints that are not capable of performing any type of auto-run behavior are included in the compliant list (M1).

### Measures



| Measure   | Definition   |
|---|--|
| M1 = List of endpoints adhering to the specified configuration (compliant list)         | A list of all endpoints that adhere to the specified configuration.    |
| M2 = List of endpoints not adhering to the specified configuration (non-compliant list) | A list of endpoints that do not adhere to the specified configuration. |
| M3 = Count of items in M1   | A count of the total number of items in M1.                            |
| M4 = Count of items in M2   | A count of the total number of items in M2.                            |
| M5 = Count of items in I1   | A count of the total number of items in I1.                            |

## Metrics

### Coverage

| Metric  | Calculation |
|---|-------------|
| The ratio of endpoints properly disabling auto-run compared to the total number of endpoints. | $M3 / M5$   |



---

## CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services

---

The focus of this control is to manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers. A common denominator is that attackers will always search for, and attempt to exploit, accessible and vulnerable network services. The most common attacks are generally against hosts such as web servers, mail servers, file and printer servers, etc.

The CIS states this Control is critical:

*“Attackers search for remotely accessible network services that are vulnerable to exploitation. Common examples include poorly configured web servers, mail servers, file and print services, and DNS servers installed by default on a variety of different device types, often without a business need for the given service. Many software packages automatically install services and turn them on as part of the installation of the main software package without informing a user or administrator that the services have been enabled. Attackers scan for such services and attempt to exploit these services, often attempting to exploit default user IDs and passwords or widely available exploitation code.”*

The journey of implementing the Foundational CIS Controls continues with CIS Control 9 Limitation and Control of Network Ports, Protocols, and Services. The full CIS 9 Control evolves around organizations ensuring that only those ports, protocols, and services with a validated business requirement are open/running on each system. Organizations are also directed to perform automated scans on a regular basis against all systems to ensure that unauthorized ports/services are detected. The specific sub-controls that are part of Implementation Group 1 (IG1) are:

- 9.4 Apply Host-Based Firewalls or Port-Filtering



## CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services

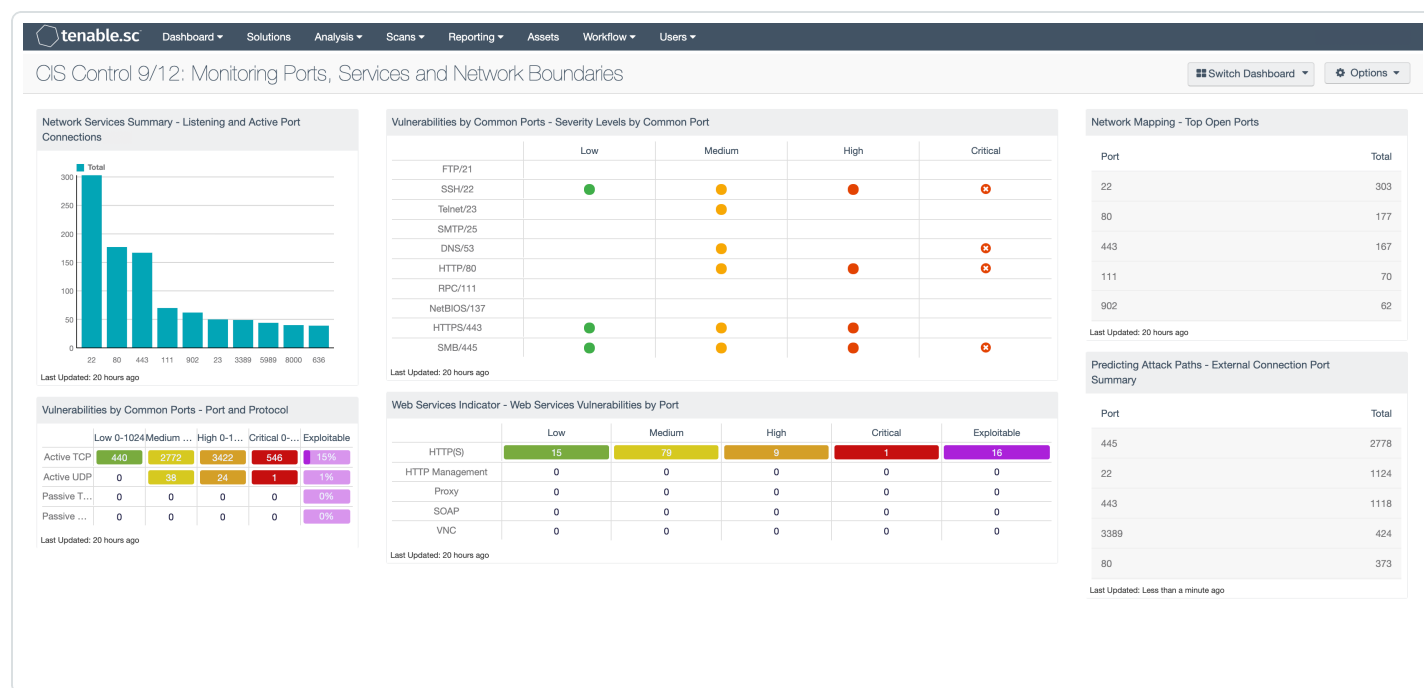
| Sub-Control | Asset Type | Security Function | Control Title  | Control Descriptions  | Implementation Groups |   |   |
|-------------|------------|-------------------|--|---|-----------------------|---|---|
|             |            |                   |  |   | 1                     | 2 | 3 |
| 9.1         | Devices    | Identify          | Associate Active Ports, Services, and Protocols to Asset Inventory | Associate active ports, services, and protocols to the hardware assets in the asset inventory.  |                       |   |   |
| 9.2         | Devices    | Protect           | Ensure Only Approved Ports, Protocols, and Services Are Running    | Ensure that only network ports, protocols, and services listening on a system with validated business needs are running on each system.   |                       |   |   |
| 9.3         | Devices    | Detect            | Perform Regular Automated Port Scans                               | Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.   |                       |   |   |
| 9.4         | Devices    | Protect           | Apply Host-Based Firewalls or Port-Filtering                       | Apply host-based firewalls or port-filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed. |                       |   |   |
| 9.5         | Devices    | Protect           | Implement Application Firewalls                                    | Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.     |                       |   |   |



## Preface on Sub-Control 9.4

The CIS recommends that to meet the requirements for IG1, organizations should at a minimum apply host-based firewalls or port-filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed. For CIS Control 9, Tenable products allow security operations teams to use Tenable Security Center Continuous View to analyze endpoints and check firewall configurations, as well as track open ports and services.

To further assist organizations the CIS Control 9/12, the "Monitoring Ports, Services and Network Boundaries" dashboard focuses on the tracking of active ports, services, and protocols. Tenable Security Center is able to routinely scan the network for open ports and services. Nessus scanners are capable of scanning internal and external assets on the network. Tenable Security Center can also use passive detection to find systems that are communicating with the internal network from external or untrusted devices.



For more information about the CIS Control 9 dashboard, see [CIS Control 9/12: Monitoring Ports, Services and Network Boundaries](#).

There are a variety of methods that can be employed to assist organizations with port filtering, or determining if host-based firewalls are in use. Nessus has a variety of scanning methods to detect open ports and services. The Nessus SYN scanner, plugin ID [11219](#), is less intrusive and behaves differently by simplifying the scanning process. The scanner sends packets and waits for a response,



but does not initiate the full three-way handshake. It does not open sockets, but generates raw packets using low-level libraries.

Info

## Nessus SYN scanner (11219)

### Synopsis

It is possible to determine which TCP ports are open.

### Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

### Solution

Protect your target with an IP filter.

### Plugin Output

```
Port 3389/tcp was found to be open
```

Organizations can benefit from also using the following plugins, such as plugin [34220](#), which uses the WMI interface to run 'netstat' on the remote host to enumerate the open ports.



Info

## Netstat Portscanner (WMI) (34220)

### Synopsis

Remote open ports can be enumerated via WMI.

### Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

### See Also

#### Links:

[wikipedia.org](https://www.wikipedia.org) 

### Plugin Output

```
Port 3389/tcp was found to be open
```

Plugin [34252](#) Microsoft Remote Listeners Enumeration (WMI), can be used to obtain the names of processes listening on UDP and TCP ports.





Info

## Microsoft Windows Remote Listeners Enumeration (WMI) (34252)

### Synopsis

It is possible to obtain the names of processes listening on the remote UDP and TCP ports.

### Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

### Plugin Output

```
The Win32 process 'svchost.exe' is listening on this port (pid 988).  
  
This process 'svchost.exe' (pid 988) is hosting the following Windows services :  
TermService (@%SystemRoot%\System32\termsrv.dll,-268)
```

As related to sub-control 9.4, there are several plugins available, such as plugin ID [45052](#) WMI Firewall enumeration, which allows Nessus to use WMI to enumerate third party firewall software installed on the host. Also, using plugin 20811, Microsoft Windows Software Enumeration and a vulnerability text of “Windows Firewall” can assist in determining if the application is installed on the target host.

### Plugin Output

```
The following software are installed on the remote host :  
  
System Center Endpoint Protection [version 4.10.209.0] [installed on  
2017/04/20]  
Mozilla Firefox 76.0 (x86 en-US) [version 76.0]  
Notepad++ (64-bit x64) [version 7.8.6]  
Microsoft Office Professional Plus 2016 [version 16.0.4266.1001]  
Windows Firewall Configuration Provider [version 1.2.3412.0] [installed on  
2017/04/20]  
Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005 [version 12.0.21005]  
[installed on 2017/04/20]  
Update for Windows 10 for x64-based Systems (KB4023057) [version 2.9.0.0]  
[installed on 2018/01/11]  
Configuration Manager Client [version 5.00.8458.1000] [installed on  
2018/01/14]
```



## 9.4: Apply Host-Based Firewalls or Port-Filtering

Sub-control 9.4 states that you must apply host-based firewalls or port-filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

| Asset Type | Security Function | Implementation Groups |
|------------|-------------------|-----------------------|
| Devices    | Protect           | 1, 2, 3               |

### Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information

### Inputs

1. **Endpoint Inventory:** The endpoints that are able to scan, and therefore assumed capable of hosting firewall/port-filtering software.
2. **Policy:** A policy (or set of policies, potentially individually per endpoint) indicating which ports are allowed to be open.

### Operations

1. For each endpoint, retrieve the firewall policy.
2. For each firewall policy, enumerate both the ports which allow communication, and any configuration of a default deny rule (could that be a default?), noting along the way which policies are configured appropriately or inappropriately.

### Measures

| Measure                   | Definition                                  |
|---------------------------|---|
| M1 = List of endpoints    | A list of all endpoints.                    |
| M2 = Count of items in M1 | A count of the total number of items in M1. |



|  |   |
|--|---|
| M3 = List of endpoints with appropriately configured firewall ports policy     | A list of endpoints that have an appropriately configured firewall ports policy.        |
| M4 = Count of items in M3  | A count of the total number of items in M3.   |
| M5 = List of endpoints with inappropriately configured firewall ports policy   | A list of endpoints that do not have an appropriately configured firewall ports policy. |
| M6 = Count of items in M5  | A count of the total number of items in M5.   |
| M7 = List of endpoints with appropriately configured default deny rule         | A list of endpoints that have an appropriately configured default deny rule.            |
| M8 = Count of items in M7  | A count of the total number of items in M7.   |
| M9 = List of endpoints with inappropriately configured default deny rule       | A list of endpoints that do not have an appropriately configured default deny rule.     |
| M10 = Count of items in M9   | A count of the total number of items in M9.   |
| M11 = List of endpoints with both appropriately configured firewall policy     | A list of endpoints with both an appropriately configured firewall policy.              |
| M12 = Count of items in M11  | A count of the total number of items in M11.  |
| M13 = List of endpoints with at least one inappropriate firewall configuration | A list of all endpoints with at least one inappropriate firewall configuration.         |
| M14 = Count of items in M13  | A count of the total number of items in M13.  |

## Metrics

### Coverage

| Metric   | Calculation |
|--|-------------|
| The ratio of correctly configured endpoints compared to the total number of endpoints. | $M14 / M2$  |



---

## CIS Control 10: Data Recovery Capabilities

---

The focus of this control is to ensure that the processes and tools used to properly back up critical information are in place within the organization and a proven methodology for timely recovery of data exists.

The CIS states this Control is critical:

*“When attackers compromise machines, they often make significant changes to configurations and software. Sometimes attackers also make subtle alterations of data stored on compromised machines, potentially jeopardizing organizational effectiveness with polluted information. When the attackers are discovered, it can be extremely difficult for organizations without a trustworthy data recovery capability to remove all aspects of the attacker’s presence on the machine.”*

The journey of implementing the CIS Controls continues with data recovery capabilities. This control addresses the importance of backing-up and protecting an organization's system data. Organizations which implement sound data backup strategies ensure their ability to recover lost data or data that has been tampered-with quickly and efficiently. Properly archiving key system data, periodic integrity testing, and having at least one offline backup destination are all crucial in restoring systems and resuming service with the least amount of downtime. This control helps to guide the organization through this review process. The four specific sub-controls that are part of Implementation Group 1 (IG1) are:

- 10.1: Ensure Regular Automated Backups
- 10.2: Perform Complete System Backups
- 10.4: Protect Backups
- 10.5: Ensure All Backups Have at Least One Offline Backup Destination



## CIS Control 10: Data Recovery Capabilities

| Sub-Control | Asset Type | Security Function | Control Title   | Control Descriptions   | Implementation Groups |   |   |
|-------------|------------|-------------------|---|--|-----------------------|---|---|
|             |            |                   |   |  | 1                     | 2 | 3 |
| 10.1        | Data       | Protect           | Ensure Regular Automated Backups                                | Ensure that all system data is automatically backed up on a regular basis.   |                       |   |   |
| 10.2        | Data       | Protect           | Perform Complete System Backups                                 | Ensure that all of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.                               |                       |   |   |
| 10.3        | Data       | Protect           | Test Data on Backup Media                                       | Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.   |                       |   |   |
| 10.4        | Data       | Protect           | Protect Backups   | Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services. |                       |   |   |
| 10.5        | Data       | Protect           | Ensure All Backups Have at Least One Offline Backup Destination | Ensure that all backups have at least one offline (i.e., not accessible via a network connection) backup destination.  |                       |   |   |

The organization should take their time during this process, being sure to review all the back-up policies and conduct integrity tests on randomly selected backups, at random intervals. Tenable Security Center can assist in some areas as there are many active plugins such as 20175 Veritas Backup Agent Detection, and passive detections such as 6575 Carbonite 'Cloud' Backup Service User-Agent Detection that can assist in determining if back-up software/services are detected. Using previous methods, plugin 20811 Windows Software Enumeration can be used to determine if any backup client is installed on endpoints. However, most of the work within this CIS control comes from testing and validation tasks.

### Info

## Microsoft Windows Installed Software Enumeration (credentialed check) (20811)

[Launch Remediation Scan](#)

```
swmsm [version 12.0.0.1] [installed on 2016/05/03]
Dell Digital Delivery [version 3.1.1002.0] [installed on 2016/03/17]
Apple Mobile Device Support [version 13.0.0.38] [installed on 2019/09/17]
Backup and Sync from Google [version 3.45.5545.5747] [installed on 2019/07/03]
MSXML 4.0 SP2 (KB954430) [version 4.20.9870.0] [installed on 2016/06/16]
Microsoft Silverlight [version 5.1.50918.0] [installed on 2019/01/29]
Slack Machine-Wide [version 4.0.0.0] [installed on 2019/07/27]
Security Update for Microsoft Office 2016 (KB3114690) 32-Bit Edition
Update for Microsoft Office 2016 (KB2920712) 32-Bit Edition
Update for Microsoft Office 2016 (KB3141456) 32-Bit Edition
Update for Microsoft Project 2016 (KB4484345) 32-Bit Edition
Update for Microsoft Office 2016 (KB3115001) 32-Bit Edition
Update for Microsoft Office 2016 (KB2920717) 32-Bit Edition
```



As shown above, using Nessus plugin [20811](#) to enumerate installed software on an endpoint, we are able to determine that a cloud backup solution is installed. However, you must manually test and validate the process.



## 10.1: Ensure Regular Automated Backups

Sub-control 10.1 states that you must ensure that all system data is automatically backed up on a regular basis.

| Asset Type | Security Function | Implementation Groups |
|------------|-------------------|-----------------------|
| Data       | Protect           | 1, 2, 3               |

### Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 5.1: Establish Secure Configurations

### Inputs

1. **Endpoint Inventory:** Inventory of all endpoints.
2. **Backup configuration policy:** Show the backup configuration policy is available.
3. **Backup software:** Show the backup software (either OS or 3d party) configuration is available and able to be queried.
4. **Backup logs:** Show the backup software logs are available and can be queried
5. **Backup staleness threshold:** A successful backup staleness threshold is defined. This indicates the maximum time period allowed between backups. The CIS recommends this occur at least weekly.

### Operations

1. For each endpoint, examine its backup configuration with the available configuration policy. Note appropriately configured and inappropriately configured endpoints. Then, examine its logs to determine the most recent successful backup completion time. Note whether it was run within the enterprise-defined staleness threshold.



2. Enumerate the endpoints that are both appropriately configured and that do not have stale backups.
3. Compare an endpoint's backup configuration with available configuration policy.
4. Interrogate logs to determine most recent successful backup completion time.

## Measures

| Measure   | Definition   |
|---|--|
| M1 = List of endpoints  | A list of all endpoints.   |
| M2 = Count of items in M1   | A count of the total number of items in M1.  |
| M3 = List of appropriately configured endpoints                                   | A list of endpoints that are configured correctly.   |
| M4 = Count of items in M3   | A count of the total number of items in M3.  |
| M5 = List of inappropriately configured endpoints                                 | A list of endpoints that are configured incorrectly.   |
| M6 = Count of items in M5   | A count of the total number of items in M5.  |
| M7= List of endpoints both appropriately configured and without stale backups     | A list of all endpoints that are both configured correctly and also do not have any stale backups. |
| M8 = Count of items in M7   | A count of the total number of items in M7.  |
| M9 = List of endpoints either inappropriately configured or without stale backups | A list of endpoints that are configured incorrectly or that do not have any stale backups.         |
| M10 = Count of items in M9  | A count of the total number of items in M9.  |

## Metrics

### Coverage

| Metric | Calculation |
|--------|-------------|
|--------|-------------|





The percentage of endpoints that are successfully backing up system data on a regular basis.

M8 / M2



## 10.2: Perform Complete System Backups

Sub-control 10.2 states that you must ensure that all of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.

| Asset Type | Security Function | Implementation Groups |
|------------|-------------------|-----------------------|
| Data       | Protect           | 1, 2, 3               |

### Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 5.1: Establish Secure Configurations

### Inputs

1. **Key Systems:** The list of "key systems" identified by the organization, as derived from the end-point inventory (sub-control 1.4).
2. **Backup configuration policy:** The organization's backup/imaging configuration policy.

### Assumptions

- Backup software (either OS or 3d party) is installed and appropriately configured on the "key systems" identified in I1.

### Operations

1. For each endpoint in the list of "key systems", examine its backup configuration against the available backup configuration policy. Note which endpoints are configured appropriately and inappropriately.

### Measures

| Measure | Definition |
|---------|------------|
|---------|------------|



|   |  |
|---|--|
| M1 = List of "key system" endpoints                   | A list of "key system" endpoints.                        |
| M2 = Count of items in M1                             | A count of the total number of items in M1.              |
| M3 = List of appropriately configured "key systems"   | A list of "key systems" that are configured correctly.   |
| M4 = Count of items in M3                             | A count of the total number of items in M3.              |
| M5 = List of inappropriately configured "key systems" | A list of "key systems" that are configured incorrectly. |
| M6 = Count of items in M5                             | A count of the total number of items in M5.              |

## Metrics

### Coverage

| Metric  | Calculation |
|---|-------------|
| The percentage of key systems that are successfully backed up as a complete system. | $M4 / M2$   |



## 10.4: Protect Backups

Sub-control 10.4 states that you must ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.

| Asset Type | Security Function | Implementation Groups |
|------------|-------------------|-----------------------|
| Data       | Protect           | 1, 2, 3               |

### Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 5.1: Establish Secure Configurations

### Inputs

1. **Endpoint inventory:** The list of endpoints configured for periodic backup, derived from the endpoint inventory (sub-control 1.4).
2. **Backup configuration policy:** The organization's backup configuration policy.

### Assumptions

- Backup software (either OS or 3d party) is installed and appropriately configured on endpoints identified in I1.

### Operations

1. Interrogate the organization's backup configuration policy to determine if backups are configured to be encrypted.
2. For each endpoint, examine its backup configuration policy to ensure that encrypted backups are configured. Note which endpoints are configured appropriately and inappropriately.

### Measures



| Measure   | Definition   |
|---|--|
| M1 = List of endpoints                            | A list of endpoints.                                 |
| M2 = Count of items in M1                         | A count of the total number of items in M1.          |
| M3 = List of appropriately configured endpoints   | A list of endpoints that are configured correctly.   |
| M4 = Count of items in M3                         | A count of the total number of items in M3.          |
| M5 = List of inappropriately configured endpoints | A list of endpoints that are configured incorrectly. |
| M6 = Count of items in M5                         | A count of the total number of items in M5.          |

## Metrics

### Coverage

| Metric   | Calculation |
|--|-------------|
| The percentage of backups that are protected via physical security/encryption. | $M6 / M2$   |



## 10.5: Ensure All Backups Have at Least One Offline Backup Destination

Sub-control 10.5 states that you must ensure that all backups have at least one offline (i.e., not accessible via a network connection) backup destination.

| Asset Type | Security Function | Implementation Groups |
|------------|-------------------|-----------------------|
| Data       | Protect           | 1, 2, 3               |

### Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 5.1: Establish Secure Configurations

### Inputs

1. **Endpoint Inventory:** A list of endpoints.
2. **Backup configuration policy:** The backup configuration policy, assuming the inclusion of “off-line” backup destinations.

### Operations

1. Collect a list of endpoints that do/do not match the policy specified in I2.

### Measures

| Measure                                | Definition                                  |
|--|---|
| M1 = List of endpoints                 | A list of endpoints.                        |
| M2 = Count of items in M1              | A count of the total number of items in M1. |
| M3 = List of endpoints matching policy | A list of endpoints that match the policy.  |
| M4 = Count of items in M3              | A count of the total number of items in M3. |



|  |   |
|--|---|
| M5 = List of endpoints not matching policy | A list of endpoints that do not match the policy. |
| M6 = Count of items in M5                  | A count of the total number of items in M5.       |

## Metrics

### Coverage

| Metric   | Calculation |
|--|-------------|
| The ratio of endpoints matching the backup configuration policy compared to the total number of endpoints. | $M4 / M2$   |

### Lack of Coverage

| Metric   | Calculation |
|--|-------------|
| The ratio of endpoints not matching the backup configuration policy compared to the total number of endpoints. | $M5 / M2$   |



## CIS Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches

The focus of this control is to establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

The CIS states this Control is critical:

*"As delivered from manufacturers and resellers, the default configurations for network infrastructure devices are geared for ease-of-deployment and ease-of-use – not security. Open services and ports, default accounts (including service accounts) or passwords, support for older (vulnerable) protocols, pre-installation of unneeded software; all can be exploitable in their default state. The management of the secure configurations for networking devices is not a one-time event, but a process that involves regularly re-evaluating not only the configuration items but also the allowed traffic flows. Attackers take advantage of network devices becoming less securely configured over time as users demand exceptions for specific business needs. Sometimes the exceptions are deployed and then left undone when they are no longer applicable to the business needs. In some cases, the security risk of the exception is neither properly analyzed nor measured against the associated business need and can change over time.*

*Attackers search for vulnerable default settings, gaps or inconsistencies in firewall rule sets, routers, and switches and use those holes to penetrate defenses. They exploit flaws in these devices to gain access to networks, redirect traffic on a network, and intercept information while in transmission. Through such actions, the attacker gains access to sensitive data, alters important information, or even uses a compromised machine to pose as another trusted system on the network."*
















The journey of implementing the CIS Controls, continues with CIS Control 11: Secure Configuration for network devices, such as Firewalls, Routers, and Switches. Organizations are directed to review the configuration of all network devices against approved configurations. Organizations should record and mitigate any deviation. Organizations are also directed to establish a rigorous configuration management program and change control process in order to prevent attackers from exploiting network device vulnerabilities.

The specific sub-controls that are part of Implementation Group 1 (IG1) are:



- [11.4 Install the latest stable version of any security-related updates on all network devices](#)

### CIS Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches

| Sub-Control | Asset Type | Security Function | Control Title  | Control Descriptions  | Implementation Groups   |   |   |
|-------------|------------|-------------------|--|---|---|---|---|
|             |            |                   |  |   | 1   | 2   | 3   |
| 11.1        | Network    | Identify          | Maintain Standard Security Configurations for Network Devices                            | Maintain documented security configuration standards for all authorized network devices.  |   |    |    |
| 11.2        | Network    | Identify          | Document Traffic Configuration Rules   | All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.                                    |   |    |    |
| 11.3        | Network    | Detect            | Use Automated Tools to Verify Standard Device Configurations and Detect Changes          | Compare all network device configurations against approved security configurations defined for each network device in use, and alert when any deviations are discovered.  |   |    |    |
| 11.4        | Network    | Protect           | Install the Latest Stable Version of Any Security-Related Updates on All Network Devices | Install the latest stable version of any security-related updates on all network devices.   |  |    |    |
| 11.5        | Network    | Protect           | Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions          | Manage all network devices using multi-factor authentication and encrypted sessions.  |   |   |   |
| 11.6        | Network    | Protect           | Use Dedicated Workstations for All Network Administrative Tasks                          | Ensure network engineers use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be segmented from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading email, composing documents, or surfing the Internet. |   |  |  |
| 11.7        | Network    | Protect           | Manage Network Infrastructure Through a Dedicated Network                                | Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.   |   |  |  |

For CIS Control 11, Tenable products allow the organization to actively and passively discover network devices and software. Using the same methods as discussed in Control 1 and Control 2, active scanning allows for network device mapping and software enumeration. Devices identified in Control 1 as network devices, firewalls, routers, and switches must be used as a reference for this control. Software versions that were enumerated in Control 2 are also required. Both of these efforts contribute greatly to this control.

To further assist organizations with CIS Control 11: Secure Network Devices, the dashboard focuses on the compliance summary of network devices. Tenable Security Center is able to routinely scan



the network for network devices and enumerate installed software, extracting software, vendor, and version information. Nessus scanners are capable of scanning internal and external assets to map out network devices. Tenable Security Center can also use passive detection to discover network devices that are not being scanned.





## Preface on Sub-Control 11.4

Tenable Security Center provides innovative ways to find vulnerabilities for network devices using different attributes, such as the Common Platform Enumeration (CPE). Tenable Security Center uses CPE strings “bluecoat, brocade, check\_point, checkpoint, cisco, citrix, dell, f5, fortinet, hp, hua-wei, juniper, netapp, netgear, paloaltonetworks, pfsense, sonicwall, ssh, veritas, vmware, websense” to locate vulnerabilities that are likely related to network devices. These vulnerabilities help support CIS sub control 11.4: Install the Latest Stable Version of Any Security Related Updates on All Network Devices. Components include trend lines which are calculated over 3 months, and that use the Last Observed Filter set to “Within the Last Day”. This allows analysts to track changes from one day to the next, showing a more accurate change. If scans are run weekly, then a user should modify the field to 7 days, so the change from scan to scan is accurately measured.

The ultimate goal of this sub-control is to have a score (or ratio) of zero (The number of network devices all have up to date software versions, i.e., there are no missing patches/updates). Using this method, we can easily identify unsupported versions of software on network devices. The following example from pluginID 55933 Juniper Junos Unsupported Version Detection uses the above listed filters as a base query.

### Plugin Output

```
Installed version      : 15.1X53-D58.3
Junos release         : 15.1X53
End of life date      : 2018-12-05
End of extended support date : 2019-05-05
EOE and EOS URL       : http://www.juniper.net/support/eol/junos.html
```



## 11.4: Install the Latest Stable Version of Any Security-Related Updates on All Network Devices

Sub-control 11.4 states that you must ensure that all system data is automatically backed up on a regular basis.

| Asset Type | Security Function | Implementation Groups |
|------------|-------------------|-----------------------|
| Network    | Protect           | 1, 2, 3               |

### Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information

### Inputs

1. **Network device inventory:** The network device inventory, derived from the endpoint inventory (sub-control 1.4).
2. **Network device version information:** A list of acceptable versions for each model of network device in I1. This version information needs to be updated frequently to reflect current version information and age off outdated versions.

### Operations

1. For each network device in I1, compare the network device's version to the allowable versions from I2.
2. Generate a list of those network devices that match an allowable version (M1).
3. Generate a list of those network devices that do not match an allowable version (M2).

### Measures

| Measure                      | Definition                 |
|------------------------------|----------------------------|
| M1 = List of network devices | A list of network devices. |



|  |   |
|--|---|
| M2 = Count of items in M1  | A count of the total number of items in M1.                       |
| M3 = List of network devices that match an allowable version (compliant list)            | A list of network devices that match an allowable version.        |
| M4 = Count of items in M3  | A count of the total number of items in M3.                       |
| M5 = List of network devices that do not match an allowable version (non-compliant list) | A list of network devices that do not match an allowable version. |
| M6 = Count of items in M5  | A count of the total number of items in M5.                       |

## Metrics

### Coverage

| Metric   | Calculation                                |
|--|--|
| The percentage of inventoried network devices that match the allowable version for that device/OS. | If $M2 > 0$ , then $M4 / M2$ ; otherwise 0 |



## CIS Control 12: Boundary Defense

The focus of this control is to ensure that the entry points into the network are clearly defined and monitored. Network boundaries in today's environment do not have a clear edge, and are typically no longer defined as a single ingress point protected by a firewall and edge routers of the past. Today, the network perimeter extends well beyond this gateway into the organization, and encompasses the cloud when using AWS, ASURE, or other services. A network edge is also the reach of a wireless network radio signal, and the VPN endpoints with more users working at home. This CISO must have a clear understanding of each network edge and the risks associated with each edge.

The CIS states this Control is critical:

*"Attackers focus on exploiting systems that they can reach across the Internet, including not only DMZ systems but also workstations and laptop computers that pull content from the Internet through network boundaries. Threats such as organized crime groups and nation-states use configuration and architectural weaknesses found on perimeter systems, network devices, and Internet-accessing client machines to gain initial access into an organization. Then, with a base of operations on these machines, attackers often pivot to get deeper inside the boundary to steal or change information or to set up a persistent presence for later attacks against internal hosts. Additionally, many attacks occur between business partner networks, sometimes referred to as extranets, as attackers hop from one organization's network to another, exploiting vulnerable systems on extranet perimeters."*

The journey of implementing the CIS Controls continues with understanding the boundaries of a the network and defining how access should be controlled. Organizations are directed to deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed. The two specific sub-controls that are part of Implementation Group 1 (IG1) are:

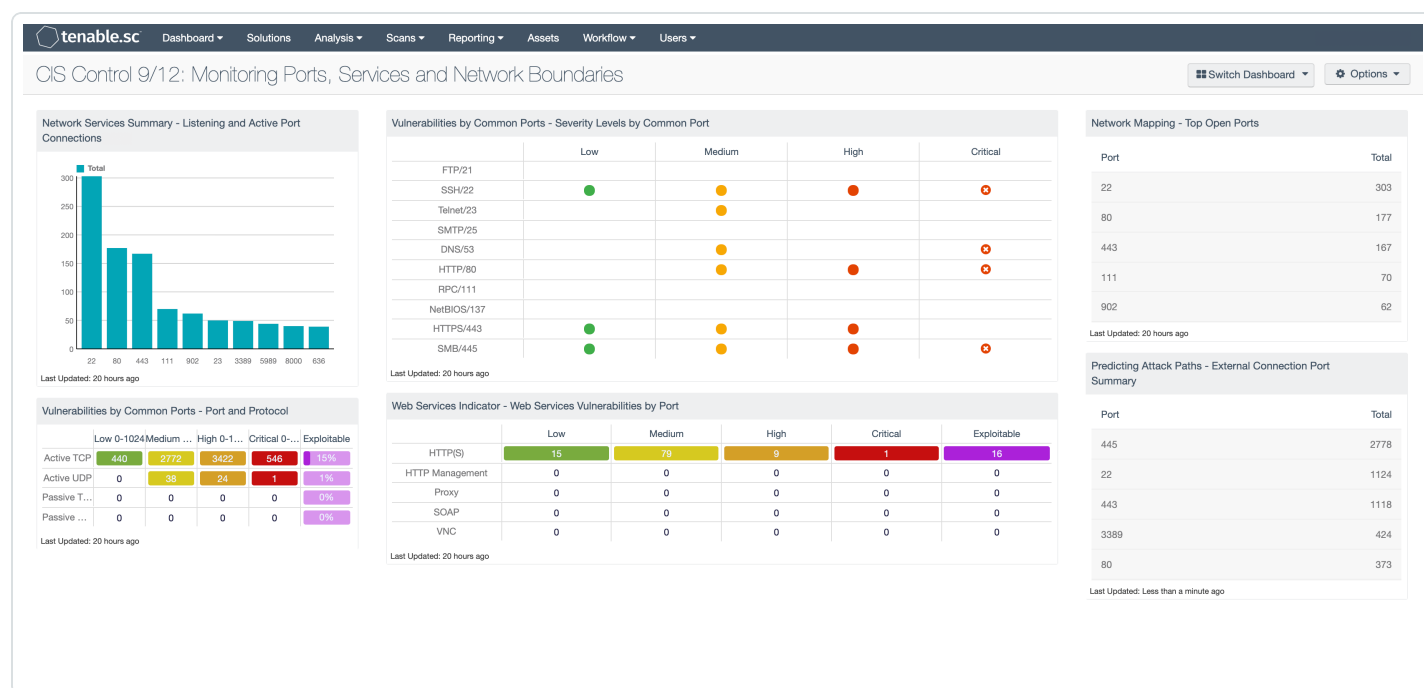
- [12.1: Maintain an Inventory of Network Boundaries](#)
- [12.4: Deny Communication Over Unauthorized Ports](#)

For CIS Control 12, Tenable products allow the organization to actively and passively discover networks. Using the same methods as discussed in Control 9, active scanning allows for TCP port enumeration and network mapping efforts. Along with Control 1, network addresses can be discovered and documented. A valuable aid in this process is to use passive scanning around the network to



identify systems that access the network from different locations. Both of these efforts contribute greatly to this control.

To further assist organizations the CIS Control 9/12: Monitoring Ports, the "Services and Network Boundaries" dashboard focuses on the tracking of active ports, services, and protocols. Tenable Security Center is able to routinely scan the network for open ports and services. Nessus scanners are capable of scanning internal and external assets to map out subnets that are in use on the network. Tenable Security Center can also use passive detection to discover subnets that are not being scanned.



<https://www.tenable.com/sc-dashboards/cis-control-912-monitoring-ports-services-and-network-boundaries>

The CAS provides guidance on how to assess the organization's progress in this journey. This guide illustrates how the CISO can effectively measure cybersecurity success. Shown below are the CIS Control 12 IG levels and requirements:



## CIS Control 12: Boundary Defense

| Sub-Control | Asset Type | Security Function | Control Title   | Control Descriptions   | Implementation Groups |   |   |
|-------------|------------|-------------------|---|--|-----------------------|---|---|
|             |            |                   |   |  | 1                     | 2 | 3 |
| 12.1        | Network    | Identify          | Maintain an Inventory of Network Boundaries                         | Maintain an up-to-date inventory of all of the organization's network boundaries.  |                       |   |   |
| 12.2        | Network    | Detect            | Scan for Unauthorized Connections Across Trusted Network Boundaries | Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary.  |                       |   |   |
| 12.3        | Network    | Protect           | Deny Communications With Known Malicious IP Addresses               | Deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges at each of the organization's network boundaries.  |                       |   |   |
| 12.4        | Network    | Protect           | Deny Communication Over Unauthorized Ports                          | Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries. |                       |   |   |
| 12.5        | Network    | Detect            | Configure Monitoring Systems to Record Network Packets              | Configure monitoring systems to record network packets passing through the boundary at each of the organization's network boundaries.  |                       |   |   |
| 12.6        | Network    | Detect            | Deploy Network-Based IDS Sensors                                    | Deploy network-based Intrusion Detection Systems (IDS) sensors to look for unusual attack mechanisms and detect compromise of these systems at each of the organization's network boundaries.  |                       |   |   |
| 12.7        | Network    | Protect           | Deploy Network-Based Intrusion Prevention Systems                   | Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries.   |                       |   |   |
| 12.8        | Network    | Detect            | Deploy NetFlow Collection on Networking Boundary Devices            | Enable the collection of NetFlow and logging data on all network boundary devices.   |                       |   |   |
| 12.9        | Network    | Detect            | Deploy Application Layer Filtering Proxy Server                     | Ensure that all network traffic to or from the Internet passes through an authenticated application layer proxy that is configured to filter unauthorized connections.   |                       |   |   |
| 12.10       | Network    | Detect            | Decrypt Network Traffic at Proxy                                    | Decrypt all encrypted network traffic at the boundary proxy prior to analyzing the content. However, the organization may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.           |                       |   |   |
| 12.11       | Users      | Protect           | Require All Remote Logins to Use Multi-Factor Authentication        | Require all remote login access to the organization's network to encrypt data in transit and use multi-factor authentication.  |                       |   |   |
| 12.12       | Devices    | Protect           | Manage All Devices Remotely Logging Into Internal Network           | Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.     |                       |   |   |





---

## Preface on Sub-Controls 12.1 and 12.4

---

Both of these sub controls are supported by first having a good network discovery process. Tenable Security Center helps customers gain a more accurate understanding of the systems active within their environment. As the systems are identified and the security team moves from the Discover to the Access phase, the team begins to understand what normal is, and gains an understanding of the traffic authorized. At the completion of these two steps, the security team is ready to start progressing in sub control 12.1 and begin taking inventory of all the networks, establishing a baseline of traffic patterns. As the team Analyzes (the third step in the life cycle) the previously collected data, a fundamental pattern should emerge and documentation of authorized traffic will reveal itself.

When documenting the inventory, the organization should consider the follow key items for traffic classification:

- What Classless Inter-Domain Routing (CIDR) boundaries are used, and how do they map to VLAN's?
- Who are the primary users or operators in the subnet or network segment.
- What is the traffic that is normal traffic?
- Are there services running in the network segment?
- Where are the network access controls in relation to the network segment?

As the security team defines each of these questions for each network segment, a network traffic policy will develop. From these set up policies, a clear set of access controls can be defined.



## 12.1: Maintain an Inventory of Network Boundaries

Sub-control 12.1 states that you must maintain an up-to-date inventory of all of the organization's network boundaries.

| Asset Type | Security Function | Implementation Groups |
|------------|-------------------|-----------------------|
| Network    | Identify          | 1, 2, 3               |

### Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information

### Inputs

1. **Device inventory:** An inventory of expected boundary devices (M1) as derived from the end-point inventory (sub-control 1.4).

### Operations

1. Utilize a discovery tool or process to examine the network topology. Then, collect the list of devices that are considered boundary devices (M2).
2. Evaluate the difference between I1 and Operation 1 to get the list of non-inventoried boundary devices (M3).

### Measures

| Measure  | Definition                                     |
|--|--|
| M1 = List of expected network boundary devices   | A list of expected network boundary devices.   |
| M2 = Count of items in M1                        | A count of the total number of items in M1.    |
| M3 = List of discovered network boundary devices | A list of discovered network boundary devices. |



|   |   |
|---|---|
| M4 = Count of items in M3                     | A count of the total number of items in M3. |
| M5 = List of non-inventoried boundary devices | A list of non-inventoried boundary devices. |
| M6 = Count of items in M5                     | A count of the total number of items in M5. |

## Metrics

### Coverage

| Metric   | Calculation |
|--|-------------|
| The ratio of non-inventoried boundary devices compared to expected boundary devices. If the calculated value is greater than zero, the inventory is not current. | $M6 / M2$   |



## 12.4: Deny Communication Over Unauthorized Ports

Sub-control 12.1 states that you must deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.

| Asset Type | Security Function | Implementation Groups |
|------------|-------------------|-----------------------|
| Network    | Protect           | 1, 2, 3               |

### Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 2.4: Track Software Inventory Information

### Inputs

1. **List of endpoints to scan:** The list of endpoints to scan that are assumed capable of hosting firewall/port-filtering software as derived from the endpoint inventory (.sub-control 1.4) Additionally, this could potentially be informed by the software inventory (sub-control 2.4)
2. **Open policies:** A policy (or set of policies, potentially individually per endpoint) indicating the ports that are allowed to be open.

### Operations

1. For each endpoint, retrieve its firewall policy.
2. For each endpoint/firewall policy pair, examine the endpoint's configuration to enumerate the ports that allow communication. Also, examine any configuration of a default deny rule. Note which endpoints are configured appropriately or inappropriately.

### Measures

| Measure | Definition |
|---------|------------|
|---------|------------|



|   |  |
|---|--|
| M1 = List of scanned endpoints  | A list of all scanned endpoints.   |
| M2 = Count of items in M1   | A count of the total number of items in M1.  |
| M3 = List of endpoints with appropriate port configuration                              | A list of endpoints with appropriate port configuration.                             |
| M4 = Count of items in M3   | A count of the total number of items in M3.  |
| M5 = List of endpoints with inappropriate port configuration                            | A list of endpoints with inappropriate port configuration.                           |
| M6 = Count of items in M5   | A count of the total number of items in M5.  |
| M7= List of endpoints with appropriately configured default deny rule                   | A list of all endpoints with an appropriately configured default deny rule.          |
| M8 = Count of items in M7   | A count of the total number of items in M7.  |
| M9 = List of endpoints within appropriately configured default deny rule                | A list of endpoints with an inappropriately configured default deny rule.            |
| M10 = Count of items in M9  | A count of the total number of items in M9.  |
| M11 = List of endpoints with both appropriately configured ports and default deny rules | A list of endpoints with both appropriately configured ports and default deny rules. |
| M12 = Count of items in M11   | A count of the total number of items in M11.   |

## Metrics

### Coverage

| Metric   | Calculation |
|--|-------------|
| The ratio of correctly configured endpoints compared to the total number of endpoints. | $M12 / M2$  |



## CIS Control 13: Data Protection

The focus of this control is to ensure that all data is classified and protected in accordance with established data classifications. To establish these data classifications, organizations should develop a list of the key data types and define the overall importance to the organization. This can be used to create a data classification scheme for the organization. Labels, such as “Sensitive,” “Business Confidential”, and “Public,” should be used. The information owners need to be aware of the classification policy and the tools, procedures, and controls on said data.

The CIS states this Control is critical:

*“Data resides in many places. Protection of that data is best achieved through the application of a combination of encryption, integrity protection, and data loss prevention techniques. As organizations continue their move towards cloud computing and mobile access, it is important that proper care be taken to limit and report on data exfiltration while also mitigating the effects of data compromise.”*

*Some organizations do not carefully identify and separate their most sensitive and critical assets from less sensitive, publicly accessible information on their internal networks. In many environments, internal users have access to all or most of the critical assets. Sensitive assets may also include systems that provide management and control of physical systems, such as Supervisory Control and Data Acquisition (SCADA). Once attackers have penetrated such a network, they can easily find and exfiltrate important information, cause physical damage, or disrupt operations with little resistance. For example, in several high-profile breaches over the past few years, attackers were able to gain access to sensitive data stored on the same servers with the same level of access as far less important data. There are also examples of using access to the corporate network to gain access to, then control over, physical assets and cause damage.”*

The journey of implementing the CIS Controls continues with the prevention of data exfiltration, mitigating the effects of exfiltrated data, and ensuring the privacy and integrity of sensitive information. As with many of the CIS controls, the first step is establishing an asset inventory. With data files, this can feel like an insurmountable task. This is where knowing what is stored on the network, and where, is extremely important. Properly storing the data at rest or on mobile systems is critical to the security and tracking of the data. This control helps guide the organization through this review process. The three specific sub-controls that are part of Implementation Group 1 (IG1) are:

- [13.1: Maintain an Inventory of Sensitive Information](#)
- [13.2: Remove Sensitive Data or Systems Not Regularly Accessed by Organization](#)
- [13.6: Encrypt Mobile Device Data](#)

For CIS Control 13, Tenable products allow security operations teams to use Tenable Security Center Continuous View to analyze and search large amounts of data files for sensitive data. Located on the Tenable download portal and in Tenable Security Center feed, the security team can download and install audit files for sensitive data. Using these audit templates, file systems can be scanned and checked for sensitive data. For many organizations, these files need to be customized for optimum effectiveness. The Tenable Professional Services team can help with customization.

The screenshot displays the 'Add Audit File Template' interface in Tenable Security Center. The interface is divided into three main sections:

- Left Pane:** A list of audit templates, including 'TNS File Analysis - US Health Insurance Claim Number (HICN)', 'TNS File Analysis - ICD-10 Medical Coding', 'TNS File Analysis - Adult Media Browser Usage', 'TNS File Analysis - Source Code Errors', 'TNS File Analysis - Source Code Leakage', 'TNS File Analysis - Social Security Number (General)', 'TNS File Analysis - Social Security Number (Internal)', 'TNS File Analysis - Classified Documents', 'TNS File Analysis - Financial Statement', and 'TNS File Analysis - Employee Salary List'.
- Central Pane:** A list of audit files, each with a download icon, a name, a description, a size, and a 'Checksum' link. The files listed are:
  - Social Security Number (By State)
  - Adult Media
  - content\_address\_phone.audit
  - content\_ICD-10\_medical\_coding.audit
  - Financial Statement
  - Source Code Errors
  - content\_US\_HICN.audit
  - content\_DL\_number.audit
  - Credit Card Number
- Right Pane:** A detailed view of the selected audit file, showing its name, description, size, and a 'Checksum' link.

There are 4 existing dashboards that are designed to work with these audit files. These templates can be used to get started in using Tenable Security Center to assist IG1 organizations with Control 13.



## CIS Control 13: Data Protection

| Sub-Control | Asset Type | Security Function | Control Title   | Control Descriptions  | Implementation Groups |   |   |
|-------------|------------|-------------------|---|---|-----------------------|---|---|
|             |            |                   |   |   | 1                     | 2 | 3 |
| 13.1        | Data       | Identify          | Maintain an Inventory of Sensitive Information                          | Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider.   |                       |   |   |
| 13.2        | Data       | Protect           | Remove Sensitive Data or Systems Not Regularly Accessed by Organization | Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand-alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed. |                       |   |   |
| 13.3        | Data       | Detect            | Monitor and Block Unauthorized Network Traffic                          | Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.  |                       |   |   |
| 13.4        | Data       | Protect           | Only Allow Access to Authorized Cloud Storage or Email Providers        | Only allow access to authorized cloud storage or email providers.   |                       |   |   |
| 13.5        | Data       | Detect            | Monitor and Detect Any Unauthorized Use of Encryption                   | Monitor all traffic leaving the organization and detect any unauthorized use of encryption.   |                       |   |   |
| 13.6        | Data       | Protect           | Encrypt Mobile Device Data  | Utilize approved cryptographic mechanisms to protect enterprise data stored on all mobile devices.  |                       |   |   |
| 13.7        | Data       | Protect           | Manage USB Devices  | If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.   |                       |   |   |
| 13.8        | Data       | Protect           | Manage System's External Removable Media's Read/Write Configurations    | Configure systems not to write data to external removable media, if there is no business need for supporting such devices.  |                       |   |   |
| 13.9        | Data       | Protect           | Encrypt Data on USB Storage Devices                                     | If USB storage devices are required, all data stored on such devices must be encrypted while at rest.   |                       |   |   |





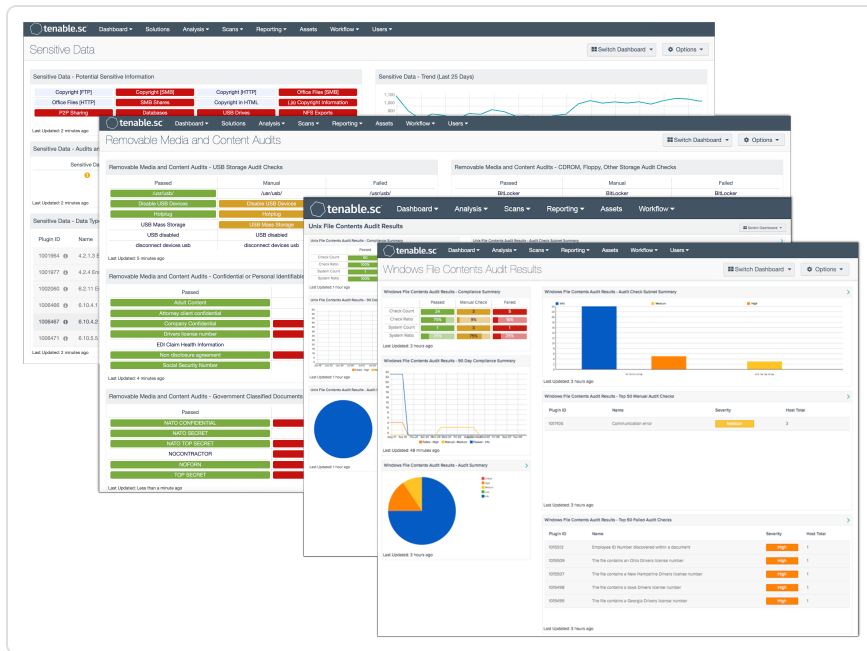
---

## Preface on Sub-Controls 13.1 and 13.2

---

As with previous controls, Control 13.1 requires an initial inventory be collected. Using the data from previous controls, the security team can formulate a plan to create the inventory of Data assets. Tenable Security Center is often associated with multiple scans per-week (for example, discovery, mitigation, and vulnerability scans). Scanning systems using the Content audit files can be very disk intensive, and Nessus reads the first part of many files. You can plan these scans more strategically, and store this data in a separate repository. The data should not be mixed with other vulnerability or compliance data. After the data is collected, the security team can begin to identify the best approach to managing the classification and data leakage prevention task. Listed below are descriptions of the current dashboard templates, all of which present the data differently and can help in understanding the where data is located.

**Sensitive Data:** Sensitive data includes, but is not limited to, personal and financial data, credit cards, Social Security numbers, and any other data that can facilitate identity theft, or identify an individual. Other forms of sensitive data may include copy-written data. Sensitive data can also be customer data, contact information, memberships, or political opinions. With the increasing amount of data being generated by businesses and individuals across the Internet, locating and protecting sensitive data has become crucial. Intruders and malicious organizations attempt to gain access to sensitive data through weakness and vulnerabilities in computer systems and networks. Identifying these weaknesses and keeping systems updated is solid first step to protecting sensitive data. This dashboard summarizes for the analyst a variety of checks from sensitive data audits, and checks for the presence of items that may contain sensitive data. Compliance failures could potentially lead to the loss of sensitive data.



For more information about the sensitive data dashboard, see [Systems with Sensitive Data](#).

**Windows or Unix File Contents Audit Results:** Governance, Risk Management, and Compliance (GRC) is a substantial part of any information assurance program. A GRC requires information systems to be audited, regardless of the standard to which the audit is performed. Tenable Security Center Continuous View using Nessus can perform Unix Content .audit checks. The content audit checks differ from Unix Configuration .audit checks in that they are designed to search a Unix file system for specific file types containing sensitive data rather than enumerate system configuration settings. The Content .audit checks include a range of options to help the auditor narrow down the search parameters and more efficiently locate and display noncompliant data. An example of non-compliant content is PII (Personally Identifiable Information) or PHI (Protected Health Information). This dashboard provides the audit results for Windows or Unix File Contents.

- <https://www.tenable.com/sc-dashboards/windows-audit-check-dashboards>
- <https://www.tenable.com/sc-dashboards/linux-audit-check-dashboards>

**Removable Media and Content Audits:** Data loss can occur through several methods. This dashboard focuses on tracking usage of USB devices, CD-ROMs, DVD-ROMs, and other removable media auditable events. Security analysts should also be concerned about the classification of data stored on local computers. In conjunction with scans using Nessus content audit files, systems containing classified data are easily identified. This dashboard focuses on auditing the use of removable media and storage of sensitive documents on local storage devices. The first step in monitoring sensitive



data is to have an operational data classification policy and detailed set of storage guidelines. The next step is to create an auditing program for all storage mediums. Tenable provides a series of audit files called Sensitive Content Audit Policies for Nessus and SecurityCenter Continuous View (CV). These audit policies look for credit cards, Social Security numbers, and many other types of sensitive data. Many of the other audit files contain audit controls for CD-ROMs, USB devices, and other storage types.

To audit for the storage of classified data, the organization should download the appropriate content audit files and modify the files accordingly. There are two modifications that may be required: the `file_extension` and `max_size` values. The `file_extension` [`file_extension: 'pdf' | 'doc'`] value contains the extension of the files that will be searched. The `max_size` value is the amount of data in the file that will be searched. For example, if the `max_size` is set to 20k, then the first 20k of the file will be searched. Other fields that might need adjusting are the `regex` and `expect` fields. However, these changes require extensive testing.

- <https://www.tenable.com/sc-dashboards/removable-media-and-content-audits>



---

## **Preface on Sub-Control 13.6**

---

Tenable Security Center does support an MDM integration solution, however the purpose is to detect vulnerabilities on mobile devices. The details of data stored on mobile devices is not recorded in data received from the MDM solutions. Whichever MDM solution that the organization is using should support requiring encryption to be enabled.



## 13.1: Maintain an Inventory of Sensitive Information

Tenable Security Center does support an MDM integration solution, however the purpose is to detect vulnerabilities on mobile devices. The details of data stored on mobile devices is not recorded in data received from the MDM solutions. Whichever MDM solution that the organization is using should support requiring encryption to be enabled.

| Asset Type | Security Function | Implementation Groups |
|------------|-------------------|-----------------------|
| Data       | Identify          | 1, 2, 3               |

### Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory

### Inputs

1. **Classification Scheme:** The organizationally-defined classification scheme.
2. **Sensitive information data set:** The data set of sensitive information for which the organization is responsible, mapped to the classification scheme defined by I1.
  - a. Review the available Tenable Audit files to see if an existing audit file is available.
3. **Endpoint/system mapping:** A mapping of an organization's endpoints/systems containing sensitive information classified by I2. Ideally, this uses the endpoint inventory (sub-control 1.4).
  - a. This can be the output of any matches found using audit scans with content audit file templates.

### Operations

1. Create the mappings of information deemed "sensitive" to the organization's classification scheme.
2. Create the mappings of classified, sensitive information to the endpoints/systems on which that information is stored.

### Measures



- M1:
  - 1 if the mappings of “sensitive” information to the organization’s classification scheme is provided.
  - 0 if the mappings of “sensitive” information to the organization’s classification scheme is not provided.
- M2:
  - 1 if the mappings of classified, sensitive information to the endpoints/systems on which it resides is provided.
  - 0 if the mappings of classified, sensitive information to the endpoints/systems on which it resides is not provided.

## Metrics

### Existence

| Metric   | Calculation      |
|--|------------------|
| The inventory of all sensitive information, cross-referenced with the systems on which that information is kept. | <b>M1 AND M2</b> |



## 13.2: Remove Sensitive Data or Systems Not Regularly Accessed by Organization

Sub-control 13.2 states that you must remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand-alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.

| Asset Type | Security Function | Implementation Groups |
|------------|-------------------|-----------------------|
| Data       | Protect           | 1, 2, 3               |

### Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 13.1: Maintain an Inventory of Sensitive Information

### Inputs

1. **List of sensitive systems:** A list of sensitive systems. Ideally, this uses the endpoint inventory (sub-control 1.4).
  - a. The list of systems from 13.1 scanning with Content Audit files can identify the systems with sensitive data.
2. **Access frequency:** The access frequency for any sensitive systems.
3. **Access frequency threshold:** An organizationally-defined access frequency threshold.

### Assumptions

- Access to sensitive data takes place through some system. Therefore the system, when processing, storing, or transmitting sensitive data, is a sensitive system.
- Isolation/exposure score of zero is assumed ideal.

### Operations



1. Determine the subset of sensitive systems that are infrequently used (using all Inputs).
2. For each infrequently used sensitive system, calculate the system's isolation/exposure.

## Measures

| Measure  | Definition   |
|--|--|
| M1 = List of all systems used to process sensitive information                                 | A list all systems used to process sensitive information.                                    |
| M2 = Count of items in M1  | A count of the total number of items in M1.  |
| M3 = Set of infrequently used sensitive systems  | A list of infrequently used sensitive systems.   |
| M4 = Count of infrequently used sensitive systems  | A count of infrequently used sensitive systems.  |
| M5 = List of infrequently used sensitive systems with isolation/exposure scores greater than 0 | A list of infrequently used sensitive systems with isolation/exposure scores greater than 0. |
| M6 = Count of items in M4  | A count of the total number of items in M4.  |

## Metrics

### Coverage

| Metric  | Calculation |
|---|-------------|
| The percentage of infrequently used sensitive systems that are not properly isolated. | $M6 / M4$   |





## 13.6: Encrypt Mobile Device Data

Sub-control 13.6 states that you must utilize approved cryptographic mechanisms to protect enterprise data stored on all mobile devices.

| Asset Type | Security Function | Implementation Groups |
|------------|-------------------|-----------------------|
| Data       | Protect           | 1, 2, 3               |

### Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 2.1: Maintain an Inventory of Authorized Software
- Sub-control 5.1: Establish Secure Configurations

### Inputs

1. **Approved mobile devices:** The list of approved mobile devices. This is derived from the endpoint inventory (sub-control 1.4).
2. **Approved mobile device encryption software:** The list of approved mobile device encryption software. Ideally, this is derived from the authorized software list (sub-control 2.1).
3. **Approved software configuration policy:** For each software in I2, the approved software configuration policy.

### Operations

1. For each mobile device in I1, determine if any of the approved encryption software from Input 2 is installed.
2. For each mobile device with installed approved encryption software, collect the software configuration information and compare it to the approved configuration policy (I3).

### Measures



| Measure   | Definition  |
|---|---|
| M1 = List of approved mobile devices  | A list of approved mobile devices.  |
| M2 = Count of items in M1   | A count of the total number of items in M1.                                       |
| M3 = List of approved mobile devices with approved encryption software installed    | A list of approved mobile devices with approved encryption software installed.    |
| M4 = Count of items in M3   | A count of the total number of items in M3.                                       |
| M5 = List of approved mobile devices without approved encryption software installed | A list of approved mobile devices without approved encryption software installed. |
| M6 = Count of items in M5   | A count of the total number of items in M5.                                       |
| M7 = List of appropriately configured mobile devices                                | A list of appropriately configured mobile devices.                                |
| M8 = Count of items in M7   | A count of the total number of items in M7.                                       |
| M9 = List of inappropriately configured mobile devices                              | A list of inappropriately configured mobile devices.                              |
| M10 = Count of items in M9  | A count of the total number of items in M9.                                       |

## Metrics

### Installed Software Coverage

| Metric   | Calculation |
|--|-------------|
| The percentage of approved mobile devices that are equipped with approved encryption software. | $M4 / M2$   |

### Appropriately Configured Devices

| Metric  | Calculation |
|---|-------------|
| The percentage of approved mobile devices equipped with approved encryption software that meet or exceed the approved configuration policy. | $M8 / M2$   |



## CIS Control 14: Controlled Access Based on the Need to Know

The focus of this control is to ensure users are only allowed access to information they are authorized or needed to perform job duties. There are several layers to this complex problem, beginning with network segmentation, and growing to data classification and Data Loss Prevention (DLP) products.

The CIS states this Control is critical:

*“Encrypting data provides a level of assurance that even if data is compromised, it is impractical to access the plaintext without significant resources; however, controls should also be put in place to mitigate the threat of data exfiltration in the first place. Many attacks occurred across the network, while others involved physical theft of laptops and other equipment holding sensitive information. Yet, in many cases, the victims were not aware that the sensitive data were leaving their systems because they were not monitoring data outflows. The movement of data across network boundaries both electronically and physically must be carefully scrutinized to minimize its exposure to attackers.”*

The journey of implementing the CIS Controls continues with controlling access using Access Control Lists (ACL). Organizations are directed to protect all information stored on systems using native ACL methods. These methods include network layer access controls, file level permissions, and other application centric controls. The specific sub-controls that are part of Implementation Group 1 (IG1) are:

- [14.6: Protect Information Through Access Control Lists](#)

Managing ACL or Dynamic ACL (DACL) is a complicated task at all levels of IT operations. The best approach is to have a clearly defined access policy and to conduct repeated internal audits. Some organizations take an approach to deny all access, and then open up access as needed. This approach is good for file systems or databases, but is harder when looking at network based ACL. To automate the audit process, Tenable Security Center can be configured with custom audit files to review configurations and report on the status. This customization is a very advanced process, and should be done with aid of professional services.

The organization should take their time during this process and review all the access requirements at each level. In some cases, several controls come together to create the completed security control. For example, access to a database system starts at the network layer, but restricts access



based on IP and TCP ports. User and services accounts are needed, which may lead to file level permissions. Finally, data level ACL must be created. If any one step in the ACL is misconfigured, the system could have too much access or no access at all. Use the data collected in Controls 1 & 5 to help establish the requirements and begin documenting access requirements.



## 14.6: Protect Information Through Access Control Lists

Sub-control 14.6 states that you must leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit.

| Asset Type | Security Function | Implementation Groups |
|------------|-------------------|-----------------------|
| Date       | Protect           | 1, 2, 3               |

### Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 5.1: Establish Secure Configurations

### Inputs

1. **Endpoint Inventory:** The list of all endpoints.
2. **Access control configuration policy:** The organizationally defined access control configuration policy.

### Operations

1. For each endpoint in I1, collect the “ground truth” access policy for that endpoint and compare it to the access control configuration policy in I2. Generate a list of endpoints which comply with the specified access control configuration policy (M1) and a list of endpoints that do not comply with the specified policy (M2).

### Measures

| Measure  | Definition  |
|--|---|
| M1 = List of endpoints that comply with access control configuration policy (compliant list) | A list of endpoints that comply with the access control configuration policy. |
| M2 = List of endpoints that do not comply with   | A list of endpoints that do not comply  |



|  |   |
|--|---|
| access control configuration policy (non-compliant list)           | with the access control configuration policy. |
| M3 = Count of items in M1  | A count of the total number of items in M1.   |
| M4 = Count of items in M2  | A count of the total number of items in M2.   |
| M5 = Count of endpoints in I1 (total number of endpoints to check) | A count of all the endpoints in I1.           |

## Metrics

### Coverage

| Metric   | Calculation |
|--|-------------|
| The percentage of endpoints which are compliant with the organization's access control policy. | $M3 / M5$   |



## CIS Control 15: Wireless Access Control

The focus of this control is to ensure wireless access is configured to track and control access, prevent unauthorized access. If misconfigurations are found, the settings should be corrected. Wireless access has become a common and natural part of a majority of organizations network infrastructure. Wireless access is beneficial, but exposes networks to problems related to network boundaries, all of which come back to this basic series of questions:

- **Who** has access?
- **What** is being accessed?
- **Why** wireless access is required?
- **Where** from which locations is access required?
- **When** is access appropriate?

The CIS states this Control is critical:

*“Major thefts of data have been initiated by attackers who have gained wireless access to organizations from outside the physical building, bypassing organizations’ security perimeters by connecting wirelessly to access points inside the organization. Wireless clients accompanying travelers are infected on a regular basis through remote exploitation while on public wireless networks found in airports and cafes. Such exploited systems are then used as backdoors when they are reconnected to the network of a target organization. Other organizations have reported the discovery of unauthorized wireless access points on their networks, planted and sometimes hidden for unrestricted access to an internal network. Because they do not require direct physical connections, wireless devices are a convenient vector for attackers to maintain long-term access into a target environment.”*

The journey of implementing the CIS Controls continues with controlled use of wireless networking. Organizations are directed to verify that Advanced Encryption Standard (AES) is configured for all wireless technology. The sub-control that is part of Implementation Group 1 (IG1) is:

- [15.7: Leverage the Advanced Encryption Standard \(AES\) to Encrypt Wireless Data](#)



## CIS Control 15: Wireless Access Control

| Sub-Control | Asset Type | Security Function | Control Title  | Control Descriptions  | Implementation Groups |   |   |
|-------------|------------|-------------------|--|---|-----------------------|---|---|
|             |            |                   |  |   | 1                     | 2 | 3 |
| 15.1        | Network    | Identify          | Maintain an Inventory of Authorized Wireless Access Points                             | Maintain an inventory of authorized wireless access points connected to the wired network.  |                       |   |   |
| 15.2        | Network    | Detect            | Detect Wireless Access Points Connected to the Wired Network                           | Configure network vulnerability scanning tools to detect and alert on unauthorized wireless access points connected to the wired network.   |                       |   |   |
| 15.3        | Network    | Detect            | Use a Wireless Intrusion Detection System  | Use a wireless intrusion detection system (WIDS) to detect and alert on unauthorized wireless access points connected to the network.   |                       |   |   |
| 15.4        | Devices    | Protect           | Disable Wireless Access on Devices if Not Required                                     | Disable wireless access on devices that do not have a business purpose for wireless access.   |                       |   |   |
| 15.5        | Devices    | Protect           | Limit Wireless Access on Client Devices  | Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks. |                       |   |   |
| 15.6        | Devices    | Protect           | Disable Peer-to-Peer Wireless Network Capabilities on Wireless Clients                 | Disable peer-to-peer (ad hoc) wireless network capabilities on wireless clients.  |                       |   |   |
| 15.7        | Network    | Protect           | Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data               | Leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit.  |                       |   |   |
| 15.8        | Network    | Protect           | Use Wireless Authentication Protocols That Require Mutual, Multi-Factor Authentication | Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), that requires mutual, multi-factor authentication.              |                       |   |   |
| 15.9        | Devices    | Protect           | Disable Wireless Peripheral Access to Devices  | Disable wireless peripheral access of devices [such as Bluetooth and Near Field Communication (NFC)], unless such access is required for a business purpose.  |                       |   |   |
| 15.10       | Network    | Protect           | Create Separate Wireless Network for Personal and Untrusted Devices                    | Create a separate wireless network for personal or untrusted devices. Enterprise access from this network should be treated as untrusted and filtered and audited accordingly.                            |                       |   |   |





## 15.7: Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data

Sub-control 15.7 states that you must leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit.

| Asset Type | Security Function | Implementation Groups |
|------------|-------------------|-----------------------|
| Network    | Protect           | 1, 2, 3               |

### Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information

### Inputs

1. **List of wireless devices:** A list of wireless devices. This is derived from the Endpoint Inventory (sub-control 1.4).
2. **List of AES-capable wireless devices:** A list of all AES-capable wireless devices (sub-control 1.5).

### Operations

1. For each AES-capable wireless device, collect the cipher suite configuration.

### Measures

| Measure                                   | Definition  |
|---|---|
| M1 = List of wireless devices             | A list of wireless devices.   |
| M2 = Count of items in M1                 | A count of the total number of items in M1.   |
| M3 = List of AES-capable wireless devices | A list of AES-capable wireless devices. Using the regex provided above, the organization can get a count of systems |



|  |  |
|--|--|
|  | with AES configured.   |
| M4 = Count of items in M3  | A count of the total number of items in M3.  |
| M5 = List of non-AES-capable wireless devices                        | A list of non-AES-capable wireless devices. Using the regex provided above, the organization can get a count of systems without AES configured.        |
| M6 = Count of items in M5  | A count of the total number of items in M5.  |
| M7 = List of appropriately configured AES-capable wireless devices   | A list of appropriately configured AES-capable wireless devices. Using the regex above, the organization can find the systems with only AES enabled.   |
| M8 = Count of items in M7  | A count of the total number of items in M7.  |
| M9 = List of inappropriately configured AES-capable wireless devices | A list of inappropriately configured AES-capable wireless devices. Using the regex above, the organization can find the systems with only AES enabled. |
| M10 = Count of items in M9   | A count of the total number of items in M9.  |

## Metrics

### Coverage

| Metric   | Calculation |
|--|-------------|
| The percentage of AES-capable devices that are configured to use cipher suites leveraging AES. | $M8 / M4$   |



## CIS Control 16: Account Monitoring and Control

The focus of this control is to ensure that all accounts are managed in a fashion that promotes clean account hygiene. This misuse or neglect of account maintenance can lead to system compromise.

The CIS states this Control is critical:

*“Attackers frequently discover and exploit legitimate but inactive user accounts to impersonate legitimate users, thereby making discovery of attacker behavior difficult for security personnel watchers. Accounts of contractors and employees who have been terminated and accounts formerly set up for Red Team testing (but not deleted afterwards) have often been misused in this way. Additionally, some malicious insiders or former employees have gained access to accounts left behind in a system long after contract expiration, maintaining their access to an organization’s computing system, and sensitive data for unauthorized and sometimes malicious purposes.”*

The journey of implementing the CIS Controls continues with practicing good user account hygiene and maintenance. Many systems (operating systems and application systems) may have the ability to set controls and policies on user accounts. The centralized management of these types of accounts can often be neglected or fall out of scope of normal business processes. Organizations are directed to disable any unassociated or dormant accounts. These accounts are often overlooked or set up with a default password, both of which are undesirable for more than a short period of time. For example, if a user contacts the helpdesk to change the password, then it is appropriate for a default password to be set. However, the password should then be changed within minutes, not weeks. Organizations are directed to configure systems to automatically lock workstation sessions after a specified inactivity period. This setting is a common configuration and is set using Group Policy Objects for Windows computers.

The three specific sub-controls that are part of Implementation Group 1 (IG1) are:

- [16.8: Disable Any Unassociated Accounts](#)
- [16.9: Disable Dormant Accounts](#)
- [16.11: Lock Workstation Sessions After Inactivity](#)

For CIS Control 16, there is a strong connection to CIS Control 4 which speaks to elevated privileges. Control 16 looks at all accounts and how local computer/application policy can be configured to



support good account hygiene. Tenable products allow security operations teams to use Tenable Security Center Continuous View to analyze system configurations, many of which set local security policies, e.g., control of screen locking. In addition to several audit checks, there are many plugins that assist in tracking accounts that are unused, passwords that have never been changed, and so forth. Account management is often easily controlled by properly configured systems or centralized authentication. Tenable Security Center quickly identifies the systems with an issue and can help the organization create a plan of action to remediate or mitigate the risk associated with account management. The CIS Control 4/5 Secure Configurations and Group Memberships Dashboard provides useful information to assist organizations with this control.

**Account Status Indicators - Windows SMB Account Information**

- Use Domain SID to Enumerate User: Guessable User Credentials
- Use Host SID to Enumerate Local U: Registry Winlogon Cached Passwords
- Registry Last Logged User Name Di: Obtains the Password Policy
- Blank Administrator Password: Guest Account Local User Access
- Last Logged On User Disclosure: Registry Enumerate the list of SNMF
- Use Host SID to Enumerate Local U
- Last Updated: Less than a minute ago

**Account Status Indicators - Local Users Information**

- Automatically Disabled Accounts: Can't Change Password
- Disabled Accounts: Never Changed Password
- User has Never Logged in: Passwords Never Expires
- Last Updated: Less than a minute ago

**CSC - Account and Group Information**

| Plugin ID | Name                    | Family    | Seve... | T... |
|-----------|-------------------------|-----------|---------|------|
| 17651     | Microsoft Windows SMB : | Window... | Info    | 15   |
| 38689     | Microsoft Windows SMB   | Windows   | Info    | 14   |
| 10902     | Microsoft Windows       | Window... | Info    | 14   |
| 71246     | Enumerate Local Group   | Windows   | Info    | 13   |
| 72684     | Enumerate Users via WMI | Windows   | Info    | 11   |

Last Updated: Less than a minute ago

**CSC - Compliance Checks**

|             | Systems | Scans (Last 7 Days) | Passed | Manual | Failed |
|-------------|---------|---------------------|--------|--------|--------|
| All CIS CSC | 44      | ✓                   | 38%    | 9%     | 57%    |
| All Checks  | 67      | ✓                   | 38%    | 7%     | 57%    |

Last Updated: Less than a minute ago

**CSC - Compliance Checks By Keyword**

|            | Systems | Scans (Last 7 Days) | Passed | Manual | Failed |
|------------|---------|---------------------|--------|--------|--------|
| All        | 67      | ✓                   | 38%    | 7%     | 57%    |
| Account    | 43      | ✓                   | 11%    | 2%     | 57%    |
| Audit      | 39      | ✓                   | 15%    | 16%    | 69%    |
| Disable    | 38      | ✓                   | 10%    | 1%     | 59%    |
| Enable     | 40      | ✓                   | 51%    | 1%     | 48%    |
| Log        | 42      | ✓                   | 29%    | 4%     | 68%    |
| Password   | 37      | ✓                   | 20%    | 2%     | 78%    |
| Permission | 35      | ✓                   | 43%    | 1%     | 50%    |
| User       | 45      | ✓                   | 38%    | 3%     | 59%    |

Last Updated: Less than a minute ago

**Prioritize Hosts - Top Hosts with Compliance Concerns**

| IP Address  | DNS   | Total | Vulnerabilities |
|-------------|---|-------|-----------------|
| 10.10.10.10 | ubuntu1904-desktop.target.tenablesecurity.com | 283   | 258             |
| 10.10.10.10 | debian9.target.tenablesecurity.com            | 282   | 257             |
| 10.10.10.10 | ubuntu1810-desktop.target.tenablesecurity.com | 277   | 251             |
| 10.10.10.10 | ubuntu1904server.target.tenablesecurity.com   | 276   | 251             |
| 10.10.10.10 | ubuntu1810-server.target.tenablesecurity.com  | 274   | 249             |

Last Updated: Less than a minute ago

**Account Status Indicators - Users and SID Information**

- Use Host SID to Enumerate Local U: Local User Information
- Automatically disabled accounts: Can't change password
- Disabled accounts: Never changed passwords
- User has never logged on: Passwords never expire
- Guest Account Local User Access: Use Host SID to Enumerate Local U
- Enumerate Local Group Members: Enumerate Local Users
- Last Updated: Less than a minute ago

**Account Status Indicators - Group Memberships**

- User Aliases List: User Groups List
- Account Operators Group User List: Administrators Group User List
- Server Operators Group User List: Backup Operators Group User List
- Print Operators Group User List: Replicator Group User List
- Guest Account Belongs to a Group: Domain Administrators Group User I
- Last Updated: Less than a minute ago

**CIS - Configuration Info Collected during Active Scanning.**

| Name   | Host Total |
|--|------------|
| Host Fully Qualified Domain Name (FQDN) Resolution | 170        |
| Common Platform Enumeration (CPE)                  | 163        |
| Device Type  | 158        |
| SSH Algorithms and Languages Supported             | 132        |
| SSH Server Type and Version Information            | 132        |

Last Updated: Less than a minute ago

For more information about the CIS Control 4/5 dashboard, see [CIS Control 4/5: Secure Configurations & Group Memberships](#).

NIST also provides helpful information directly related to this CIS Control under the [NIST Special Publication 800-53 \(Rev. 4\) - AC-2 ACCOUNT MANAGEMENT](#).



## CIS Control 16: Account Monitoring and Control

| Sub-Control | Asset Type | Security Function | Control Title  | Control Descriptions   | Implementation Groups |   |   |
|-------------|------------|-------------------|--|--|-----------------------|---|---|
|             |            |                   |  |  | 1                     | 2 | 3 |
| 16.1        | Users      | Identify          | Maintain an Inventory of Authentication Systems                | Maintain an inventory of each of the organization's authentication systems, including those located on-site or at a remote service provider.   |                       |   |   |
| 16.2        | Users      | Protect           | Configure Centralized Point of Authentication                  | Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.   |                       |   |   |
| 16.3        | Users      | Protect           | Require Multi-Factor Authentication                            | Require multi-factor authentication for all user accounts, on all systems, whether managed on-site or by a third-party provider.   |                       |   |   |
| 16.4        | Users      | Protect           | Encrypt or Hash All Authentication Credentials                 | Encrypt or hash with a salt all authentication credentials when stored.  |                       |   |   |
| 16.5        | Users      | Protect           | Encrypt Transmittal of Username and Authentication Credentials | Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.   |                       |   |   |
| 16.6        | Users      | Identify          | Maintain an Inventory of Accounts                              | Maintain an inventory of all accounts organized by authentication system.  |                       |   |   |
| 16.7        | Users      | Protect           | Establish Process for Revoking Access                          | Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor. Disabling these accounts, instead of deleting accounts, allows preservation of audit trails. |                       |   |   |
| 16.8        | Users      | Respond           | Disable Any Unassociated Accounts                              | Disable any account that cannot be associated with a business process or business owner.   |                       |   |   |
| 16.9        | Users      | Respond           | Disable Dormant Accounts                                       | Automatically disable dormant accounts after a set period of inactivity.   |                       |   |   |
| 16.10       | Users      | Protect           | Ensure All Accounts Have An Expiration Date                    | Ensure that all accounts have an expiration date that is monitored and enforced.   |                       |   |   |
| 16.11       | Users      | Protect           | Lock Workstation Sessions After Inactivity                     | Automatically lock workstation sessions after a standard period of inactivity.   |                       |   |   |
| 16.12       | Users      | Detect            | Monitor Attempts to Access Deactivated Accounts                | Monitor attempts to access deactivated accounts through audit logging.   |                       |   |   |
| 16.13       | Users      | Detect            | Alert on Account Login Behavior Deviation                      | Alert when users deviate from normal login behavior, such as time-of-day, workstation location, and duration.  |                       |   |   |



## Preface on Sub-Controls 16.8, 16.9, and 16.11

### Sub Controls 16.8 & 16.9

Sub-control 16.8 is not a technical control, as this requires a human to make the association between the role of the person and the account. However, Tenable Security Center is able to query systems and retrieve account names. Once the account names are collected, an organization can set up a manual process to review the accounts. There are plugins that can be used to look for accounts that are not active, and priority can be given to those systems. This process supports 16.9, as the dormant accounts may be identified during the review process. The **"CSF - Account and Group Information"** table located in the CIS Control 4/5 dashboard provides the query to use to get the information needed to support the account review process.

This table displays detections of account and group information, such as accounts that have never been logged into, disabled accounts, and group user lists. This information is obtained through Nessus credentialed scans. Most of these detections contain lists of accounts in the output. The "Obtains the Password Policy" detection contains the retrieved password policy in its output. Click on the **Browse Component Data** icon on the component to view the vulnerability analysis screen. Here, you can view the detections and investigate further. On the analysis screen, set the tool to **Vulnerability Detail List** to view the full details for each detection, including description and output.

The screenshot displays the Tenable Security Center interface for Vulnerability Analysis. The left pane shows the 'Enumerate Users via WMI (72684)' plugin output, which lists user details for three users: Admin, Administrator, and Guest. The right pane shows a 'Vulnerability Summary' table with 21 results. The table columns are Plugin ID, Name, Family, Severity, VPR, and Total. The results include detections for disabled accounts, never changed passwords, and group user lists.

| Plugin ID | Name  | Family                        | Severity | VPR | Total |
|-----------|---|-------------------------------|----------|-----|-------|
| 10399     | SMB Use Domain SID to Enumerate Users                                   | Windows : User management     | Info     | 9   | 9     |
| 10897     | Microsoft Windows - Users Information : Disabled Accounts               | Windows : User management     | Info     | 9   | 9     |
| 10898     | Microsoft Windows - Users Information : Never Changed Password          | Windows : User management     | Info     | 9   | 9     |
| 10899     | Microsoft Windows - Users Information : User Has Never Logged In        | Windows : User management     | Info     | 9   | 9     |
| 10900     | Microsoft Windows - Users Information : Passwords Never Expire          | Windows : User management     | Info     | 4   | 4     |
| 10908     | Microsoft Windows 'Domain Administrators' Group User List               | Windows : User management     | Info     | 2   | 2     |
| 46742     | Microsoft Windows SMB Registry : Enumerate the list of SNMP communities | Windows                       | Info     | 1   | 1     |
| 10904     | Microsoft Windows 'Backup Operators' Group User List                    | Windows : User management     | Info     | 1   | 1     |
| 60019     | Mac OS X Admin Group User List  | MacOS X Local Security Checks | Info     | 1   | 1     |
| 10895     | Microsoft Windows - Users Information : Automatically Disabled Accounts | Windows : User management     | Info     | 1   | 1     |



## Sub Control 16.11


This control focuses more on desktop computers, but can also affect applications, routers, switches and Linux servers. The configurations, however, are very different. As mentioned in the CIS Control 5 with baseline settings, Organizations should begin with CIS Benchmark. Tenable Security Center comes with audit files that are created based on the benchmarks, and this feature can be used to address this sub control. In the CIS Control 4/5 dashboard, the center column provides audit results for the benchmarks with various key words.

The screenshot displays the Tenable Security Center interface. At the top is a navigation bar with the Tenable logo and various menu items: Dashboard, Solutions, Analysis, Scans, Reporting, Assets, Workflow, and Users. Below this is a header for 'Vulnerability Analysis' with an 'Options' button. The main content area shows a 'Vulnerability Detail List' with a 'High' severity rating for the control '2.3.7.3 Ensure 'Interactive logon: Machine account lockout threshold''. The control is categorized as 'High' and is the 7th of 9 results. The interface includes buttons for 'Accept Risk' and 'Recast Risk'. The control details are organized into several sections: 'Solution' (To establish the recommended configuration via GP, set the following UI path to 10 or fewer invalid logon attempts, but not 0: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Machine account lockout threshold), 'Audit File' (auditFile.tGnT6L), 'Information' (This security setting determines the number of failed logon attempts that causes the machine to be locked out. Failed password attempts against workstations or member servers that have been locked using either CTRL+ALT+DELETE or password protected screen savers counts as failed logon attempts.), 'Discovery' (First Discovered: Over a year ago, Last Observed: Today), 'Host Information' (IP Address: 172.26.48.97 (TCP), Agent ID: ed4380e8-70dd-4e93-887d-c2bfc5157ead, DNS: windows81.target.tenablesecurity.com, MAC Address: 00:50:56:a6:09:c1, NetBIOS: WORKGROUP\WINDOWS81, Repository: REPO 2135), 'Plugin Details' (Plugin ID: 1007121, Family: N/A), and 'Reference Information'.

In the “CSF - Compliance Checks By Keyword” matrix, the “Log” row finds all audit checks with the word “Log” present. Each column provides a specific view into the queries with different tools and respective filters. The key to this control hover is illustrated in the “CIS Microsoft Windows Server 2019 Benchmark” setting index 2.3.7.3. In this setting, a Windows 2019 server is audited for the Interactive Logon setting. This is the key setting used to track this session timeout. The organization must review each benchmark and look for similar examples to find the exact matches. However, if the base work used in the setting is “log”, then this filter in this row returns the results. For Cisco routers, the search would be “exec-timeout”, which would not match. While Tenable can provide



some keywords for searching, the organization is strongly encouraged to review the CIS Benchmark and select the correct terms.

| CSF - Compliance Checks By Keyword  |         |                  |        |        |        |
|--|---------|------------------|--------|--------|--------|
|  | Systems | Scans (Last 7... | Passed | Manual | Failed |
| All  | 3       | None             | 50%    | 1%     | 49%    |
| Account  | 1       | None             | 80%    | 0%     | 20%    |
| Audit  | 0       | None             | -      | -      | -      |
| Disable  | 1       | None             | 50%    | 0%     | 50%    |
| Enable   | 1       | None             | 80%    | 0%     | 20%    |
| Log  | 1       | None             | 54%    | 0%     | 46%    |
| Password   | 1       | None             | 67%    | 0%     | 33%    |
| Permission   | 0       | None             | -      | -      | -      |
| User   | 1       | None             | 0%     | 29%    | 71%    |

Last Updated: 4 hours ago

- CIS Microsoft Windows Server 2019 Benchmark
  - <https://workbench.cisecurity.org/files/2630>
  - "2.3.7.3 Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second (s), but not 0'"
  - CIS\_DC\_SERVER\_2019\_Level\_1\_v1.1.0.audit
- Cisco IOS 15 Benchmark v4.0.1
  - <https://workbench.cisecurity.org/files/2585>
  - 1.2.9 Set 'exec-timeout' to less than or equal to 10 minutes 'line vty'"
  - CIS\_Cisco\_IOS\_15\_v4.0.1\_Level\_1.audit

Below is a series of search terms and regular expressions to match:

REGEX: `[il]dle[tT]imeout[il]nactive`





## Search Terms

- Inactive
- Timeout
- Idle connections
- Idle Timeout
- user shell timeout
- connection Timeout
- SSH Idle Timeout
- DCUI timeout
- shell services timeout
- terminate idle ESXi
- exec-timeout



## 16.8: Disable Any Unassociated Accounts

Sub-control 16.8 states that you must disable any account that cannot be associated with a business process or business owner.

| Asset Type | Security Function | Implementation Groups |
|------------|-------------------|-----------------------|
| Users      | Respond           | 1, 2, 3               |

### Dependencies

- None

### Inputs

1. **Inventory of accounts:** An inventory of all accounts.
2. **Inventory of business processes and/or business owners:** An inventory of all business processes and/or business owners.

### Operations

1. For each account, enumerate any associated business processes or ownership.

### Measures

| Measure  | Definition   |
|--|--|
| M1 = List of Accounts  | A list of all accounts. This number should be calculated per system/application/centralized authentication source. |
| M2 = Count of items in M1  | A count of the total number of items in M1.  |
| M3 = List of accounts not associated with any business process or ownership. | A list of all accounts not associated with any business process or ownership.                                      |
| M4 = Count of items in M3  | A count of the total number of items in M3.  |
| M5 = List of accounts asso-  | A list of all accounts associated with at least one business pro-  |



|   |  |
|---|--|
| ciated with at least one business process or ownership. | cess or ownership. After the initial review, a database can be created to correlate all the accounts for future assessments. |
| M6 = Count of items in M5                               | A count of the total number of items in M5.  |

## Metrics

### Coverage

| Metric  | Calculation |
|---|-------------|
| The percentage of accounts that are associated with at least one business process or ownership. | $M6 / M2$   |



## 16.9: Disable Dormant Accounts

Sub-control 16.9 states that you must automatically disable dormant accounts after a set period of inactivity.

| Asset Type | Security Function | Implementation Groups |
|------------|-------------------|-----------------------|
| Users      | Respond           | 1, 2, 3               |

### Dependencies

- None

### Inputs

1. **Account Inventory:** The list of all accounts created in the enterprise
2. **Definition of "dormant threshold":** An organizationally defined policy indicating a "dormant threshold". This serves as the period of inactivity after which the account is considered dormant. The CIS recommends this be set to 1 month.

### Assumptions

- The list of accounts for the enterprise includes OS-level, database, internal, and external application accounts.
- Based on the account location, a query interface is assumed that enables the collection of a "last activity" timestamp, such as last logon, as well as a status indicating if the account is enabled or disabled.

### Operations

1. For each account, enumerate any associated business processes or ownership.

### Measures

| Measure               | Definition              |
|-----------------------|-------------------------|
| M1 = List of Accounts | A list of all accounts. |



|  |   |
|--|---|
| M2 = Count of items in M1  | A count of the total number of items in M1.   |
| M3 = List of accounts marked as enabled  | A list of all accounts marked as enabled.   |
| M4 = Count of items in M3  | A count of the total number of items in M3.   |
| M5 = List of accounts enabled and not used for a time period outside the dormant threshold | A list of all accounts that are enabled and have not been used for a time period outside the dormant threshold. |
| M6 = Count of items in M5  | A count of the total number of items in M5.   |

## Metrics

### Dormant Accounts

| Metric   | Calculation |
|--|-------------|
| The percentage of all accounts that are currently dormant but still enabled. | $M6 / M2$   |

### Enabled Dormant Accounts

| Metric  | Calculation |
|---|-------------|
| The percentage of accounts that are marked enabled, that are currently dormant and still enabled. | $M3 / M2$   |



## 16.11: Lock Workstation Sessions After Inactivity

Sub-control 16.11 states that you must automatically lock workstation sessions after a standard period of inactivity.

| Asset Type | Security Function | Implementation Groups |
|------------|-------------------|-----------------------|
| Users      | Protect           | 1, 2, 3               |

### Dependencies

- Sub-control 1.4: Maintain Detailed Asset Inventory
- Sub-control 1.5: Maintain Asset Inventory Information
- Sub-control 5.1: Establish Secure Configurations

### Inputs

1. **List of workstations with locking:** A list of workstations which have enabled automatic workstation locking
2. **List of workstations:** A list of all workstations.
3. **Workstation configuration policy:** The workstation configuration policy that establishes the organization's workstation locking time threshold.

### Operations

1. For each workstation with locking enabled, collect the locking time threshold.
2. Collect the list of workstations whose locking time threshold exceeds the value specified by 13.

### Measures

| Measure                   | Definition   |
|---------------------------|--|
| M1 = List of Workstations | A list of all systems discovered using Tenable Security Center and checked with audit files. |



|  |  |
|--|--|
| M2 = Count of items in M1  | A count of the total number of items in M1.                                  |
| M3 = List of workstations with automatic workstation locking enabled | A list all of workstations with automatic workstation locking enabled.       |
| M4 = Count of items in M3  | A count of the total number of items in M3.                                  |
| M5 = List of appropriately configured workstations                   | A list of all systems with the appropriate benchmark configured correctly.   |
| M6 = Count of items in M5  | A count of the total number of items in M5.                                  |
| M7 = List of inappropriately configured workstations                 | A list of all systems with the appropriate benchmark configured incorrectly. |
| M8 = Count of items in M7  | A count of the total number of items in M7.                                  |

## Metrics

### Misconfigured Workstations

| Metric   | Calculation |
|--|-------------|
| The percentage of workstations with automatic locking enabled that are configured within the locking time threshold. | $M6 / M2$   |

### Unconfigured Workstations

| Metric   | Calculation |
|--|-------------|
| The number of workstations that do not have automatic locking enabled. | $M2 - M4$   |



---

## Organizational Controls

---

Tenable Security Center and the CIS CAS helps set the foundation for the organization's journey through the Implementation Groups. The organization controls are part of IG2 and IG3, and help provide next steps and wider focus to overall risk management. At this stage the organization needs to be able to take inventory of the risk mitigation progress, and begin the planning for the next iteration of the risk mitigation efforts. CIS controls 17 - 20 provide the organization with steps which complete the IG1 journey and prepare for them for IG2 and IG3.

The four Organization controls are:

- [CIS Control 17: Implement a Security Awareness and Training Program](#)
- [CIS Control 18: Application Software Security](#)
- [CIS Control 19: Incident Response and Management](#)
- [CIS Control 20: Penetration Tests and Red Team Exercises](#)

The CIS groups these final 4 controls into the Organization Controls, and states:

*"All of these topics are a critical, foundational part of any cyber defense program, but they are different in character than CIS Controls 1-16. While they have many technical elements, these are less focused on technical controls and more focused on people and processes. They are pervasive in that they must be considered across the entire enterprise, and across all of CIS Controls 1-16. Their measurements and metrics of success are driven more by observations about process steps and outcomes, and less by technical data gathering. They are also complex topics in their own right, each with an existing body of literature and guidance.*

*Therefore we present CIS Controls 17-20 as follows: for each CIS Control, we identify a small number of elements that we believe are critical to an effective program in each area. We then describe processes and resources which can be used to develop a more comprehensive enterprise treatment of each topic. Although there are many excellent commercial resources available, we provide open and non-profit sources where possible. The ideas, requirements, and processes expressed in the references are well supported by the commercial marketplace."*

Tenable Security Center provides valuable information to aid in these final 4 steps, each of which will be discussed individually. However, for the IG1 journey there are no measurable steps to be





taken. The final section in this guide will provide suggestions on how the data previously collected can be used to aid in closing of the IG1 journey and preparation for IG2.



## CIS Control 17: Implement a Security Awareness and Training Program

The security awareness program is influenced by the maturity of an organization. For example a small company with 100 employees or less can have a very informal program, while a fortune 500 company on average has over 60,000 employees and must have a very formal program.

CIS Control 17 states:

*"For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs."*

*Why Is This CIS Control Critical?*

*It is tempting to think of cyber defense primarily as a technical challenge, but the actions of people also play a critical part in the success or failure of an enterprise. People fulfill important functions at every stage of system design, implementation, operation, use, and oversight. Examples include: system developers and programmers (who may not understand the opportunity to resolve root cause vulnerabilities early in the system life cycle); IT operations professionals (who may not recognize the security implications of IT artifacts and logs); end users (who may be susceptible to social engineering schemes such as phishing); security analysts (who struggle to keep up with an explosion of new information); and executives and system owners (who struggle to quantify the role that cybersecurity plays in overall operational/mission risk, and have no reasonable way to make relevant investment decisions)."*

Tenable Security Center provides reports and other data display tools to help the security awareness team understand how risk mitigation efforts are progressing. As shown in the image below, we have created accounts for the executive team who organizationally, is responsible for assets. This visualization can be used to help provide awareness of the current state of the vulnerability management program. Other filters and queries can also be used to help illustrate risk management functions. As the organization matures and becomes more security aware, these types of reports can also serve as Key Performance Indicators (KPI).



## Vulnerability Analysis

Options ▾

## Filters



## Severity



Low, Medium, High, Critical

## Address

All

## Plugin Name

All

Select Filters

Clear Filters

Load Query

## User Responsibility Summary ▾

Jump to Vulnerability Detail List

Total Results: 10

| Users              | Score | Total ▾ | Vulnerabilities |       |  |
|--------------------|-------|---------|-----------------|-------|--|
| Sales              | 47256 | 11561   | 935             | 10169 |  |
| BusinessOperations | 67674 | 7133    | 3113            | 2963  |  |
| HumanResources     | 8311  | 2234    | 1945            |       |  |
| ProductManagement  | 7449  | 1540    | 1258            |       |  |
| Engineering        | 8795  | 1525    | 1286            |       |  |
| Legal              | 5648  | 1320    | 1156            |       |  |
| Research           | 5714  | 1303    | 1133            |       |  |
| Marketing          | 4672  | 1301    | 1213            |       |  |
| Accounting         | 8748  | 1301    |                 |       |  |
| ITOperations       | 6440  | 1220    | 1062            |       |  |



## CIS Control 18: Application Software Security

As an organization grows, custom applications are often developed to help with business workflow or other services which are offered to customers. These applications expose the organization to risk. Additionally, if the data stored is customer data, the customers may also be exposed. There are several tools in the market to help with Application Software Security. For example, the non-profit group [Open Web Application Security Project® \(OWASP\)](#) provides information to aid in the detection and mitigation of such risk.

CIS Control 18 states:

*“Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.*

*Why Is This CIS Control Critical?*

*Attacks often take advantage of vulnerabilities found in web-based and other application software. Vulnerabilities can be present for many reasons, including coding mistakes, logic errors, incomplete requirements, and failure to test for unusual or unexpected conditions. Examples of specific errors include: the failure to check the size of user input; failure to filter out unneeded but potentially malicious character sequences from input streams; failure to initialize and clear variables; and poor memory management allowing flaws in one part of the software to affect unrelated (and more security critical) portions.*

*There is a flood of public and private information about such vulnerabilities available to attackers and defenders alike, as well as a robust marketplace for tools and techniques to allow “weaponization” of vulnerabilities into exploits. In one attack, more than 1 million web servers were exploited and turned into infection engines for visitors to those sites using SQL injection. During that attack, trusted websites from state governments and other organizations compromised by attackers were used to infect hundreds of thousands of browsers that accessed those websites. Many more web and non-web application vulnerabilities are discovered on a regular basis.”*

[Tenable Web App Scanning](#) and Tenable Container Security products provide assistance in the discovery and assessment of application vulnerabilities. However, tools that review the source code should also be used. Detailed analysis tools can be integrated into the build process to assess the software against vulnerable libraries or common coding mistakes. Addressing vulnerable libraries or common mistakes can help address these risks.



---

## CIS Control 19: Incident Response and Management

---

A big part of a mature information security program is the Incidence Response (IR) program. The organization will grow into this practice as the size of the organization increases. However, the need for such a team remains constant. Many security incidents happen because a company is unaware of the asset or risk to the asset. The first and arguably most important step in vulnerability management is discovering assets, as risk can't be assessed, if the asset is unknown. Following all the preceding 18 CIS Controls will help bring awareness to the organization and the prepare the security team for the worst case scenario.

CIS Control 19 States:

*"Protect the organization's information, as well as its' reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.*

*Why Is This CIS Control Critical?*

*Cyber incidents are now just part of our way of life. Even large, well-funded, and technically sophisticated enterprises struggle to keep up with the frequency and complexity of attacks. The question of a successful cyber-attack against an enterprise is not "if" but "when."*

*When an incident occurs, it is too late to develop the right procedures, reporting, data collection, management responsibility, legal protocols, and communications strategy that will allow the enterprise to successfully understand, manage, and recover. Without an incident response plan, an organization may not discover an attack in the first place, or, if the attack is detected, the organization may not follow good procedures to contain damage, eradicate the attacker's presence, and recover in a secure fashion. Thus, the attacker may have a far greater impact, causing more damage, infecting more systems, and potentially exfiltrating more sensitive data than would otherwise be possible were an effective incident response plan in place."*

Tenable Security Center Continuous View provides a passive sensor that can help with enumeration of systems on the network. This passive sensor monitors network flows and looks for vulnerability based on clear text information or other traffic patterns. This detection method may assist



organizations during incident response (IR), as the passive data collected is another source of information. Tenable Security Center and this collected data is valuable to ensuring the IR team has the information they need, and a history of system vulnerabilities and configurations, especially when conducting post incident review and process improvements. For example, if the organization has a 90 day patch cycle, a major incident occurs, a finding may be the affected system was vulnerable for over 90 days. The organization should now consider changing the patching policy to a 45 day cycle. While Tenable Security Center is not an IR solution, much of the information collected and existing history can assist the organization should such an event occur.



---

## CIS Control 20: Penetration Tests and Red Team Exercises

---

As a final testament to a good security program, the CIS Control 20 recommends the organization test all the security controls. These exercises are very beneficial to training and security awareness. Many times well intended measures can be exploited. For example, a really strict password policy can result in users taping passwords to their keyboard. A great technical control, thwarted by a forgetful user and an observant adversary. Many times developers find protocols they find useful, and never realize there is an inherent security flaw, for example FTP and Telnet, are great tools. But in both cases, all credential exchanges are in clear text, allowing passwords and other information to be captured easily. Many chat programs use a form of HTTP and not HTTPS, again data is exchanged in the clear. With wireless technologies, many times with a simple wireless receiver, anyone can monitor the full exchanges of information. Penetration tests and red team exercises help to bring this information to the forefront of the security conversation.

CIS Control 20 states:

*“Test the overall strength of an organization’s defense (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.*

*Why Is This CIS Control Critical?*

*Attackers often exploit the gap between good defensive designs and intentions and implementation or maintenance. Examples include: the time window between announcement of a vulnerability, the availability of a vendor patch, and actual installation on every machine. Other examples include: well-intentioned policies that have no enforcement mechanism (especially those intended to restrict risky human actions); failure to apply good configurations to machines that come on and off of the network; and failure to understand the interaction among multiple defensive tools, or with normal system operations that have security implications.*

*A successful defensive posture requires a comprehensive program of effective policies and governance, strong technical defenses, and appropriate action by people. In a complex environment where technology is constantly evolving, and new attacker tradecraft appears regularly, organizations should periodically test their defenses to identify gaps and to assess their readiness by conducting penetration testing.”*

Tenable Security Center and Nessus are often good tools to use to aid in pre-assessment activities. Many red team members use Nessus as a network discovery tool. By using tools that do similar



tasks conducted by the adversaries, organizations are able to better detect and remediate the risk before the system is breached or compromised.

Referring back to the Basic Controls (CIS Control 1 - 6) these are the initial steps the red team will perform. The first step is to scan the network and identify hardware, then software. Now the red team has targets, they will then begin to enumerate vulnerabilities and test for baseline configurations, and so on. After a good list of vulnerabilities are collected, the fundamental controls will be tested. The vulnerabilities discovered by Tenable Security Center have an attribute called, exploitable. With this attribute the organization can easily see the low hanging fruit and plan to take the required mitigation efforts.

Shown in the “Exploitable by Malware - Exploitable Matrix” the organization can quickly see which popular attack tools their environment is most exploitable by. In these cases there are well known and widely used tools to exploit vulnerable systems. The red team will often use these tools to illustrate the likelihood a system could be compromised. Many attackers may use the same tools, or develop their own, but in either case if the organization has several exploitable systems, then there is a lot of work needed before a penetration test will be valuable. Once a majority of these vulnerabilities are mitigated, then the red team should be engaged.

| Exploitable by Malware - Exploitable Matrix |       |                           |                           |                           |
|---|-------|---------------------------|---------------------------|---------------------------|
|   | Total | Medium                    | High                      | Critical                  |
| Exploitable                                 | 3619  | <div><div></div>35%</div> | <div><div></div>48%</div> | <div><div></div>15%</div> |
| Malware                                     | 1488  | <div><div></div>9%</div>  | <div><div></div>68%</div> | <div><div></div>23%</div> |
| Core Impact                                 | 880   | <div><div></div>16%</div> | <div><div></div>64%</div> | <div><div></div>21%</div> |
| Canvas                                      | 416   | <div><div></div>22%</div> | <div><div></div>63%</div> | <div><div></div>14%</div> |
| Elliot                                      | 5     | <div><div></div>60%</div> | <div><div></div>40%</div> | <div><div></div>0%</div>  |
| ExploitHub                                  | 0     | <div><div></div>0%</div>  | <div><div></div>0%</div>  | <div><div></div>0%</div>  |
| Metasploit                                  | 684   | <div><div></div>13%</div> | <div><div></div>60%</div> | <div><div></div>26%</div> |
| Bad AutoRuns                                | 0     | NONE                      | NONE                      | <div><div></div>0%</div>  |

While Exploitable is a great attribute to use, in some cases an exploitable attribute may require a perfect storm condition. As this is the case, Tenable created the [Vulnerability Priority Rating \(VPR\)](#). VPR is the output of [Tenable Predictive Prioritization](#), and helps organizations improve their remediation efficiency and effectiveness by rating vulnerabilities based on severity level, technical impact, and threat. The technical impact measures the impact on confidentiality, integrity and availability following exploitation of a vulnerability and is equivalent to the CVSSv3 impact subscore. The threat





component reflects both recent and potential future threat activity against a vulnerability. Factors that influence VPR are public proof-of-concept (PoC) research, reports of exploitation on social media, and many others. These are primary factors used by the organization to prioritize mitigation efforts before the red team arrives, and these are the vulnerabilities that will have attempts at exploitation first. Tenable Security Center is a good source to help prepare plans to mitigate risk and complete the final control in the CIS CAS.

#### VPR Summary - First Discovered Vulnerabilities

|                 | Low (VPR 0.0-3.9) | Medium (VPR 4.0-6.9) | High (VPR 7.0-8.9) | Critical (VPR 9.0-10) |
|-----------------|-------------------|----------------------|--------------------|-----------------------|
| Current Month   | 13                | 28                   | 15                 | 3                     |
| Last Month      | 2014              | 4963                 | 62                 | 372                   |
| Current Quarter | 2028              | 4994                 | 77                 | 378                   |
| Last Quarter    | 20                | 58                   | 12                 | 5                     |
| > 180 Days      | 1420              | 3683                 | 1452               | 666                   |



## Tenable Security Center CAS Dashboard

To help bring all of the CAS controls together under one view, Tenable has created the **Implementing the CIS Control Assessment Specification (CAS)** dashboard and report for Tenable Security Center. In this dashboard and report, all the controls are brought together with corresponding audit files. A single matrix component exists for each control capturing the defined measures. For each measure there is a corresponding cell that has the vulnerability count and/or host count for each sub-control. Setting the focus allows the security team to use these numbers or queries to generate the needed information for each of the metric calculations.

To install the CAS Implementation Group 1 (IG1) dashboard:

1. Navigate to the **Dashboard** page.
2. Select **Add Dashboard** under options.
3. Search for "Implementing the CIS Control Assessment Specification (CAS)".

**Note:** Use quotes when searching for the dashboard.



4. After selecting the Dashboard, select **Add** at the bottom of the page.





After installing the dashboard from the feed, take a minute to review the contents in each matrix. This dashboard is specifically designed to work with this guide. For each control, where data can be displayed, there is a corresponding matrix. These cells provide the queries for a specific metric or input. The column or row headers indicate the sub-control or the focus related to the sub-control. The first component in the upper left hand corner is crafted to take full use of the questionnaire file **CAS Implementation Group 1 Audit File**.

Implementing the CIS Control Assessment Specification (CAS)

Switch Dashboard

Options

CAS IG1 - Audit Questions Pass/Fail

|                |              |            |            |            |
|----------------|--------------|------------|------------|------------|
| Data Collected | Data Missing | Control 1  | Control 2  | Control 3  |
| Control 4      | Control 5    | Control 6  | Control 7  | Control 8  |
| Control 10     | Control 12   | Control 13 | Control 14 | Control 16 |

Last Updated: 3 minutes ago

CAS IG1 - Control 1

|               |                   |      |
|---------------|-------------------|------|
|               | Ground Truth (Up) | Down |
| CAS 1.4 & 1.6 | 1                 | 0    |

Last Updated: 10 minutes ago

CAS IG1 - Control 2

|              |                      |                  |
|--------------|----------------------|------------------|
| Applications | Unsupported Products | Unsupported Apps |
| 65           | 20                   | 5                |

Last Updated: 10 minutes ago

CAS IG1 - Control 3

|                 |                            |
|-----------------|----------------------------|
|                 | Hosts with Missing Patches |
| Sub-Control 3.5 | 60                         |

Last Updated: 10 minutes ago

CAS IG1 - Control 4

|                 |                                |
|-----------------|--------------------------------|
|                 | Hosts with Default Credentials |
| Sub-Control 4.2 | 0                              |

Last Updated: 9 minutes ago

CAS IG1 - Control 5

|                  |         |                     |        |        |        |
|------------------|---------|---------------------|--------|--------|--------|
|                  | Systems | Scans (Last 7 Da... | Passed | Manual | Failed |
| CIS CSC v7 Co... | 1       |                     | 0%     | 0%     | 100%   |

Last Updated: 8 minutes ago

CAS IG1 - Control 7

|                       |                            |
|-----------------------|----------------------------|
|                       | Hosts with Vulnerabilities |
| Web Browser Vulns     | 20                         |
| Email Vulnerabilities | 0                          |

Last Updated: 7 minutes ago

CAS IG1 - Control 8

|                 |  |
|-----------------|--|
|                 | Hosts with Outdated Antivirus Signatures |
| Sub-Control 8.2 | 0  |

Last Updated: 11 hours ago

CAS IG1 - Control 9

|                 |                  |                           |               |
|-----------------|------------------|---------------------------|---------------|
|                 | Windows Firewall | Windows Defender Firewall | *nix Firewall |
| Sub-Control 9.4 | 0                | 0                         | 29            |

Last Updated: 7 minutes ago

CAS IG1 - Control 11

|                  |   |
|------------------|---|
|                  | Network Devices Unsupported/Missing Patches |
| Sub-Control 11.4 | 1   |

Last Updated: 7 minutes ago

CAS IG1 - Control 12

|                  |                    |                     |                       |
|------------------|--------------------|---------------------|-----------------------|
|                  | Palo Alto Firewall | Cisco Router/Switch | Juniper Router/Switch |
| Sub-Control 12.1 | 0                  | 2                   | 3                     |

Last Updated: 6 minutes ago

CAS IG1 - Control 13

|                  |                                     |
|------------------|-------------------------------------|
|                  | Hosts with Potential Sensitive Data |
| Sub-Control 13.1 | 0                                   |

Last Updated: 6 minutes ago

CAS IG1 - Control 15

|                   |               |
|-------------------|---------------|
| Wireless Networks | No Encryption |
| Other Encryption  | AES Only      |

Last Updated: 5 minutes ago

CAS IG1 - Control 16

|                          |            |                     |
|--------------------------|------------|---------------------|
|                          | Host Count | Vulnerability Count |
| Sub Control 16.8 & 16. 9 | 23         | 245                 |
| Sub Control 16.11        | 0          | 0                   |

Last Updated: 5 minutes ago

Taking into consideration working active scanning and passive monitoring activities, the dashboard initially populates with valuable information that will assist with understanding of the IG1



requirements. As mentioned throughout the document, the data collected is often beneficial for all IG levels, and for completeness we show the data in IG1, even though the requirement is IG2. For example, focusing on [Control 1](#), the requirement is to maintain an inventory. Shown below in the **CAS IG1 - Control 1** matrix, the counts provide data that helps to populate the inventory, but is not actually the organization's inventory.

| CAS IG1 - Control 1          |                   |      |
|------------------------------|-------------------|------|
|                              | Ground Truth (Up) | Down |
| CAS 1.4 & 1.6                | 1                 | 0    |
| Last Updated: 10 minutes ago |                   |      |

**Note:** For information about scanning and collecting data, see the [Tenable Security Center Large Enterprise Deployment Guide](#) and the [Tenable Professional Services Scan Strategy Guide](#).

The results from the **CAS Implementation Group 1 Audit File** help drive focus on more administrative controls, such as the existence of a policy and where it is located. Risk managers are frequently asked to provide a single report to auditors, and to provide all the data related to the audit. The audit file feature allows risk managers and the security team to provide answers to the audit questions. The first cells provide an indicator of the data collection process. If the answers are any value other than the default of “None” or “No”, the “Data Collected” indicator will be enabled. For any of the questions that are still the default, the “Data Missing” indicator will be enabled. For each of the controls with questions that are present in the audit file, there is a separate question.

| CAS IG1 - Audit Questions Pass/Fail |              |            |            |            |
|-------------------------------------|--------------|------------|------------|------------|
| Data Collected                      | Data Missing | Control 1  | Control 2  | Control 3  |
| Control 4                           | Control 5    | Control 6  | Control 7  | Control 8  |
| Control 10                          | Control 12   | Control 13 | Control 14 | Control 16 |
| Last Updated: 3 minutes ago         |              |            |            |            |

The **Implementing the CIS Control Assessment Specification (CAS)** report will provide all the queries listed in the dashboard in a more expanded format. For example, all the indicators will list detailed tables with the content presented in an easy to understand format. The dashboard and report facilitates cybersecurity success by guiding the organization through the CIS CAS IG1. Risk



managers and CISO's are able to review the IG1 steps in CAS, and then focus the operations team to implement the required controls.

Tenable provides organizations with the means to effectively address a number of the security challenges with implementing the CIS Controls v7 and assists with navigating the CAS. Tenable Security Center Continuous View is the most strategic source to start cyber hygiene for both public and private sector organizations, making foundational cybersecurity more affordable, accessible, and actionable. By providing this guide, dashboard, and report, Tenable is the first and only vendor to automate both the implementation and auditing of an organization's adherence to IG1, maximizing limited budgets and resource-constrained teams. Tenable Security Center and CAS together helps organizations transform the Controls into actionable cybersecurity recommendations and integrate basic cyber hygiene across their operations.



---

## Appendix

---

- [Audit File Scan Tutorial](#)
  - [CIS CAS Audit Requirements](#)
  - [Create a New Repository + Scan Zone](#)
  - [Create a New Audit File + Policy](#)
  - [Create a Scan](#)
  - [Run Scan + See the Results](#)
- [CAS Implementation Group 1 Audit Questions](#)





---

## Audit File Scan Tutorial

---

This tutorial walks you through creating a policy compliance scan using a custom audit file. The tutorial is written with the assumption that the scan will be run on a known and scanned target. Additionally, when selecting a target to scan, the system should be RHEL 7 or CentOS 7 server. For ease of operation, Tenable recommends that you scan a single system and set up a single repository so the data will not be a part of any other scan result. By using a target that is known, and scans that are already working, the policy creation is much easier. The tutorial also assumes that the target system is being scanned with valid credentials, and the credentials have elevated permissions. Note that these audit checks will not actually do any scanning on the system, but the individual plugins that are used to perform the audit needs the same access as if a typical audit scan is being executed. Finally, we'll want to create a new repository and scan zone to isolate the scan data to ensure that only the desired target is being scanned.



---

## CIS CAS Audit Requirements

---

- Red Hat 7 or CentOS 7
- Root credentials
- Successful scans currently completed
- Separate repository used for the audit data collected
- Separate scan zone with only the single target used in the scan



## Create a New Repository + Scan Zone

The creation of a new repository and scan zone ensures that existing data won't be affected. To create a new repository and scan zone:

1. While logged in as an admin user, navigate to **Repositories** and click **Add** button. You should then select **IPv4 repository**.
2. Enter a name in the **Name** field and an IP range in the **IP Ranges** field. The IP range should be just the system that will be scanned to ensure that no other targets are scanned. Additionally, ensure that an organization is selected to allow a security manager to access the repository.
3. Under the **Resources** menu in the top bar, click **Scan Zones**.
4. Enter the required fields, **Name** and **Ranges**. The IP range should be just the system that will be scanned to ensure that no other targets are scanned. Ensure a scanner is selected.

The screenshot displays the Tenable.sc web interface. At the top, the navigation bar includes 'Dashboard', 'Resources', 'Repositories', 'Organizations', 'Users', 'Scanning', and 'System'. The 'Repositories' section is active, showing a table with columns for Name, Vulnerability Count, IP/Device Count, Type, and Last Updated. An 'Add' button is visible in the top right. A red arrow labeled '1' points to this button. Below the table, the 'Add Repository' form is shown with fields for Name (pre-filled with 'CIS CAS IG 1'), Description, IP Ranges (pre-filled with '0.0.0.0/0'), Organizations, and Advanced Settings. A red arrow labeled '2' points to the IP Ranges field. To the right, the 'Scan Zones' section is visible, showing a table with columns for Name, Vulnerability Count, IP/Device Count, Type, and Last Updated. A red arrow labeled '3' points to the 'Scan Zones' link in the left sidebar. Below the table, the 'Add Scan Zone' form is shown with fields for Name (pre-filled with 'CIS CAS IG 1'), Description, Ranges, and Scanners. A red arrow labeled '4' points to the Ranges field.

After creating the repository and scan zone, the next step is to prepare the requirements for the scan (Audit file, Credentials, and Policy). The credentials for the target should be known, therefore they will be re-used. Next the audit file must be imported before creating the policy. The questions for the audit file are listed in [CAS Implementation Group 1 Audit Questions](#) along with the possible values. Please refer to the questions before uploading the audit file.

**Note:** The answers to the questions also have a character limit of 160



The scan will use a **Policy Compliance Auditing** policy since the scan will be run on a known target, but if the scan will be done on a new target it may be helpful instead create a custom policy with only the “General”, “Policy Compliance”, and “Settings” plugin families enabled. Having the custom policy for the scan will allow the user to troubleshoot the scan easily if something fails (ex. credentials).



## Create a New Audit File + Policy

To create a new audit file and policy as a security manager user:

1. Under **Scans**, navigate to **Audit Files** and add the **CAS Implementation Group 1** audit file.
2. In the **Name** field, enter a name.
3. Fill out the compliance questions with the answers as described in [CAS Implementation Group 1 Audit Questions](#).

**Note:** The audit questions have two parts. The first part requires a Yes or No. The second part requires a location. If the answer to the first question is No then the answer to the second question should be "None". Every audit question that is answered "Yes" will pass, while every "No" will fail.

4. Under **Scans**, navigate to **Policies** and add a **Policy Compliance Auditing** policy.
5. Add the audit file that was created above, under **Compliance**.

The screenshot shows the Tenable.sc interface with two main panels. The left panel is titled 'Add Audit File Template' and shows the 'CAS Implementation Group 1 Audit File' template. The 'General' section has a 'Name' field with 'CIS CAS IG 1' and a 'Description' field. The 'Compliance Checks' section has two questions: '1.4 - Maintain Detailed Asset Inventory\*' with a 'No' answer, and '1.4: Location of Policy or Policy Statement\*' with a 'None' answer. The right panel is titled 'Edit Policy > Policy Compliance Auditing' and shows the 'General' section with a 'Name' field containing 'CIS CAS IG 1'. The 'Configuration' section is visible at the bottom. A table at the bottom shows the 'Policies' list with columns: Name, Tag, Type, Group, Owner, and Last Modified. The table contains one entry: 'CIS CAS IG 1', 'Advanced Scan', 'Administrator', 'Administrator', and '5 minutes ago'.

| Name         | Tag | Type          | Group         | Owner         | Last Modified |
|--------------|-----|---------------|---------------|---------------|---------------|
| CIS CAS IG 1 |     | Advanced Scan | Administrator | Administrator | 5 minutes ago |

After the policy is created the active scan can be created. Keep in mind, the target should match or be within the IP range that was input when creating the repository and scan zone.



## Create a Scan

To create a scan:

1. After creating an active scan, ensure the correct **Policy** is selected.
2. Ensure the correct **Import Repository** is selected.
3. Select the **Scan Credentials** that were created earlier.
4. Enter the target IP in **IPs / DNS Names**.

The screenshot shows the 'Create a Scan' form with the following sections and annotations:

- General** (left sidebar): Includes 'Submit' and 'Cancel' buttons.
- Targets** (left sidebar): Includes 'General', 'Settings', 'Targets', 'Credentials', and 'Post Scan' tabs.
- Target Type**: Set to 'IP / DNS Name'.
- IPs / DNS Names\***: A text input field containing '<TARGET IP>' with a red arrow labeled '4' pointing to it.
- Scan Credentials** (right sidebar): Includes 'SSH' and 'Linux Audit Creds' tabs, and a '+ Add Credential' button. A red arrow labeled '3' points to the 'SSH' tab.
- Basic** (middle section): Includes 'Scan Zone' (Automatic Distribution), 'Import Repository\*' (CIS CAS IG 1), 'Scan Timeout Act', and 'Rollover Schedule'. A red arrow labeled '2' points to the 'Import Repository\*' dropdown.
- Advanced** (bottom left): Includes 'Scan Virtual Hosts Headers', 'Track hosts which (e.g. DHCP)', 'Immediately remove that do not reply', and 'Max scan duration'.
- General** (bottom right): Includes 'Name\*' (CIS CAS IG 1), 'Description', 'Policy\*' (CIS CAS IG 1), and 'Schedule' (On Demand). A red arrow labeled '1' points to the 'Policy\*' dropdown.

Once the scan is created and run, the user can navigate to scan results and drill into the scan. Drilling into the scan result will bring the user to the **Vulnerability Analysis** page. Each CIS Control plugin name directly relates to all the previous questions that were answered in the audit file. High



severities indicate a failed compliance check, and info severities indicate a passed compliance check. If the auditing user input a "Yes" as a compliance check answer the check will have an info severity.



## Run Scan + See the Results

The scan should only be run on a system that has already been scanned or is known. Therefore, the scan shouldn't take much time at all to run.

To see the scan results:

1. Select the correct scan under **Scan Results** to see the **Vulnerability Analysis** page.

tenable.sc Dashboard Solutions Analysis Scans Reporting Assets Workflow Users secManager

All Vulnerability Analysis : Test Audit - (Oct 01, 2020) Options

Filters Vulnerability Summary Jump to Vulnerability Detail List Total Results: 28

| Plugin ID | Name   | Family | Severity | VPR | Host Total | Total |
|-----------|--|--------|----------|-----|------------|-------|
| 1000031   | CIS Control 1 (1.4) Maintain Detailed Asset Inventory  | N/A    | Info     |     | 1          | 1     |
| 1000032   | CIS Control 1 (1.6) Ensure that unauthorized assets are removed, quarantined or the inventory is updated | N/A    | Info     |     | 1          | 1     |
| 1000035   | CIS Control 3 (3.4(a)) Deploy Automated Operating System Patch Management Tools                          | N/A    | Info     |     | 1          | 1     |
| 1000036   | CIS Control 3 (3.4(b)) Deploy Automated Operating System Patch Management Tools                          | N/A    | Info     |     | 1          | 1     |
| 1000038   | CIS Control 3 (3.6(a)) Deploy Automated Software Patch Management Tools                                  | N/A    | Info     |     | 1          | 1     |
| 1000039   | CIS Control 3 (3.6(b)) Deploy Automated Software Patch Management Tools                                  | N/A    | Info     |     | 1          | 1     |
| 1000040   | CIS Control 4 (4.2) Change Default Passwords   | N/A    | Info     |     | 1          | 1     |
| 1000042   | CIS Control 5 (5.1) Establish Secure Configurations  | N/A    | Info     |     | 1          | 1     |
| 1000051   | CIS Control 10 (10.5) Ensure All Backups Have at Least One Offline Backup Destination                    | N/A    | Info     |     | 1          | 1     |
| 1000033   | CIS Control 2 (2.1(a)) Maintain and Inventory of Authorized Software                                     | N/A    | High     |     | 1          | 1     |
| 1000034   | CIS Control 2 (2.1(b)) Maintain and Inventory of Authorized Software                                     | N/A    | High     |     | 1          | 1     |
| 1000037   | CIS Control 3 (3.4(c)) Deploy Automated Operating System Patch Management Tools                          | N/A    | High     |     | 1          | 1     |
| 1000041   | CIS Control 4 (4.3) Ensure the Use of Dedicated Administrative Accounts                                  | N/A    | High     |     | 1          | 1     |
| 1000043   | CIS Control 6 (6.2(a)) Activate Audit Logging  | N/A    | High     |     | 1          | 1     |
| 1000044   | CIS Control 6 (6.2(b)) Activate Audit Logging  | N/A    | High     |     | 1          | 1     |

Select Filters Clear Filters Load Query





## CAS Implementation Group 1 Audit Questions

A "Yes" equates to a pass and a "No" equates to a fail. If "Yes", the location or specific answer is needed in the second part of the audit question. For example, for 1.4 - Maintain Detailed Asset Inventory, if the answer is yes, then you must answer the second part of the audit question about the location of the policy or policy statement. Please note there is a 160 character limit for each answer.

| Audit Question  | Answer |
|---|--------|
| 1.4 - Maintain Detailed Asset Inventory                   | No     |
| 1.4: Location of Policy or Policy Statement               | None   |
| 1.6 - Unauthorized assets are removed                     | No     |
| 1.6: Timeframe for removing/updating assets               | 999    |
| 10.1 - Ensure Regular Automated Backups                   | No     |
| 10.1: Location of List of which services are in use       | None   |
| 10.2 - Perform Complete System Backups                    | No     |
| 10.4 - Protect Backups                                    | No     |
| 10.5 - Ensure All Backups Have Offline Backup Destination | No     |
| 12.1 - Maintain an Inventory of Network Boundaries        | No     |
| 12.1: Location of the diagram/plan                        | None   |
| 12.4(a) - Deny Communications Over Unauthorized Ports     | No     |
| 12.4(a): Location of the list/document                    | None   |
| 12.4(b) - Deny Communications Over Unauthorized Ports     | No     |
| 12.4(b): Location of Policy or Policy Statement           | None   |
| 13.1 - Maintain an Inventory of Sensitive Information     | No     |
| 13.1: Location of Policy or Policy Statement              | None   |



|  |      |
|--|------|
| 13.2 - Remove Sensitive Data on Systems Not Accessed             | No   |
| 13.2: Location of Policy or Policy Statement                     | None |
| 13.6 - Encrypt Mobile Device Data                                | No   |
| 13.6: Location of Policy or Policy Statement                     | None |
| 14.6 - Protect Information Through Access Control Lists          | No   |
| 14.6: Location of Policy or Policy Statement                     | None |
| 2.1(a) - Maintain an Inventory of Authorized Software            | None |
| 2.1(a): Location of List of Approved Software                    | None |
| 2.1(b)) - Maintain Inventory of Authorized Software              | No   |
| 2.1(b): Location of Policy or Policy Statement                   | None |
| 3.4(a) - Deploy Automated OS Patch Management Tools              | No   |
| 3.4(a): Location of Policy or Policy Statement                   | None |
| 3.4(b) - Deploy Automated OS Patch Management Tools              | No   |
| 3.4(b): Location of the exception policy                         | None |
| 3.4(b): Location of the list of endpoints that have an exception | None |
| 3.4(c)) - Deploy Automated OS Patch Management Tools             | None |
| 3.4(c): Location of Policy or Policy Statement                   | None |
| 3.6(a) - Deploy Automated Software Patch Management Tools        | No   |
|  |      |
| 3.6(a): Location of Policy or Policy Statement                   | None |
| 3.6(b) - Deploy Automated Software Patch Management Tools        | No   |
| 3.6(b): Location of the exception policy                         | None |
| 3.6(b): Location of the list of endpoints that have an exception | None |



|  |                |
|--|----------------|
| 4.2 - Change Default Passwords   | No             |
| 4.2: Location of Policy or Policy Statement  | None           |
| 4.3 - Ensure the Use of Dedicated Administrative Accounts                              | No             |
| 5.1 - Establish Secure Configurations  | No             |
| 5.1: Location of the Secure Configuration documentation                                | No             |
| 6.2(a) - Activate Audit Logging  | No             |
| 6.2(a): Location of Policy or Policy Statement   | None           |
| 6.2(b) - Activate Audit Logging  | No             |
| 7.7 - Use of DNS Filtering Services  | No             |
| 7.7: Location of List of which services are in use                                     | None           |
| 8.4 - Configure Anti-Malware Scanning of Removable Media                               | No             |
| 8.5 - Configure Devices to Not Auto Run Content  | No             |
| 16.8(a) - Does the Organization have a list of all business roles?                     | No             |
| 16.8(a) - Location of Policy or Policy Statement                                       | None           |
| 16.8(b) - Does the Organization have a list of all computer and applications accounts? | No             |
| 16.8(b) - Location of Policy or Policy Statement                                       | None           |
| Attesting user to the answers provided for this report.                                | Attesting User |