Tenable Cyber Exposure Study - Cyber Essentials

Last Revised: October 23, 2025

Copyright © 2025 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Table of Contents

About Cyber Essentials

The Cyber Essentials is a UK government-backed framework which is designed to assist organisations in protecting themselves against common threats. The Cyber Essentials is built on 5 key components that, when implemented correctly, can reduce cyber risk. The five key components are:

1. Firewalls and Boundary Devices
2. Secure Configurations
3. Access Control
4. Malware Protection
5. Patch Management

The Cyber Essentials provides a basic cyber security foundation that can serve as a stepping stone to a more comprehensive zero-trust approach. The Cyber Essentials is also available as a Cyber Essentials Plus certification. The Cyber Essentials Plus requires that an accredited certification body conduct an on-site or remote audit to verify compliance.

Zero-trust and the Cyber Essentials

The Cyber Essentials discusses zero-trust, and aligns with some of the principles of zero-trust, but is not a zero-trust framework. Zero-trust is based on the principles of never trust, always verify.

Some overlapping elements of the Cyber Essentials are:

- Access Control
- Secure Configuration
- Malware Protection
- Patch Management

Cyber Essentials does not enforce zero-trust because:

- There is no mandate for continuous verification/authentication beyond the initial login.
- Cyber Essentials does not require network segmentation, or granular access control beyond a basic firewall.
- Cyber Essentials has no explicit identity and device verification requirements, which zero-trust emphasises with device trust and behavior analytics.
- Cyber Essentials provides a solid starting point for zero-trust, but does not fully implement zero-trust. Organisations that are considering zero-trust principles should also add necessary additional layers like authentication, micro-segmentation, and real-time continuous monitoring into their cyber security strategy.

See Also

- Getting Started with the Scope of Assessment
- About Cyber Essentials
- Key Component 1: Firewalls and Internet Gateways
- Key Component 2: Secure Configuration
- Key Component 3: Access Control
- Key Component 4: Malware Protection
- Key Component 5: Patch Management
- References

Getting Started with the Scope of Assessment

Scope of Assessment (IASME Question Booklet)

You will also need to answer questions regarding the computers, laptops, servers, mobile

phones, tablets, firewalls/routers and cloud services that are connected to the internet and accessing organisational data or services. All locations that are owned or operated by this organisation or sub-set, whether in the UK or internationally, should be considered "in-scope".

The level of detail required for devices is as follows:

With the exception of network devices (such as firewalls and routers), all other devices within the scope of the certification only requires the information about the make and operating system.

Additionally, maintaining a comprehensive and up-to-date asset inventory is a fundamental and critical component of any vulnerability management program. Modern IT environments encompass on-premise, cloud infrastructure, mobile devices, ephemeral and transient assets, web applications, IoT devices, and more. Asset identification of all connected assets within an organisation is a common baseline requirement in a number of security standards and frameworks. Devices are detected through active scanning with Nessus and passive network analysis with Nessus Network Monitor to build a comprehensive list of assets and provide a clear picture of risk in the environment. For more detailed information on asset inventory and discovery reference the Asset Inventory and Discovery Cyber Exposure Guide.

See Also

- About Cyber Essentials
- Getting Started
- Key Component 1: Firewalls and Internet Gateways
- Key Component 2: Secure Configuration
- Key Component 3: Access Control
- Key Component 4: Malware Protection

Getting Started

Scope of Assessment (Asset Identification)

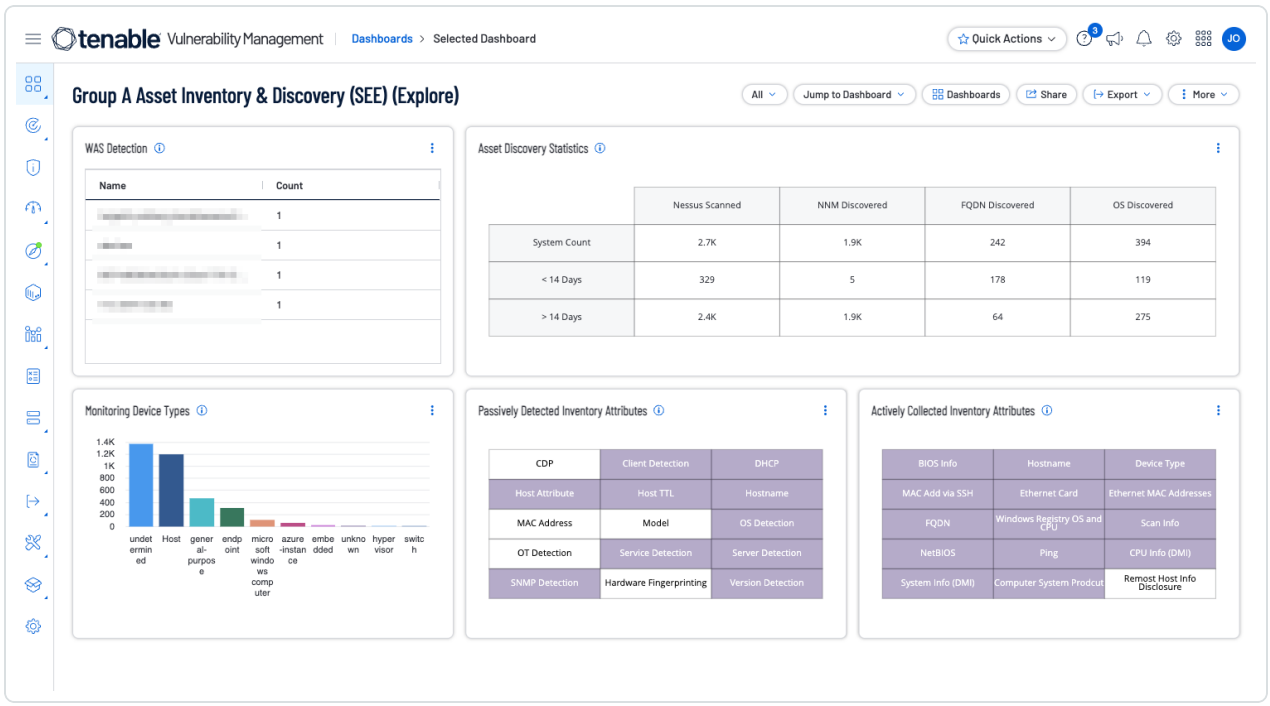
Asset identification can be difficult for a variety of reasons, such as Shadow IT, Large and Diverse Inventories, and Virtual and Cloud Assets. Tenable simplifies asset identification with a variety of methods.

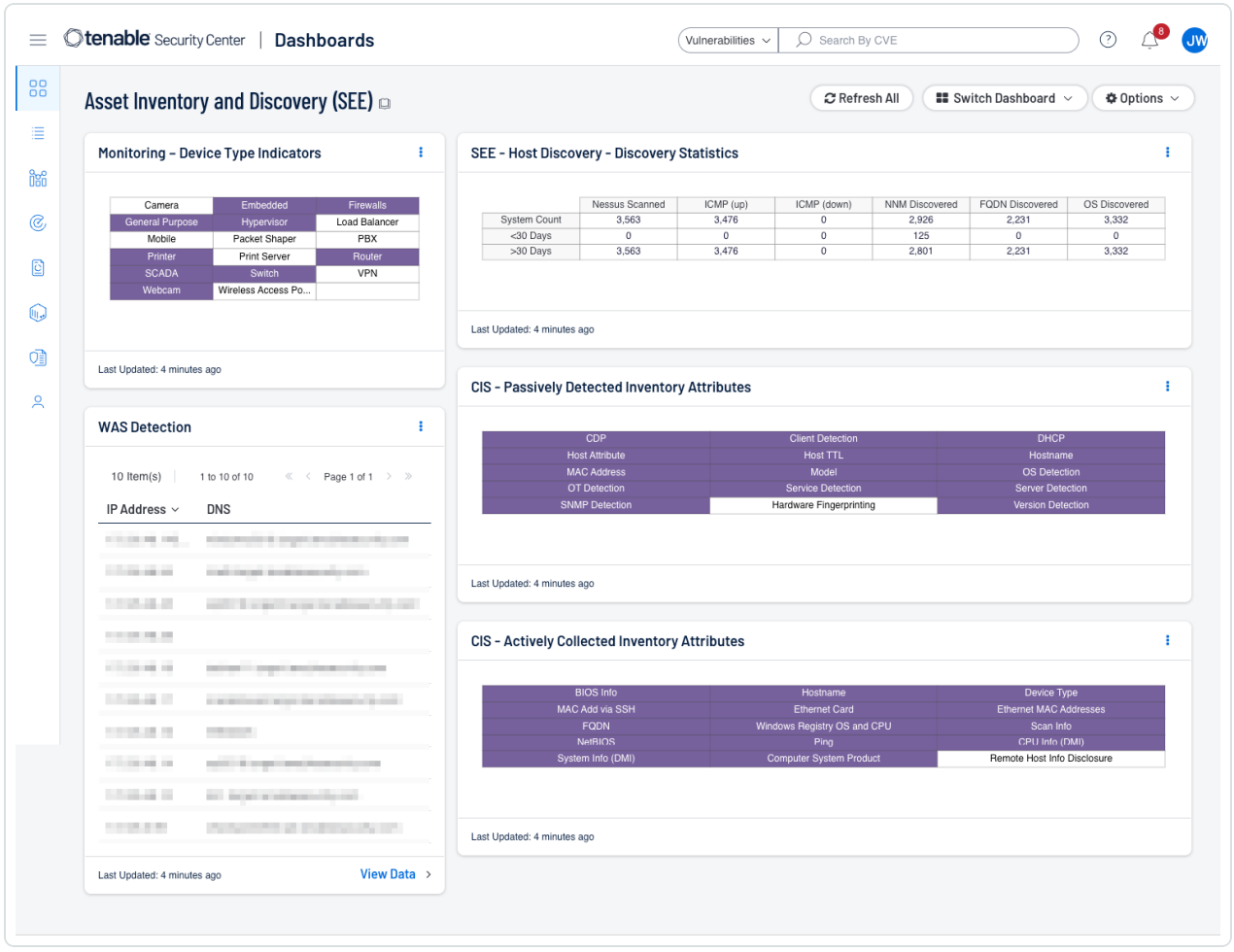
Active and Passive Scanning

Devices are detected through active scanning with Nessus and passive network analysis with Nessus Network Monitor to build a comprehensive list of assets and provide a clear picture of risk in the environment.

The Asset Inventory & Discovery (SEE) Tenable Vulnerability Management dashboard and the Asset Inventory & Discovery (SEE) Tenable.sc dashboard displayed the following provides guidance to establish an asset discovery, including:

- Actively and passively detected assets
- Asset discovery statistics
- Detected web applications
- Indications for device types (printers, cameras, routers, firewalls, WAPs)


tenable Vulnerability Management
Dashboards > Selected Dashboard
Quick Actions
Group A Asset Inventory & Discovery (SEE) (Explore)
All
Jump to Dashboard
Dashboards
Share
Export
More
WAS Detection
Name
Count
Asset Discovery Statistics
Nessus Scanned
NNM Discovered
FQDN Discovered
OS Discovered
System Count
2.7K
1.9K
242
394
< 14 Days
329
5
178
119
> 14 Days
2.4K
1.9K
64
275
Monitoring Device Types
1.4K
1.2K
1K
800
600
400
200
0
undetermined
Host
general-purpose
endpoint
microsoft windows computer
azure-instance
embedded
unknown
hypervisor
switch
Passively Detected Inventory Attributes
CDP
Client Detection
DHCP
Host Attribute
Host TTL
Hostname
MAC Address
Model
OS Detection
OT Detection
Service Detection
Server Detection
SNMP Detection
Hardware Fingerprinting
Version Detection
Actively Collected Inventory Attributes
BIOS Info
Hostname
Device Type
MAC Add via SSH
Ethernet Card
Ethernet MAC Addresses
FQDN
Windows Registry OS and CPU
Scan Info
NetBIOS
Ping
CPU Info (DMI)
System Info (DMI)
Computer System Prodcut
Remost Host Info Disclosure


tenable Security Center | Dashboards
Vulnerabilities
Search By CVE
Asset Inventory and Discovery (SEE)
Refresh All
Switch Dashboard
Options
Monitoring – Device Type Indicators
Camera
Embedded
Firewalls
General Purpose
Hypervisor
Load Balancer
Mobile
Packet Shaper
PBX
Printer
Print Server
Router
SCADA
Switch
VPN
Webcam
Wireless Access Po...
Last Updated: 4 minutes ago
SEE - Host Discovery - Discovery Statistics
Nessus Scanned
ICMP (up)
ICMP (down)
NNM Discovered
FQDN Discovered
OS Discovered
System Count
3,563
3,476
0
2,926
2,231
3,332
<30 Days
0
0
0
125
0
0
>30 Days
3,563
3,476
0
2,801
2,231
3,332
Last Updated: 4 minutes ago
WAS Detection
10 Item(s)
1 to 10 of 10
Page 1 of 1
IP Address
DNS
Last Updated: 4 minutes ago
View Data
CIS - Passively Detected Inventory Attributes
CDP
Client Detection
DHCP
Host Attribute
Host TTL
Hostname
MAC Address
Model
OS Detection
OT Detection
Service Detection
Server Detection
SNMP Detection
Hardware Fingerprinting
Version Detection
Last Updated: 4 minutes ago
CIS - Actively Collected Inventory Attributes
BIOS Info
Hostname
Device Type
MAC Add via SSH
Ethernet Card
Ethernet MAC Addresses
FQDN
Windows Registry OS and CPU
Scan Info
NetBIOS
Ping
CPU Info (DMI)
System Info (DMI)
Computer System Product
Remote Host Info Disclosure
Last Updated: 4 minutes ago

For more information on Asset Discovery and Classification see the Asset Inventory and Discovery Cyber Exposure Study.

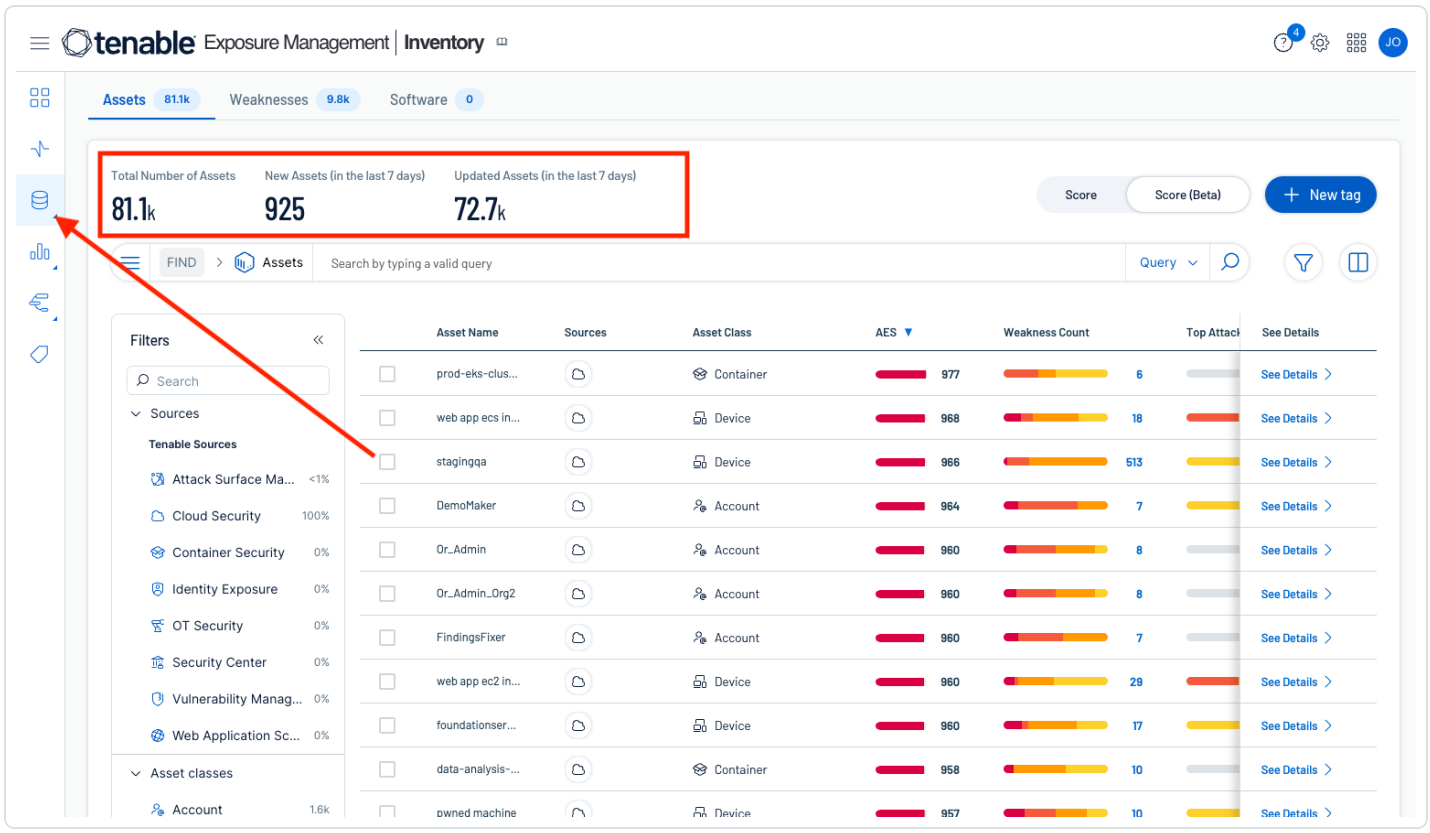
Tenable One (Exposure Management Platform)

Products such as Tenable Exposure Manage can provide asset inventory details. The Inventory Page on Tenable Exposure Management aggregates all assets and their associated entities to unify and operationalise the data. It focuses on your organization's ability to maintain an accurate inventory for all of your cyber-enabled technologies while providing data analytics and a comprehensive inventory across various sources. While asset management highlights processes and people that can be affected, Tenable Exposure Management takes this one step further by digging into the technologies that can be hacked and allowing you to gain insight into these exposures.

The **Inventory** page is the central repository of all cyber assets across an organization's attack surface by providing:

- A comprehensive list of all digital assets
- A complete view of risks using enriched context
- Built-in control, monitoring, and alerting
- Unified asset analysis to drive prioritization

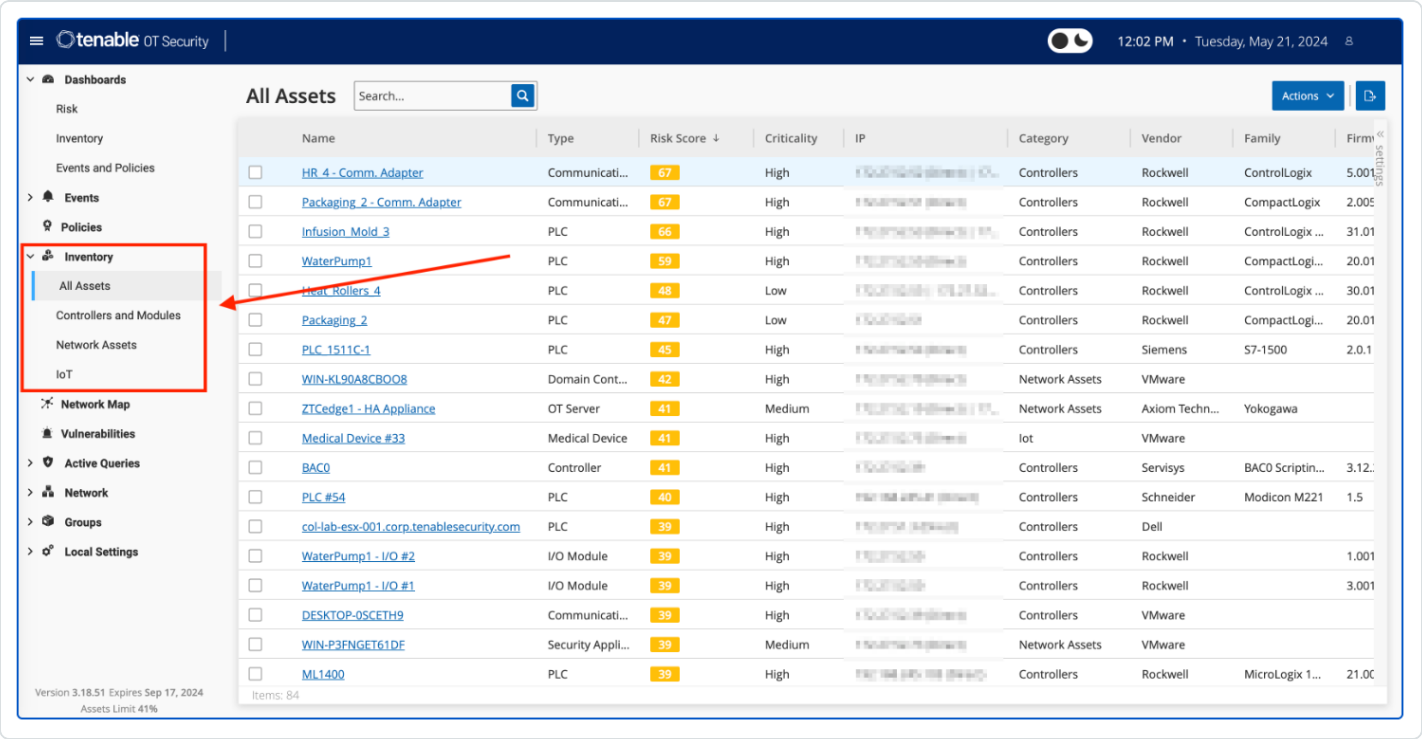
To access the inventory page first select the Inventory icon from the left navigation window, the Assets tab will display automatically, displaying asset counts on the top section.



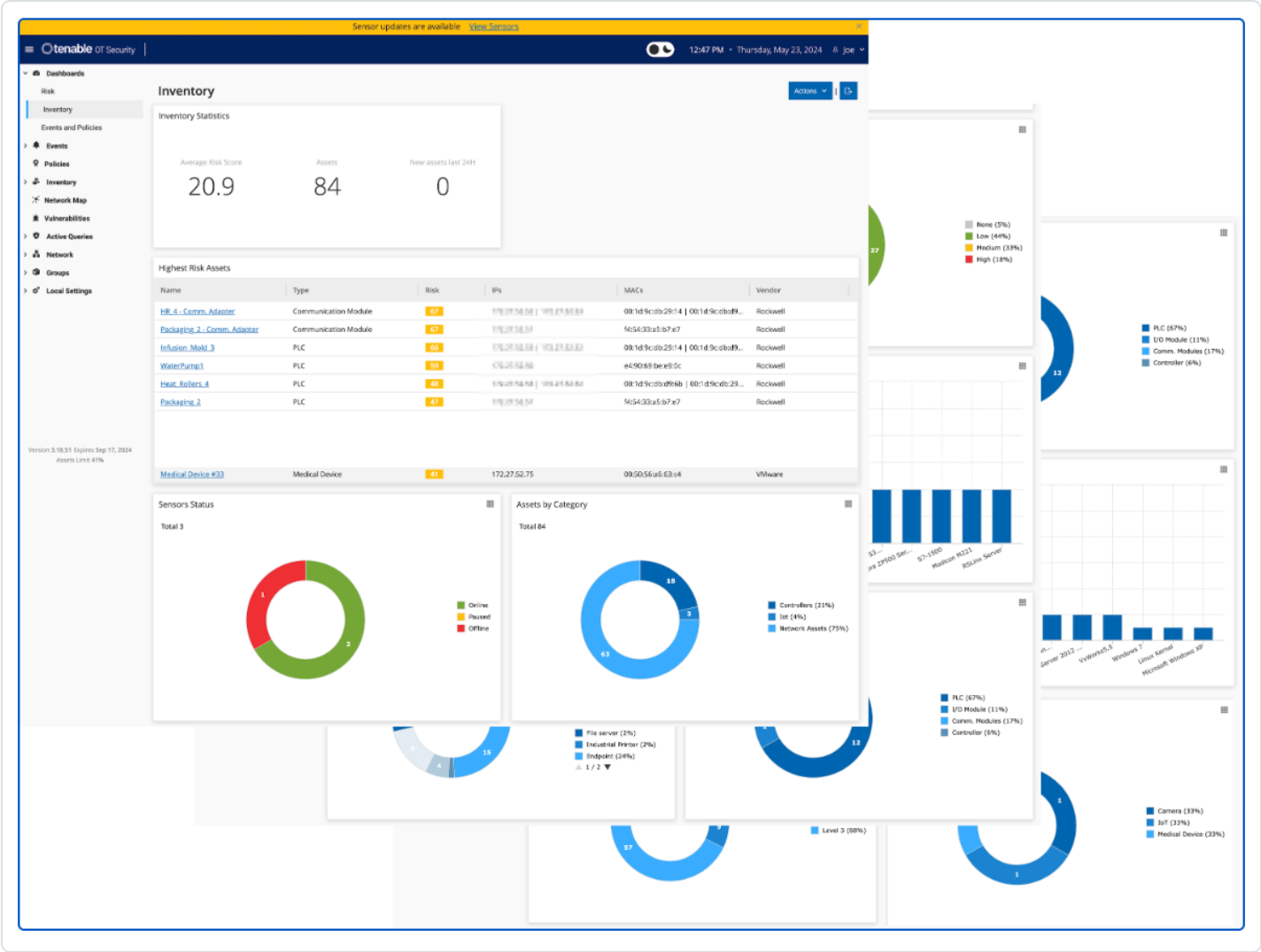
Tenable OT

For organisations with industrial controls devices that are in scope, identification of IoT assets is accomplished with Tenable OT Security. Native communication protocols are used to query both Information Technology (IT) and Operational Technology (OT) devices in your Industrial Control Systems (ICS) environment in order to identify all of the activities and actions occurring across your network. All the assets in the network appear on the Inventory page. The Inventory page includes details about the asset that enables comprehensive asset management as well as monitoring of the status of each asset and its related events. OT Security collects this data using the Network Detection and Active Query capabilities.

The **All Assets** page shows data for all types of assets. Subsets of assets are shown on separate screens for each of the following asset types: **Controllers and Modules**, **Network Assets**, and **IoT**.

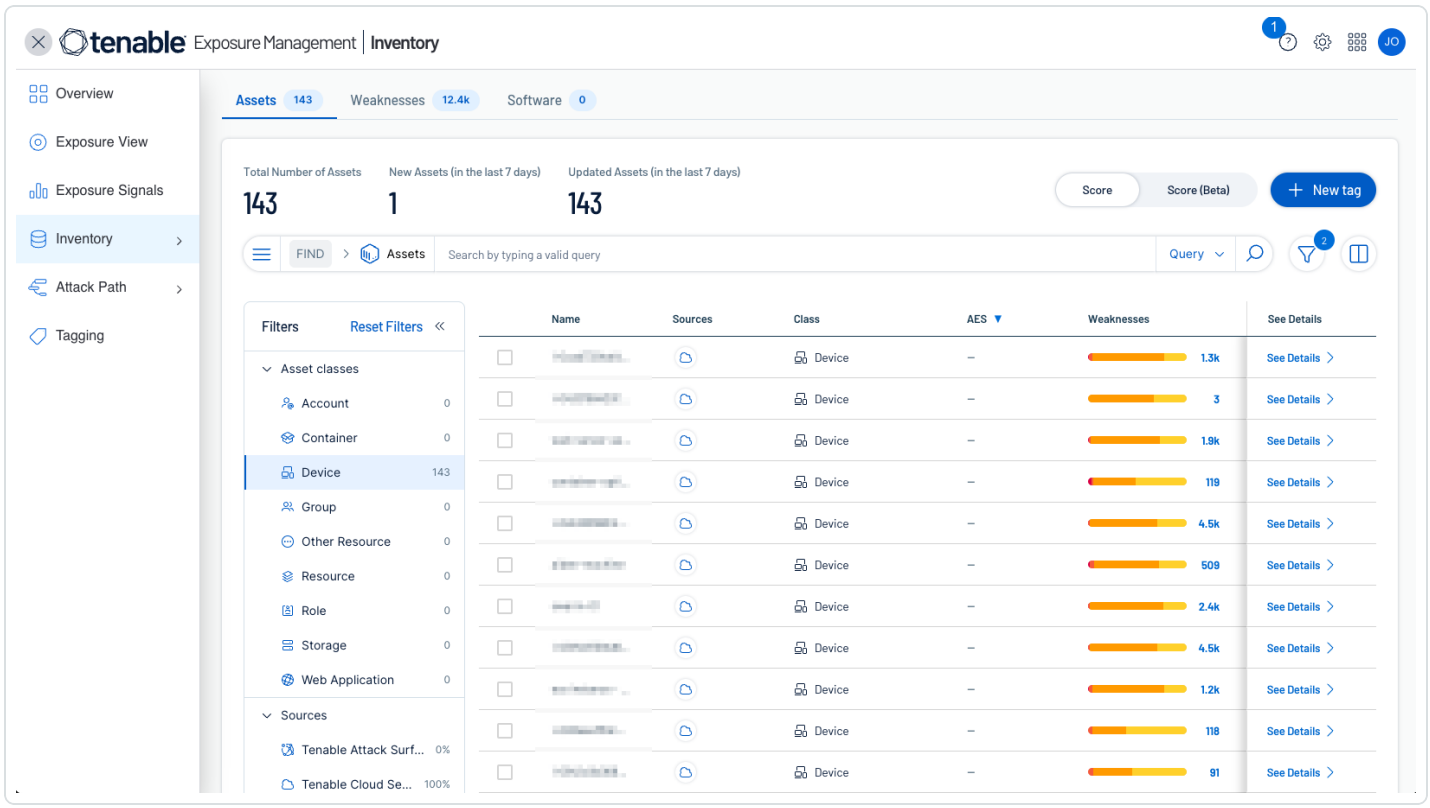


Tenable OT provides three in product dashboards that display assets in groupings such as by **Category**, **Vendor**, **Module Type**, **Purdue Level**, and more, facilitating asset management and tracking. Tenable OT Security provides a complete visibility of assets across the environment (IT and OT). A service called "Asset Gateway" receives asset information and tries to consolidate assets that have matching identifiers. In the case of an IT laptop, for example, we show "Sources" of Nessus, Agent, and Tenable OT Security all together. In the case of OT assets, they will not be merged into existing assets.



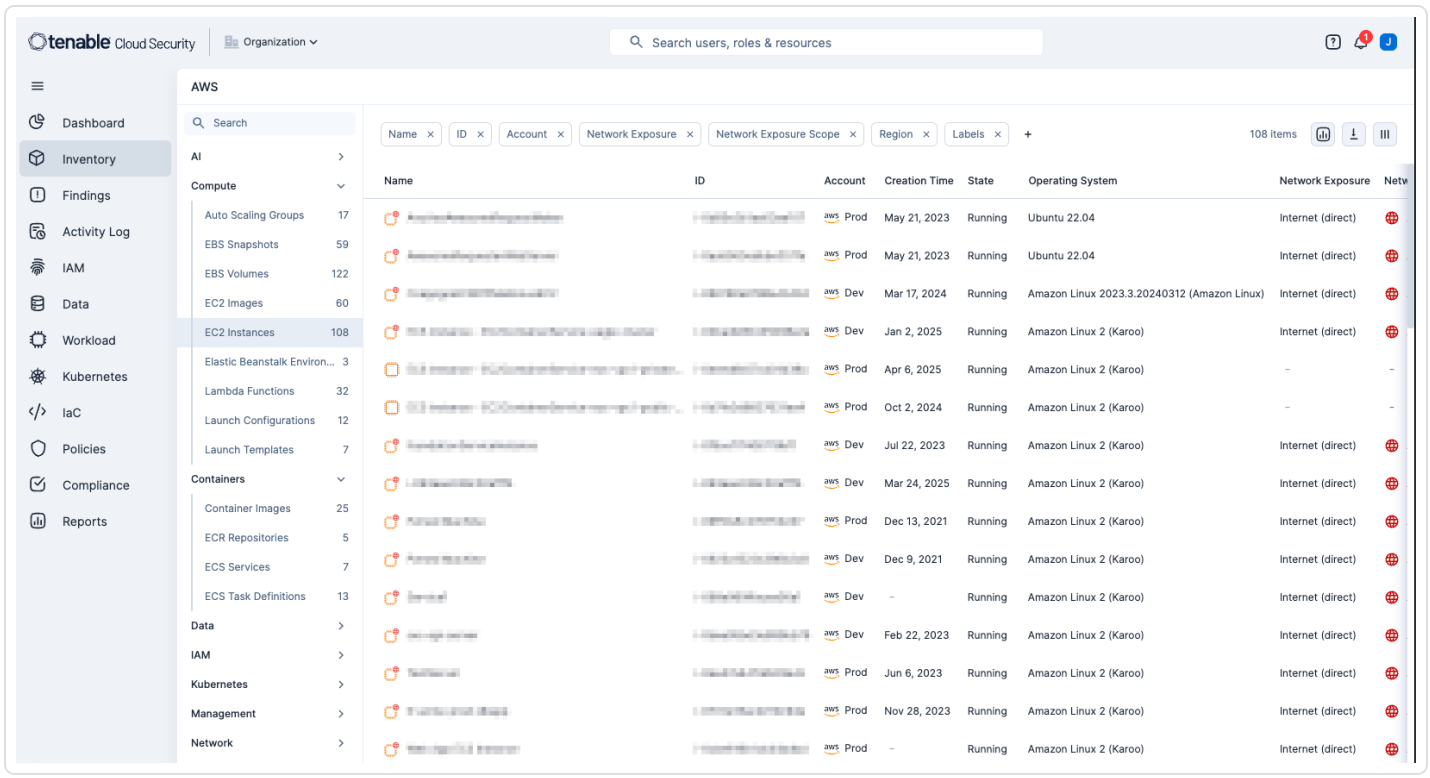
Tenable One is an exposure management platform, designed to allow customers to gain visibility across the entire modern attack surface. Tenable One focuses efforts to prevent likely attacks, and accurately communicate cyber risk to optimise business performance.

Tenable One Asset Inventory provides a comprehensive view of all assets across the entire attach surface. Sensors pull data from multiple applications across the platform, providing details on all known systems. At the highest level on the Asset Inventory page is shown the Number of Assets identified, New Assets identified in the last 7 days, and assets that have been updated in the last 7 days. Tenable One also integrates with third-party security tools to consolidate asset and vulnerability data, these integrations called Tenable One Connectors, allow organizations to ingest data from multiple sources, enriching asset inventory and enabling more effective risk assessment.



Tenable Cloud Security

Tenable Cloud Security is a Cloud Native Application Protection Platform (CNAPP) that assists organisations secure cloud environments. A few of Tenable Cloud Security's benefits include automated asset discovery, assessing and prioritising risks, and detecting threats in real-time. Cloud assets can be easily and quickly identified by navigating to the Inventory page where assets are listed by categories, such as AI, Compute, Containers, and more. In the example displayed below, Compute Assets, specifically EC2 instances are displayed.



See Also

- About Cyber Essentials
- Getting Started with the Scope of Assessment
- Key Component 1: Firewalls and Internet Gateways
- Key Component 2: Secure Configuration
- Key Component 3: Access Control
- Key Component 4: Malware Protection
- Key Component 5: Patch Management
- References

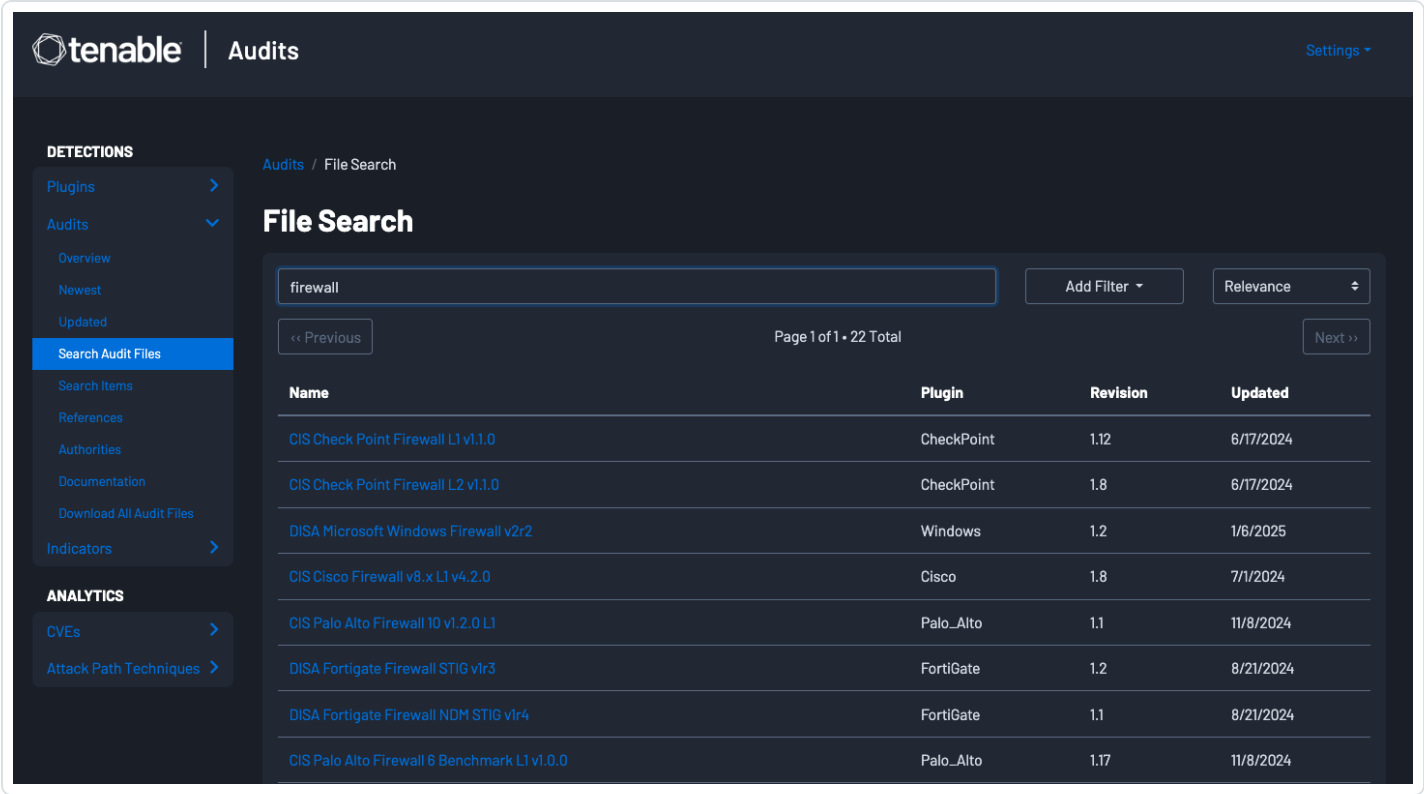
Key Component 1: Firewalls and Internet Gateways

The focus of this key component is Firewalls and Internet Gateways. This key component applies to all the following in scope devices: Boundary Firewalls, Desktop Computers, Laptops, Routers, Servers, Iaas, PaaS, and SaaS devices. Devices must be secure and only necessary network services should be able to be accessed from the Internet. The objective of this key component is the control of inbound/outbound traffic.

This requirement applies to every in scope device, and can be achieved using Boundary Firewalls to restrict inbound or outbound traffic, a software firewall which is installed and configured on each end point device, or for cloud services, data flow policies. Most end point devices, such as desktops and laptops come with software firewalls pre-installed, and the Cyber Essentials recommends that these services be enabled. Essentially, every in-scope device must be protected by either a properly configured firewall, or a network device with firewall functionality.

> **Note**: The Cyber Essentials: Requirements for IT infrastructure v3.1, published by the National Cyber Security Centre, a part of GCHQ specifies “Most desktop and laptop operating systems now come with a software firewall pre-installed, we advise that these are turned on in preference to a third-party firewall application.”

Tenable provides audit files for a number of firewall vendors, such as Palo Alto, Check Point, Fortigate, Cisco, and more. Audit files can be reviewed online here. Unless otherwise specified, recommended audit files would be those such as the Center for Internet Security (CIS) labeled audit files, which has a global mission. The CIS audit files are based on the CIS Controls and Benchmarks, which test for applicable items within the categories of Identification and Authentication, Access Control, System and Communications Protection, and Configuration Management.



Note: When scanning firewalls, run the scan against the Management Interface with the proper credentials. Interfaces other than the Management Interface may block/restrict some interactions which would prevent a complete scan.

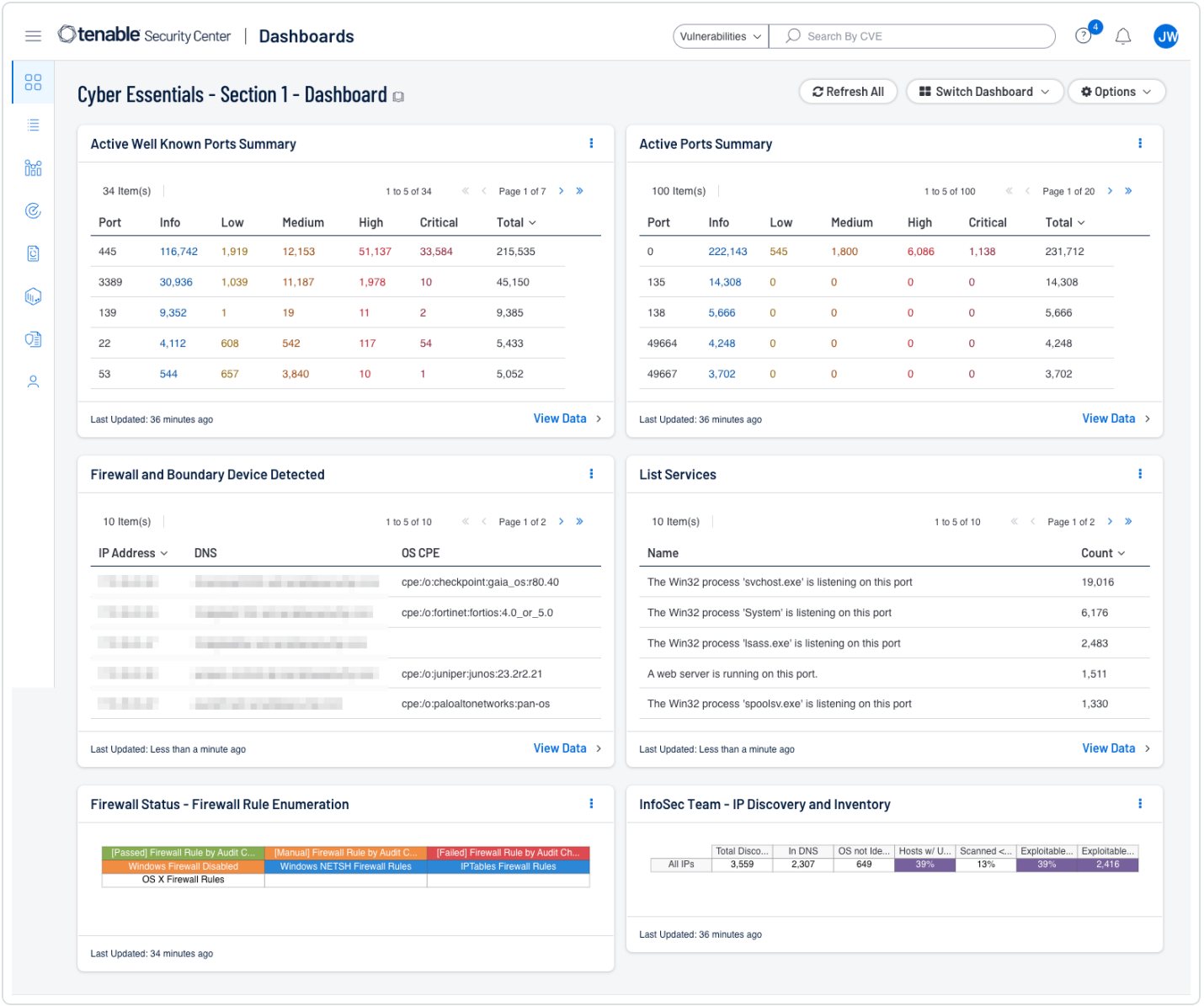
More information on configuring and using audit files can be found in the Tenable Documentation for Tenable Security Center, and Tenable Vulnerability Management. Detailed information is also available in the Tenable Compliance Checks Reference Guide.

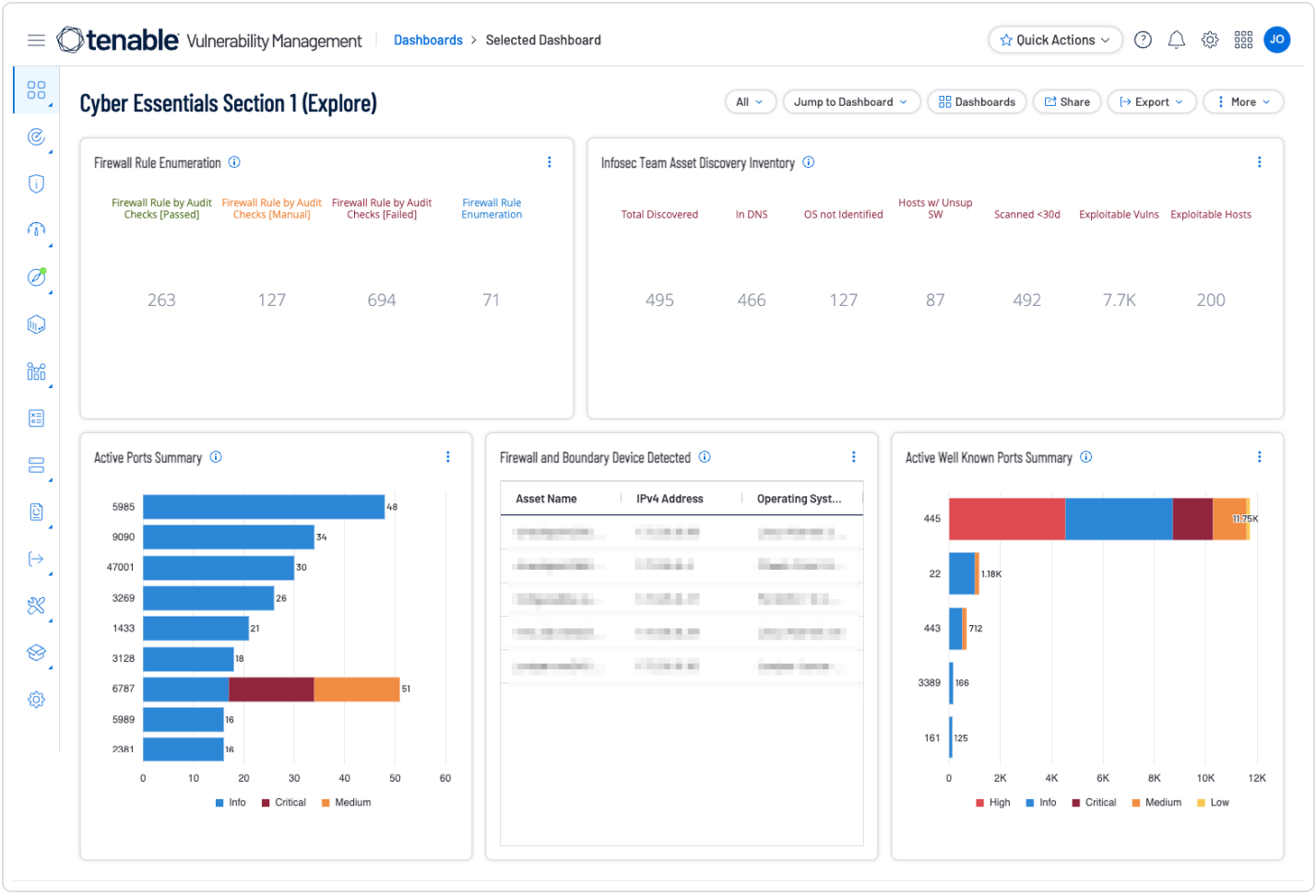
Tenable has provided a Cyber Essentials Dashboard and Report for Tenable Security Center and Tenable Vulnerability Management for this Key Component. Those dashboards and reports can be found here by using the term “Cyber Essentials” as a search query:

Security Center Dashboards and Reports

Vulnerability Management Dashboards and Reports

Shown below are screenshots of the this sections dashboards for Security Center and Vulnerability Management.


tenable Security Center | Dashboards
Vulnerabilities
Search By CVE
JW
Cyber Essentials - Section 1 - Dashboard
Refresh All
Switch Dashboard
Options
Active Well Known Ports Summary
34 Item(s)
1 to 5 of 34
Page 1 of 7
Port Info Low Medium High Critical Total
445 116,742 1,919 12,153 51,137 33,584 215,535
3389 30,936 1,039 11,187 1,978 10 45,150
139 9,352 1 19 11 2 9,385
22 4,112 608 542 117 54 5,433
53 544 657 3,840 10 1 5,052
Last Updated: 36 minutes ago
View Data
Active Ports Summary
100 Item(s)
1 to 5 of 100
Page 1 of 20
Port Info Low Medium High Critical Total
0 222,143 545 1,800 6,086 1,138 231,712
135 14,308 0 0 0 0 14,308
138 5,666 0 0 0 0 5,666
49664 4,248 0 0 0 0 4,248
49667 3,702 0 0 0 0 3,702
Last Updated: 36 minutes ago
View Data
Firewall and Boundary Device Detected
10 Item(s)
1 to 5 of 10
Page 1 of 2
IP Address DNS OS CPE
cpe:/o:checkpoint:gaia_os:r80.40
cpe:/o:fortinet:fortios:4.0_or_5.0
cpe:/o:juniper:junos:23.2r2.21
cpe:/o:paloaltonetworks:pan-os
Last Updated: Less than a minute ago
View Data
List Services
10 Item(s)
1 to 5 of 10
Page 1 of 2
Name Count
The Win32 process 'svchost.exe' is listening on this port 19,016
The Win32 process 'System' is listening on this port 6,176
The Win32 process 'lsass.exe' is listening on this port 2,483
A web server is running on this port. 1,511
The Win32 process 'spoolsv.exe' is listening on this port 1,330
Last Updated: Less than a minute ago
View Data
Firewall Status - Firewall Rule Enumeration
[Passed] Firewall Rule by Audit C...
[Manual] Firewall Rule by Audit C...
[Failed] Firewall Rule by Audit Ch...
Windows Firewall Disabled
Windows NETSH Firewall Rules
IPTables Firewall Rules
OS X Firewall Rules
Last Updated: 34 minutes ago
InfoSec Team - IP Discovery and Inventory
Total Disco... In DNS OS not Ide... Hosts w/ U... Scanned <... Exploitable... Exploitable...
All IPs 3,559 2,307 649 39% 13% 39% 2,416
Last Updated: 36 minutes ago



Firewalls Assessment Questions Directly Addressed

Questions in this section apply to: boundary firewalls, desktop computers, laptops, routers, servers, IaaS, PaaS, and SaaS. Regarding this Key Component area, the following Assessment questions can be directly addressed.

A4.1. Do you have firewalls at the boundaries between your organisation's internal networks, laptops, desktops, servers, and the internet?

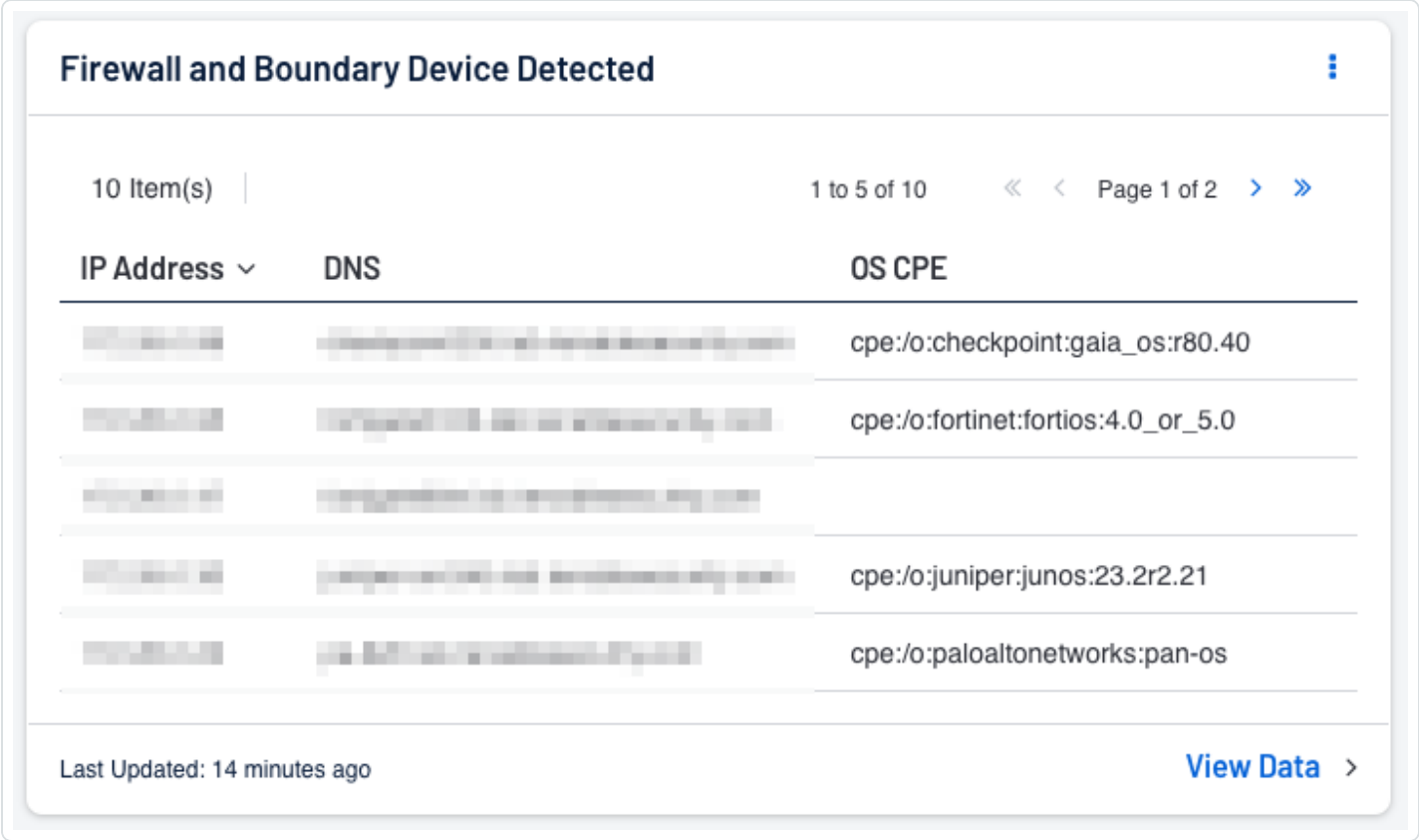
A4.1.1 Do you have software firewalls enabled on all of your computers, laptops and servers?

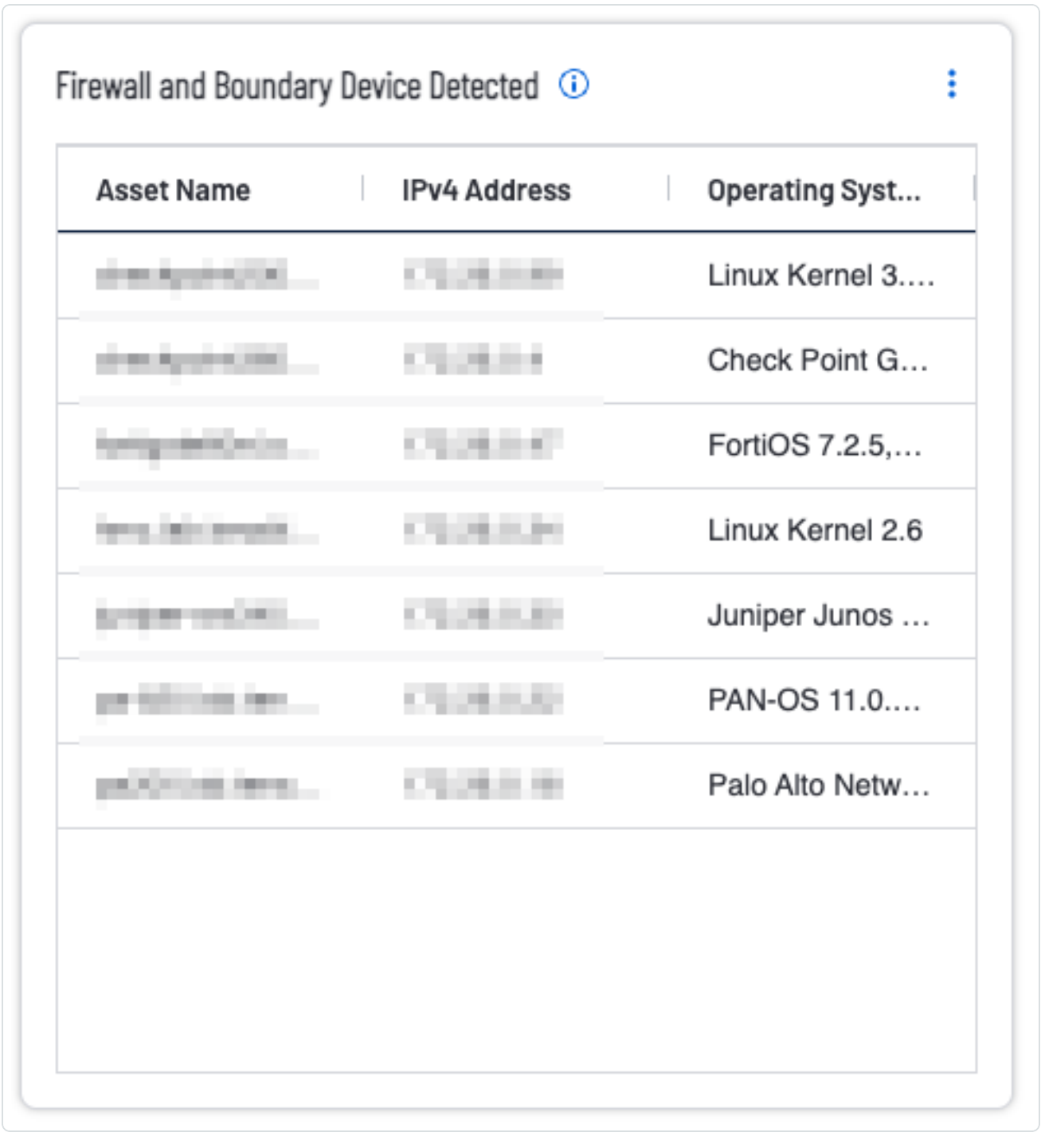
A4.1.2 If you answered no to question A4.1.1, is this because software firewalls are not installed by default as part of the operating system you are using? Please list the operating systems.

How Tenable can help: Can be accomplished by conducting discovery and assessment scans. Tenable recommends performing discovery scans to get an accurate picture of the assets on your network, and assessment scans to understand the vulnerabilities on your assets. The requirement

includes mobile devices and the cloud infrastructure, as well as any other devices in scope. Reference the Getting Started and Scope of Assessment (Asset Identification) section of this document to identify assets.

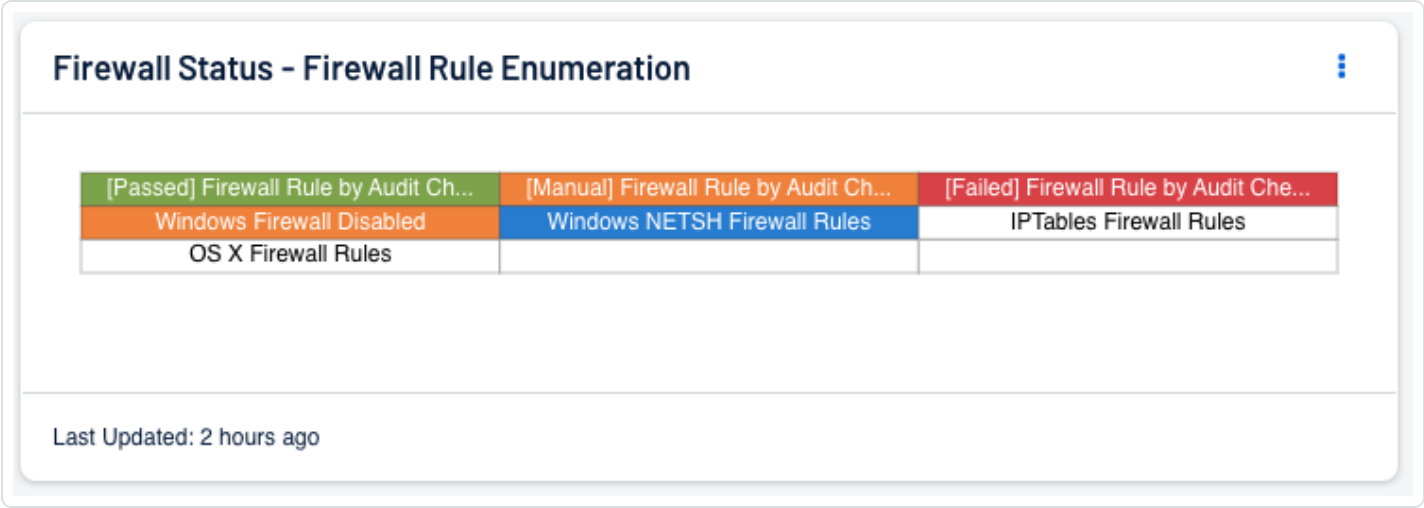
The Firewall and Boundary Device component for Tenable SC and widget for Tenable Vulnerability Management assists organisations with the rapid identification of firewall and boundary devices that have been identified in the environment. Displayed is the IP Address, DNS and OS CPE identifier for the device.





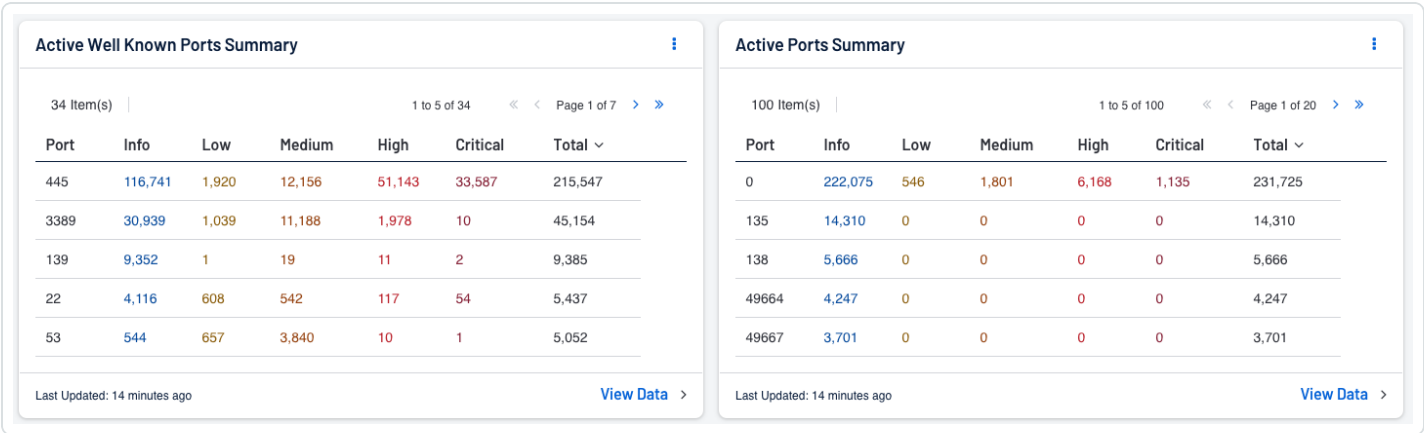
The Firewall Status - Firewall Rule Enumeration component addresses the identification of firewall software running or disabled on Windows devices, Firewall rules on macOS devices, and compliance issues. Scanning firewalls and reviewing the compliance findings can address the following items:

A4.6. Have you reviewed your firewall rules in the last 12 months? Please describe your review process.



A4.5. Do you have a process to manage your firewall?

How Tenable can help: Can be accomplished with scanning for open ports. The Active Well Known Ports Summary component display the currently active well known ports (7, 20, 21, 22, 23, 25, 53, 67, 68, 69, 80, 88, 110, 111, 123, 137, 139, 143, 161, 194, 389, 443, 445, 464, 514, 547, 596, 636, 873, 1720, 2049, 3306, 3389, 5060, 5061, 5900, 8000, 8080, 8443) along with the count of those active ports, and the Active Ports Summary component display all identified active ports.

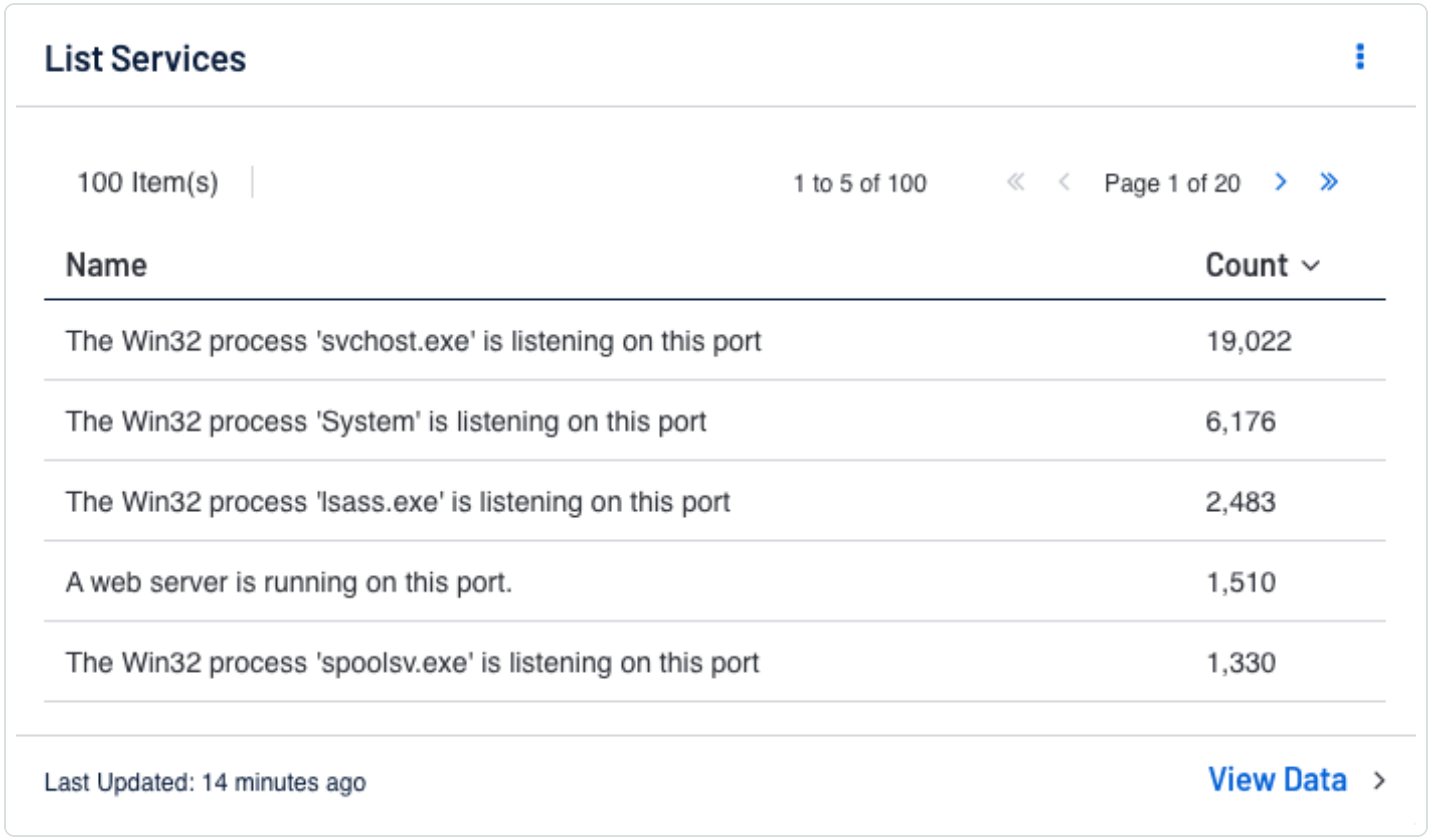


A5.4. Do you run or host external services that provide access to data (that shouldn't be made public) to users across the internet?

How Tenable can help: Can be accomplished with scanning for running services. The List Services component lists all services that have been identified in the environment, and displays them using the List Services Tool. As all devices may be in scope, all scanned devices are included in the

display. Tenable Vulnerability Management and Tenable Security Center include plugins that detect running services and process information. The information from these plugins can display unregistered software that may be running on the system that is not shown in the registry. The plugins below provide visibility into services that may appear only in running processes rather than in installed software packages. The plugins below provide this valuable information.

- 58452 - Microsoft Windows Startup Software Enumeration
- 70329 - Microsoft Windows Process Information
- 70330 - Microsoft Windows Process Unique Process Name
- 70331 - Microsoft Windows Process Module Information
- 70767 - Reputation of Windows Executables: Known Process(es)
- 70768 - Reputation of Windows Executables: Unknown Process(es)
- 70943 - Reputation of Windows Executables: Never seen process(es)
- 110483 - Unix/Linux Running Processes Information



More information can be found in the Cyber Exposure Study for Establishing a Software Inventory under Detecting Running Services.

A4.2. When you first receive an internet router or hardware firewall device, it may have had a default password on it. Have you changed all the default passwords on your boundary firewall devices?

A4.3. A. B. C. D. E. How is your firewall password configured?

Please select the option being used:

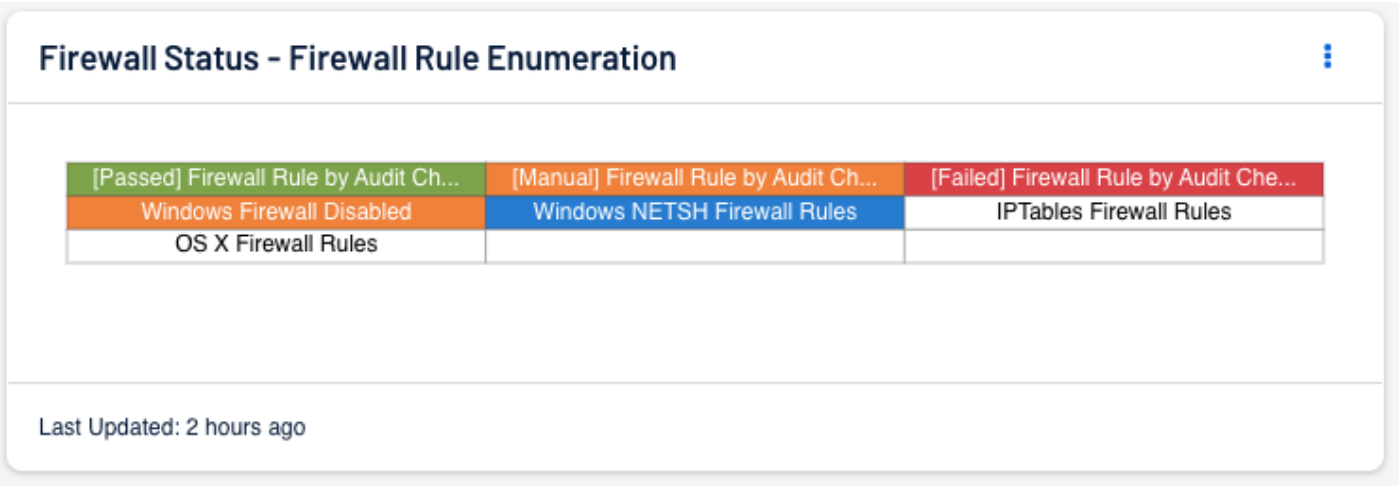
- *Multi-factor authentication, with a minimum password length 8 characters and no maximum length*
- *Automatic blocking of common passwords, with a minimum password length 8 characters and no maximum length*
- *A password minimum length of 12 characters and no maximum length*
- *Passwordless system is being used as an alternative to user name and password, please describe*
- *None of the above, please describe*

A4.7. Is your firewall configured to allow unauthenticated inbound connections?

A4.9. Are your boundary firewalls configured to allow access to their configuration settings over the internet?

A4.11. If you answered yes in question A4.9, is the access to your firewall settings protected by either multi-factor authentication or by only allowing trusted IP addresses combined with managed authentication to access the settings?

How Tenable can help: Can be accomplished with compliance scanning. The Firewall Rule Enumeration component uses plugin 56310 (Firewall Rule Enumeration) and audit checks to report on the status of software-based firewall rules. Compliance results; such as default passwords, MFA, and more are displayed on the Firewall Status - Firewall Rule Enumeration component within the appropriate Pass/Manual/Failed category.



See Also

- About Cyber Essentials
- Getting Started with the Scope of Assessment
- Key Component 1: Firewalls and Internet Gateways
- Key Component 2: Secure Configuration
- Key Component 3: Access Control
- Key Component 4: Malware Protection
- Key Component 5: Patch Management
- References

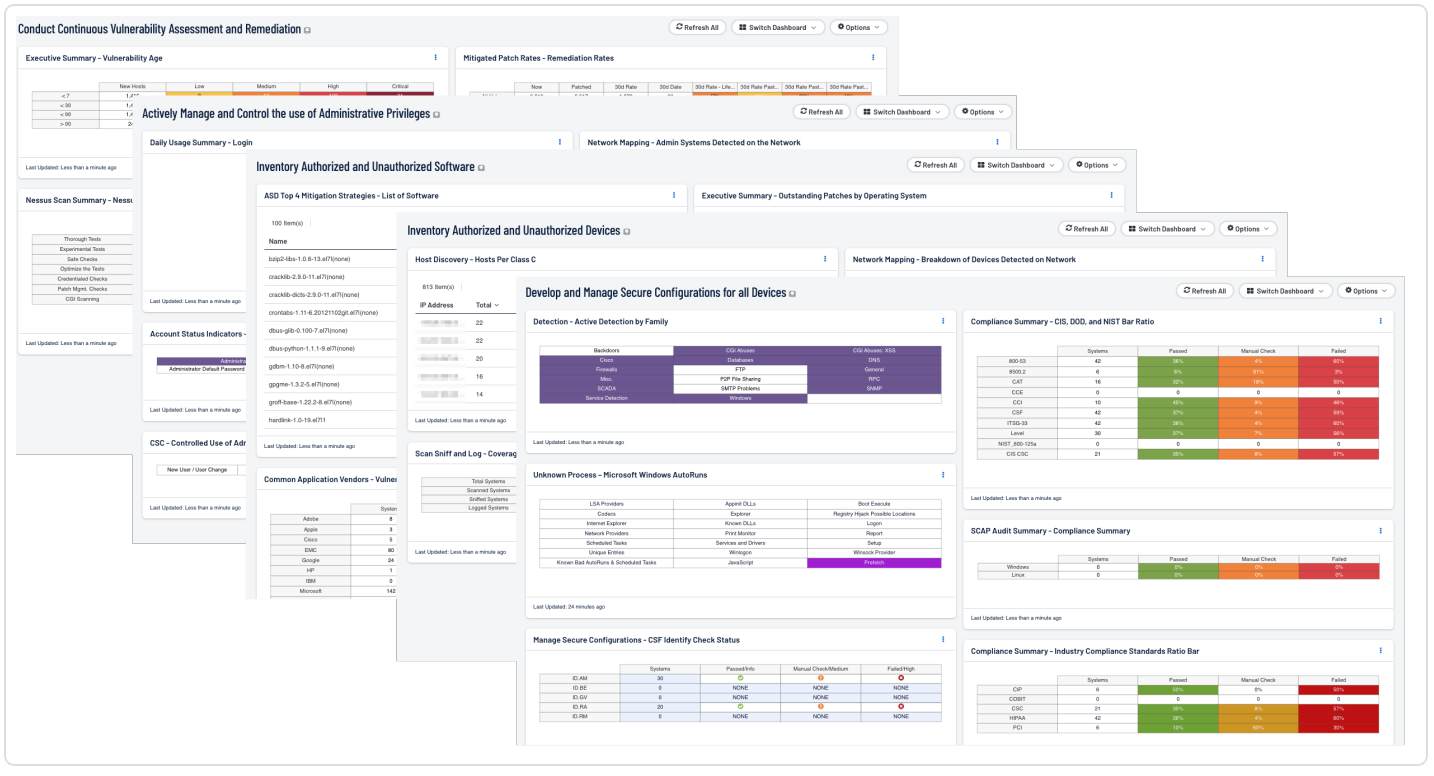
Key Component 2: Secure Configuration

Secure Configuration (also called security hygiene) is ensuring that devices and software are configured in the most secure way possible to reduce vulnerabilities and exposure to cyber threats. Unused software or services can introduce exploitable vulnerabilities. Default accounts and passwords are widely known and easy to exploit. The focus of this section applies to: servers, desktop computers, laptops, tablets, thin clients, mobile phones, IaaS, PaaS and SaaS.

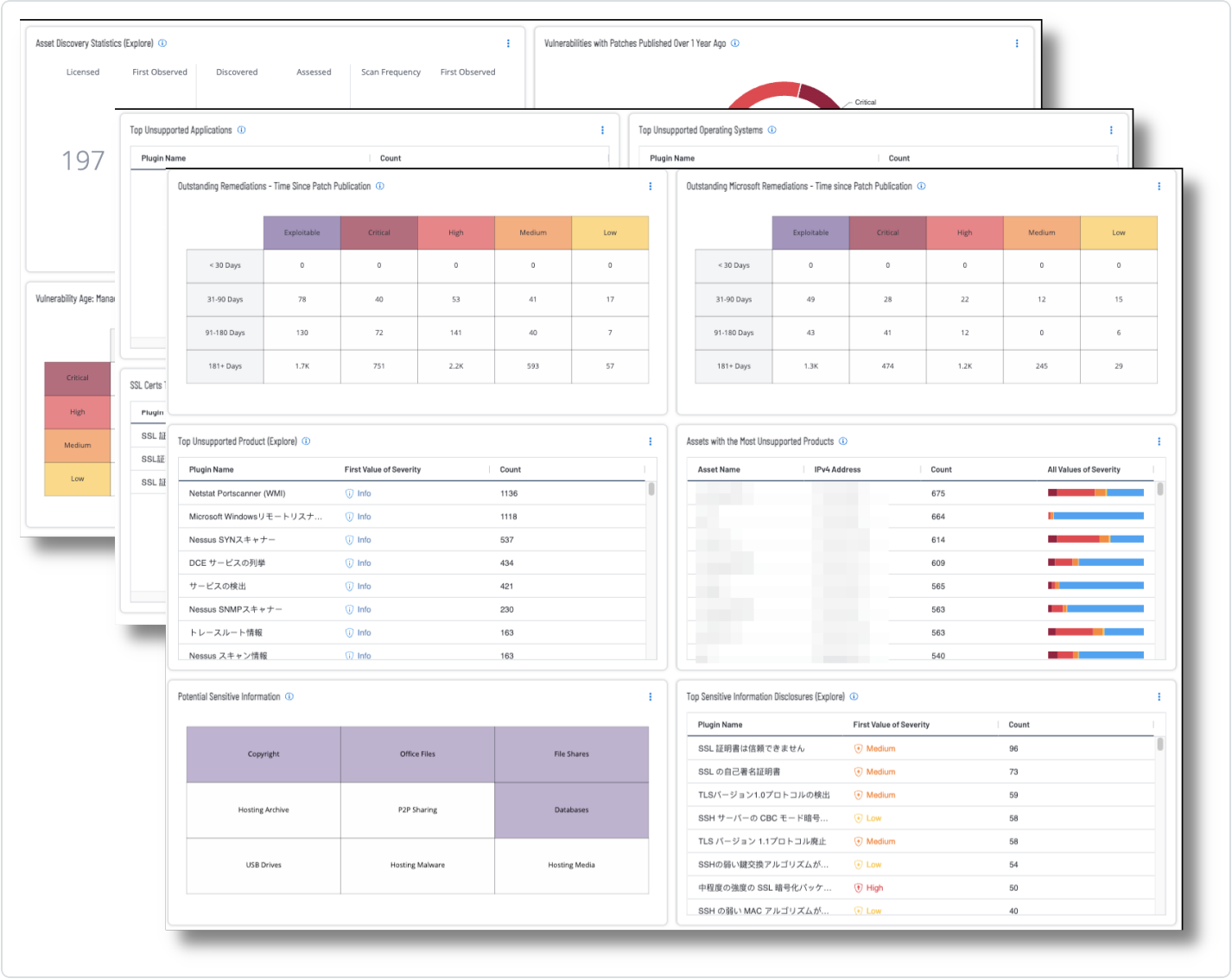
A secure configuration is your first line of defense. Default configurations and installations are not always secure. As previously stated, pre-set and widely known passwords are major weak points. Access Control will be covered in the next section. However default accounts and pre-installed software that are not needed, or no longer required may allow attackers to gain unauthorised access to sensitive information. Secure configuration begins with the identification and removal/disabling of unnecessary accounts, applications, and services, organisations can minimise vulnerabilities.

How Tenable can help: Tenable brought together a group of dashboards described in the “Tenable Solutions for the Cyber Hygiene Campaign” technical paper. These dashboards relate to the five actions identified by the Cyber Hygiene Campaign along with helping an organisation fulfil basic security needs such as monitoring.

For Tenable Security Center those dashboards are the **Cyber Hygiene** Dashboards.



For Tenable Vulnerability Management that dashboard is the Fundamental Cyber Hygiene Report Card.



The key areas of focus of these Cyber Hygiene dashboards related to the Cyber Essentials is:

Inventory Authorised and Unauthorised Devices: This collection of components provides information to analysts and auditors about systems discovered on the network and device inventory.

Inventory Authorised and Unauthorised Software: This dashboard and its components provide information to analysts about software that is discovered on the network.

Develop and Manage Secure Configurations for all Devices: Tenable has the ability to audit system configurations according to the standards. The components in this dashboard use forensic

plugins, detections, and compliance checks to provide information about how systems are configured.

Conduct Continuous Vulnerability Assessment and Remediation: Tenable has the ability to monitor for vulnerabilities using active, passive, and event-based detection.

Actively Manage and Control the Use of Administrative Privileges: A common problem found in networks is that too many accounts with administrative privileges exist. Organisations should make an effort to use dual accounts when administrative rights are to be used. This dashboard provides information about which users have administrative control and how this control is used.

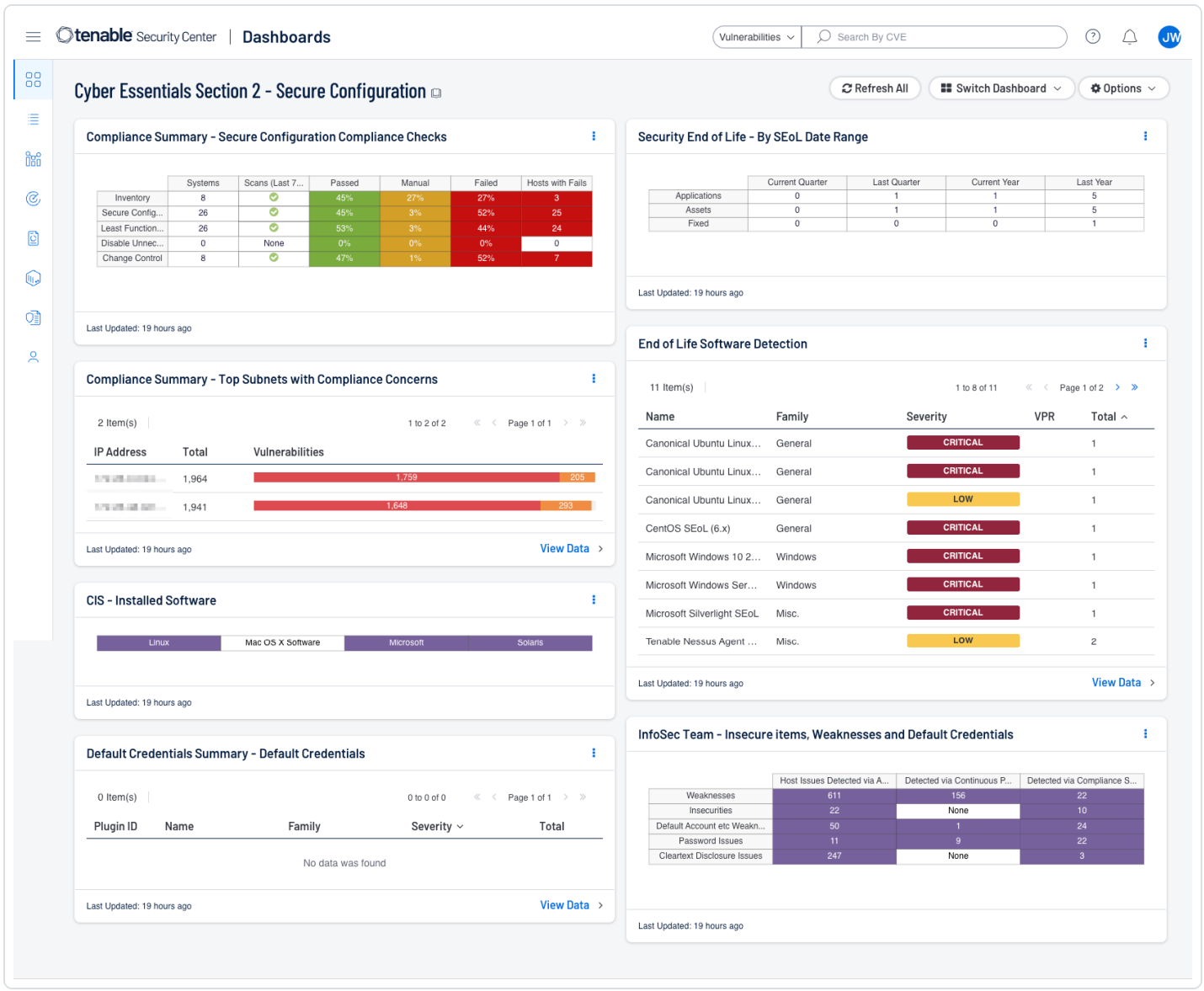
More information can be located within the Cyber Exposure Study NIS 2 Directive, Security Hygiene section.

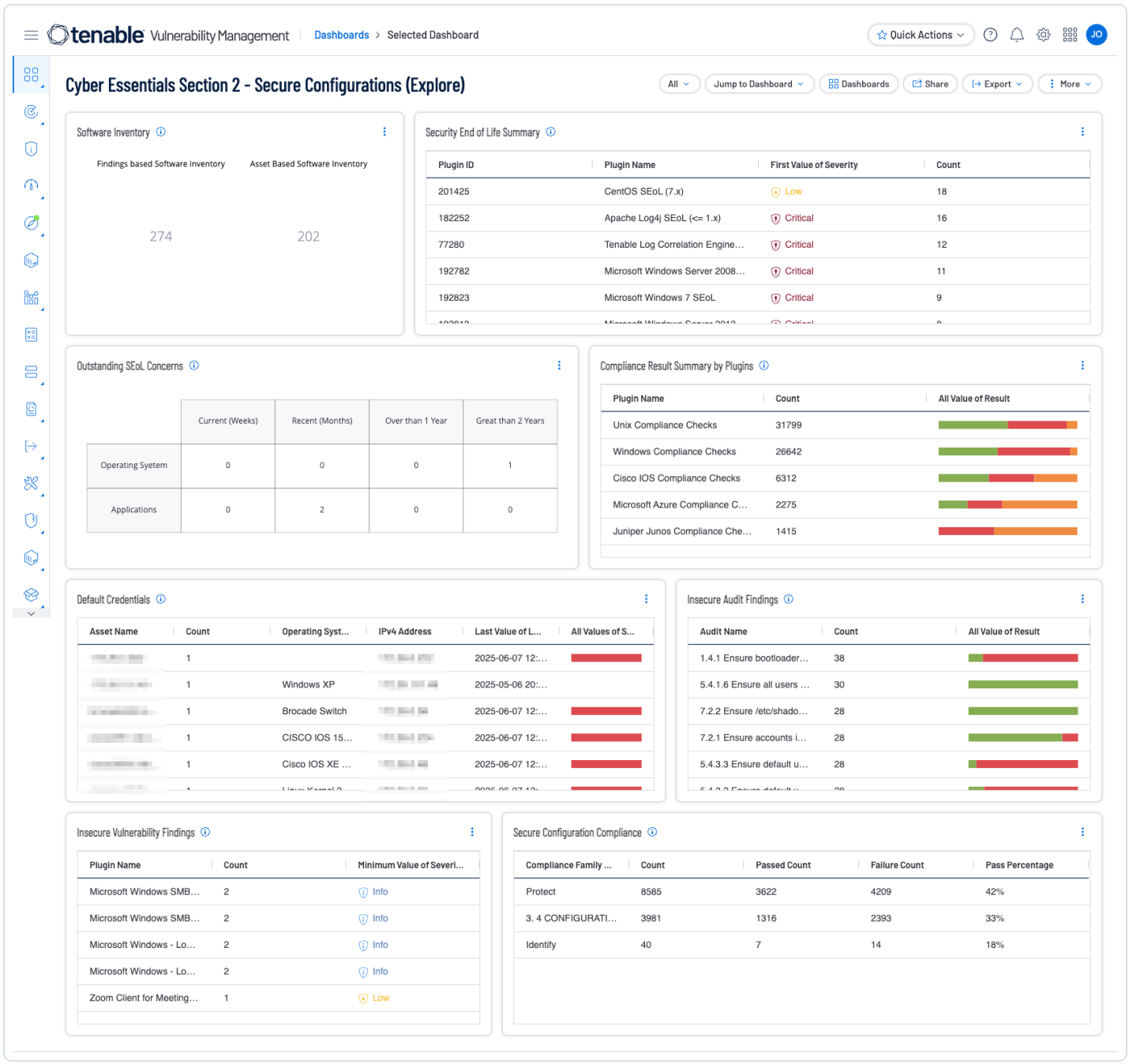
Tenable has provided a Cyber Essentials Dashboard and Report for Tenable Security Center and Tenable Vulnerability Management for this Key Component. Those dashboards and reports can be found here by using the term “Cyber Essentials” as a search query:

Security Center Dashboards and Reports

Vulnerability Management Dashboards and Reports

Shown below are screenshots of this section's dashboards for Security Center and Vulnerability Management.


tenable Security Center | Dashboards
Vulnerabilities
Search By CVE
JW
Cyber Essentials Section 2 - Secure Configuration
Refresh All
Switch Dashboard
Options
Compliance Summary - Secure Configuration Compliance Checks
Systems
Scans (Last 7...
Passed
Manual
Failed
Hosts with Fails
Inventory 8 45% 27% 27% 3
Secure Config... 26 45% 3% 52% 25
Least Function... 26 53% 3% 44% 24
Disable Unnec... 0 None 0% 0% 0% 0
Change Control 8 47% 1% 52% 7
Last Updated: 19 hours ago
Compliance Summary - Top Subnets with Compliance Concerns
2 Item(s)
1 to 2 of 2
Page 1 of 1
IP Address
Total
Vulnerabilities
1,964
1,759
205
1,941
1,648
293
Last Updated: 19 hours ago
View Data
CIS - Installed Software
Linux
Mac OS X Software
Microsoft
Solaris
Last Updated: 19 hours ago
Default Credentials Summary - Default Credentials
0 Item(s)
0 to 0 of 0
Page 1 of 1
Plugin ID
Name
Family
Severity
Total
No data was found
Last Updated: 19 hours ago
View Data
Security End of Life - By SEoL Date Range
Current Quarter
Last Quarter
Current Year
Last Year
Applications 0 1 1 5
Assets 0 1 1 5
Fixed 0 0 0 1
Last Updated: 19 hours ago
End of Life Software Detection
11 Item(s)
1 to 8 of 11
Page 1 of 2
Name
Family
Severity
VPR
Total
Canonical Ubuntu Linux... General CRITICAL 1
Canonical Ubuntu Linux... General CRITICAL 1
Canonical Ubuntu Linux... General LOW 1
CentOS SEoL (6.x) General CRITICAL 1
Microsoft Windows 10 2... Windows CRITICAL 1
Microsoft Windows Ser... Windows CRITICAL 1
Microsoft Silverlight SEoL Misc. CRITICAL 1
Tenable Nessus Agent ... Misc. LOW 2
Last Updated: 19 hours ago
View Data
InfoSec Team - Insecure items, Weaknesses and Default Credentials
Host Issues Detected via A...
Detected via Continuous P...
Detected via Compliance S...
Weaknesses 611 156 22
Insecurities 22 None 10
Default Account etc Weakn... 50 1 24
Password Issues 11 9 22
Cleartext Disclosure Issues 247 None 3
Last Updated: 19 hours ago



Secure Configuration Assessment Questions Directly Addressed

Software

A6.1. Are all operating systems on your devices supported by a vendor that produces regular security updates and vulnerability fixes?

A6.2. Is all the software on your devices supported by a supplier that produces regular vulnerability fixes for any security problems?

Removing and/or disabling unused software and services reduces the attack surface, limits vulnerabilities by preventing exploitation. Additionally, fewer applications simplifies maintenance and configuration/patch management and improves performance. Questions in this section apply to: servers, desktop computers, laptops, tablets, mobile phones, thin clients, IaaS, PaaS, and SaaS. Regarding this Key Component area, the following Assessment questions can be directly addressed.

A5.1. Have you removed or disabled software and services that you do not use on your laptops, desktop computers, thin clients, servers, tablets, mobile phones and cloud services?

How Tenable can help: Detailed information related to managing a software inventory, detecting services, application server hardening, and unsupported software is available for review in the Software Inventory section of the cyber exposure study Application Software Hardening.

Necessary User Accounts and Default Passwords

Operating Systems and applications are often distributed with service and default accounts that are either not password-protected or have a default password that is well known. Questions in this section apply to: servers, desktop computers, laptops, tablets, mobile phones, thin clients, IaaS, PaaS, and SaaS. Regarding this Key Component area, the following Assessment questions can be directly addressed.

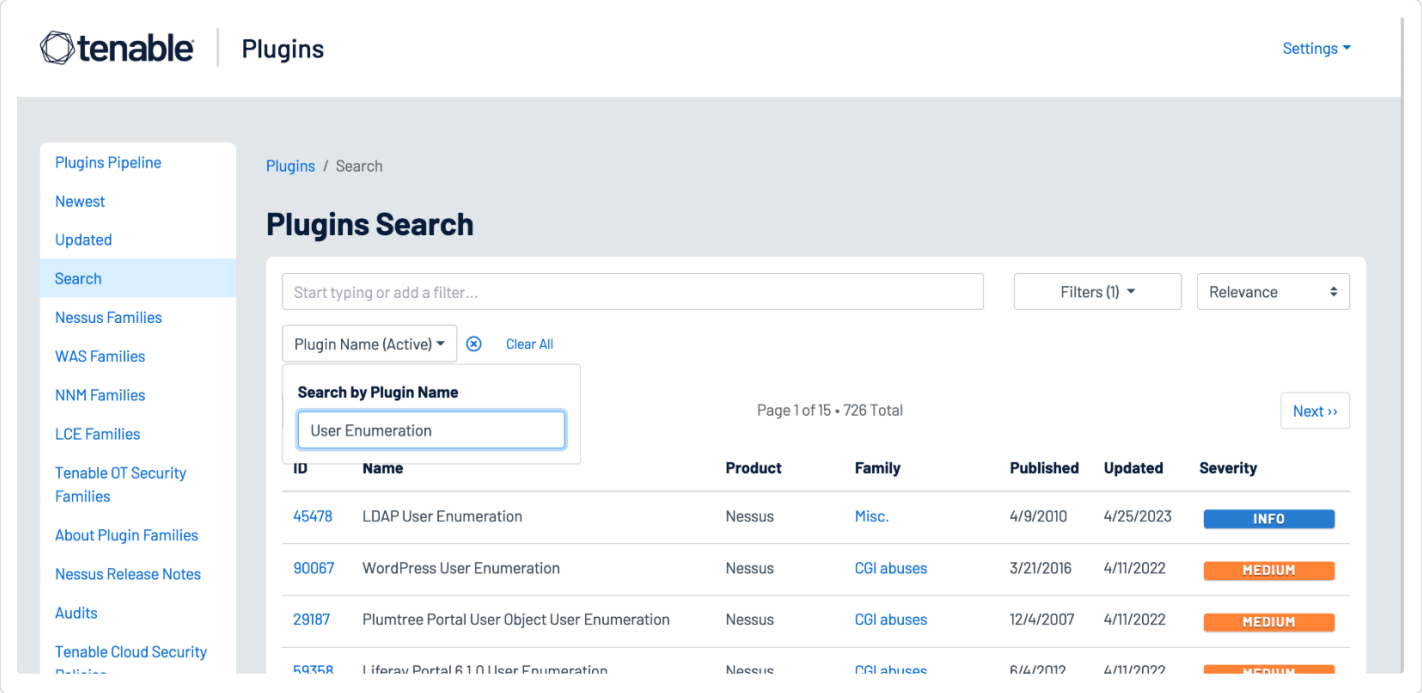
A5.2. Have you ensured that all your laptops, computers, servers, tablets, mobile devices and cloud services only contain necessary user accounts that are regularly used in the course of your business?

A5.3. Have you changed the default password for all user and administrator accounts on all your desktop computers, laptops, thin clients, servers, tablets and mobile phones that follow the Password-based authentication requirements of Cyber Essentials?

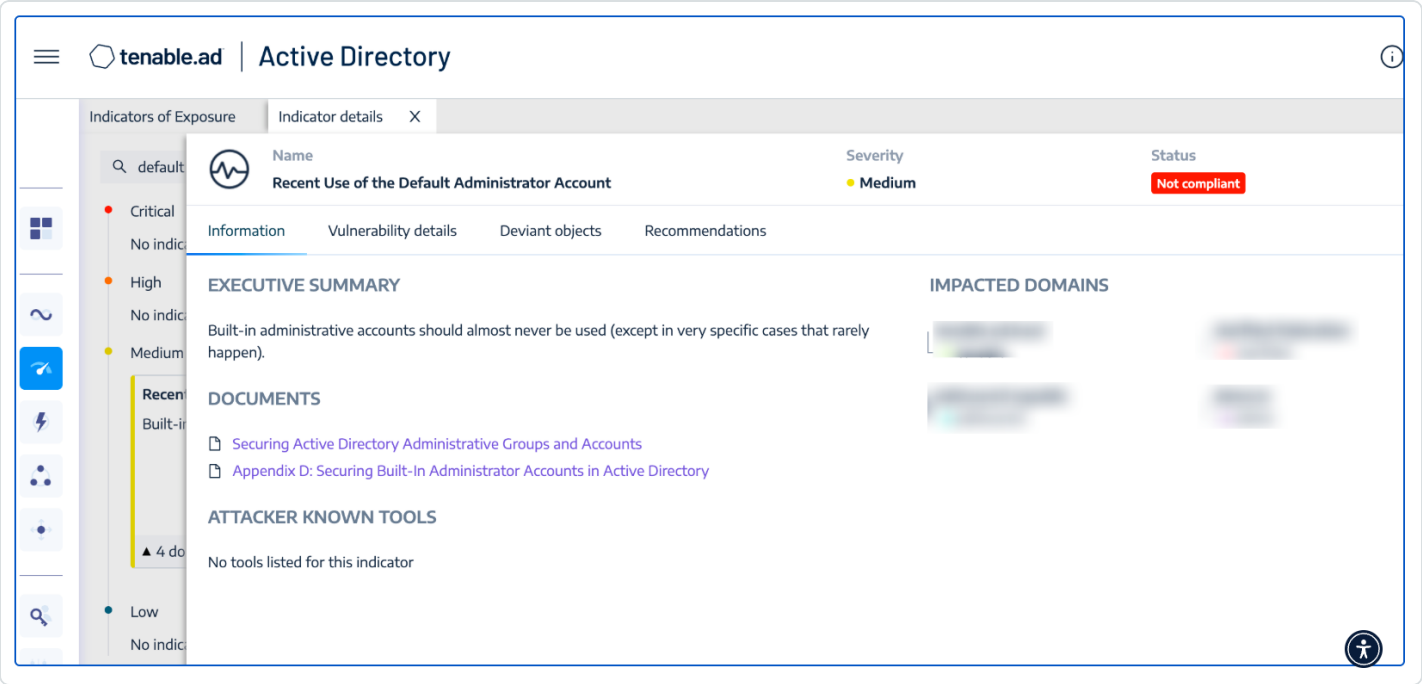
How Tenable can help: Tenable Nessus and Tenable Identity Exposure help identify these accounts, enabling organisations to review and disable any unnecessary accounts to reduce the attack surface. Organisations can leverage the following Nessus plugins to enumerate service and default accounts:

- Plugin Family: Default Unix Accounts – This plugin family contains over 170 Nessus plugins that check for the existence of default accounts/passwords on a number of devices. In addition, there are many plugins that check for simple passwords such as “0000”, “1234”, and more commonly identified password combinations for “root” or administrator accounts.

Several hundred plugins can be identified by searching for “Default Account” from the **Nessus Plugins Search** page using the Enable Default Logins filter. Nessus default account plugins are available for Databases, Web Servers, SCADA devices, Unix/Linux devices, Cisco devices and more. Many of the plugins are associated with the Default Unix Account Nessus family, however, many are in other families as well.



In addition, Tenable Identity Exposure provides the ability to determine if a default administrator account was recently used in the environment, as shown in the image below:



Compliance Scanning

Compliance and reporting are two concepts within business and regulatory frameworks. Compliance refers to the rules, regulations, standards, and laws set forth by external entities, such as government agencies, industry associations, or internal policies. Questions in this section apply to: servers, desktop computers, laptops, tablets, mobile phones, thin clients, IaaS, PaaS, and SaaS. Regarding this Key Component area, the following Assessment questions can be directly addressed.

A5.7. When not using multi-factor authentication, which option are you using to protect your external service from brute force attacks?

- A. Throttling the rate of attempts
- B. Locking accounts after 10 unsuccessful attempts
- C. None of the above, please describe

A5.8. Have you disabled any feature which allows automatic file execution of downloaded or imported files without user authorisation?

A5.9. When a device requires a user to be present, do you set a locking mechanism on your devices to access the software and services installed?

How Tenable can Help: Tenable solutions include reporting features that help organisations demonstrate compliance with a number of cybersecurity regulations. This can be valuable for NIS 2 compliance, as organisations are required to report incidents and maintain proper documentation. Risk management measures can be validated with compliance scanning, providing detailed reports on applications and assets within the organisation.

Tenable has introduced key features and content that give you visualisation of Compliance scan results through the built-in dashboards or custom dashboards using the newly added widgets. Performing a compliance audit scan is not the same as performing a vulnerability scan, although there can be some overlap. A compliance audit determines if a system is configured in accordance with an established policy. A vulnerability scan determines if the system is open to known vulnerabilities. Organisations can deploy and customise audit files to meet their local security policy. Once the audit file is customised, the file can be used with Tenable products to manage and automate the configuration compliance process. Detailed or summarised reports can also be generated in PDF format for the host audit findings. Dashboards and reports exist for a wide variety of existing compliance standards such as:

- GDPR
- HIPAA
- PCI-DSSv4.0
- ISO/IEC-27001
- NIST 800-53
- ITSG-33 (Canada)
- DISA STIG
- Center for Internet Security
- Tenable Best Practice Audits
- Vendor-Based Audits

Detailed information on all the available **Compliance** dashboards can be found online by referencing these locations for Tenable Security Center and Tenable Vulnerability Management. For each select the **Compliance and Configuration Assessment Category** to list the available content and references.

Tenable Vulnerability Management Dashboards

DASHBOARD SPOTLIGHT

Audit and Compliance Dashboards

Check out the recently released Host Audit Dashboards.

Search

Title

Dashboard Category

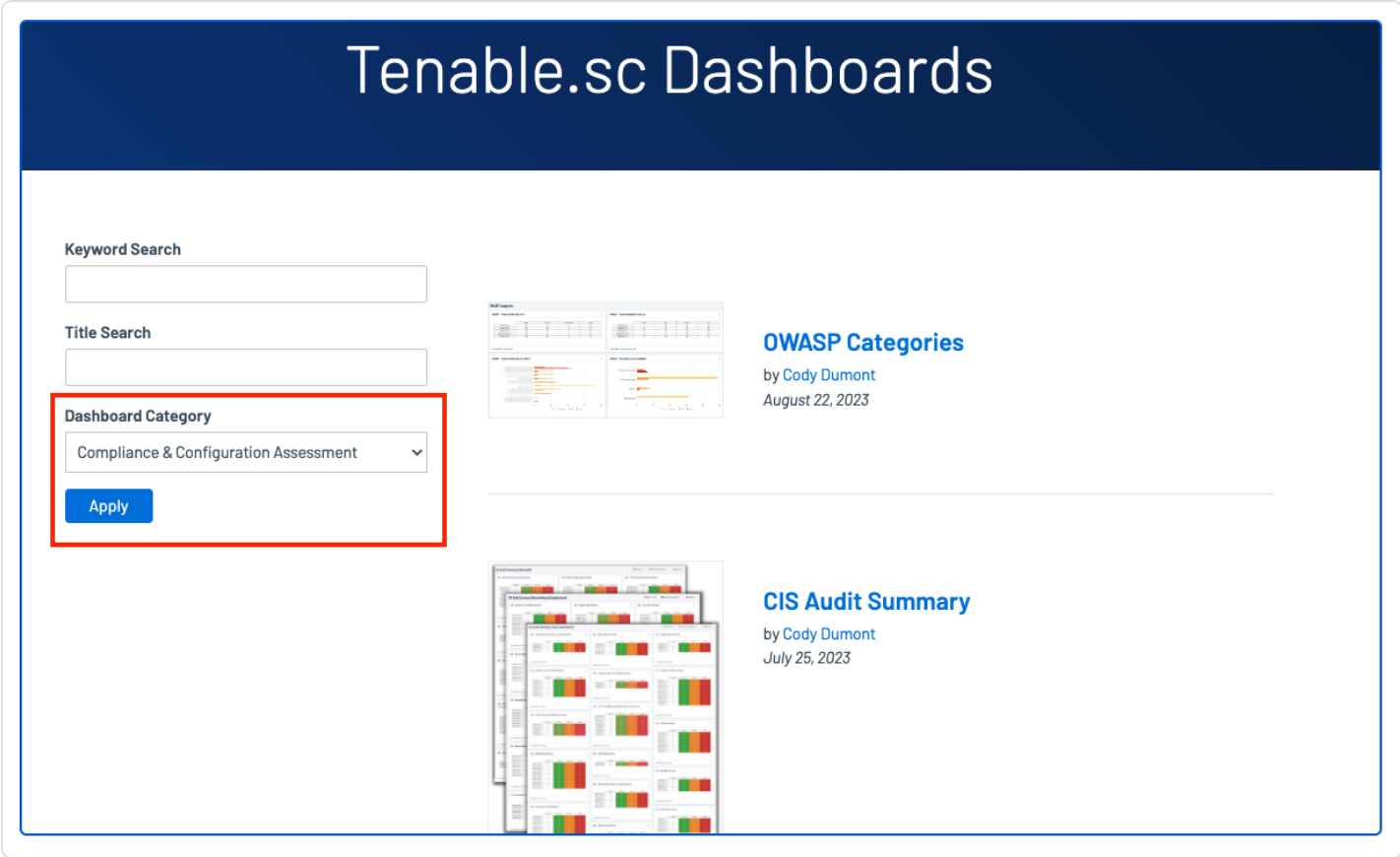
Compliance & Configuration Assessment

Apply

PCI-DSSv3.2.1 Audit Summary (Explore)

by Cesar Navas

April 23, 2024



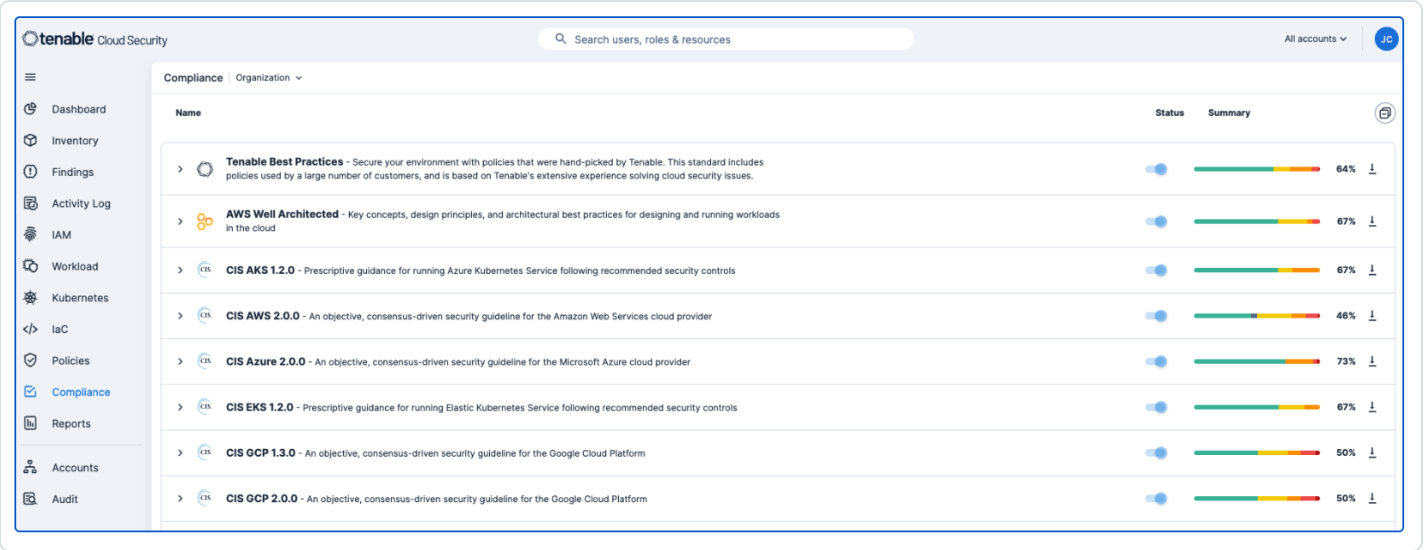
Additional details on Compliance scanning can be found within the [Host Audit Data Audit Overview Cyber Exposure Study located here].

Cloud services are an integral part of business operations, offering scalability, flexibility, and accessibility. Cloud environments store vast amounts of sensitive data, including personal information, financial records, intellectual property, and proprietary business data. Ensuring robust security measures protects this information from unauthorised access, breaches, or theft.

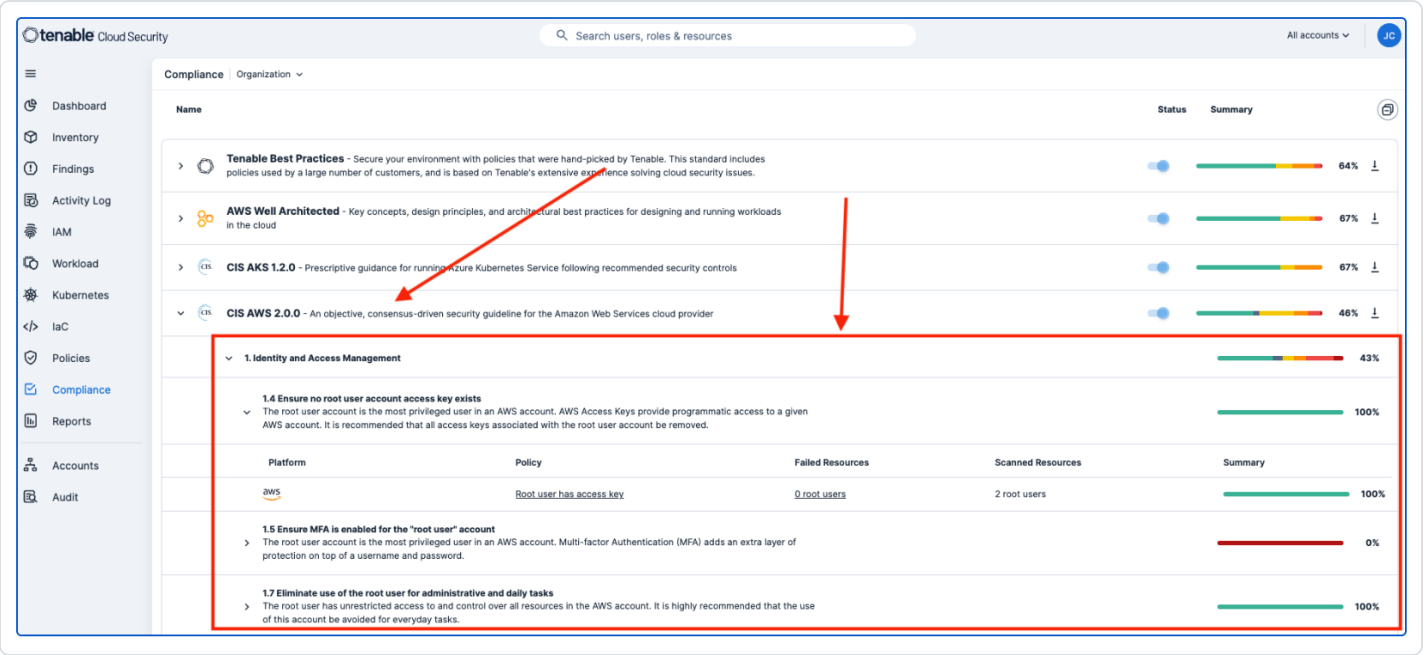
Protecting cloud environments is vital for protecting data, ensuring compliance with regulatory requirements, maintaining operational continuity, managing risks, and optimising business efficiency. Tenable Cloud Security provides out-of-the-box, continuously updated support for all major compliance frameworks, and best practices. Tenable Cloud Security provides the ability to create customised frameworks to meet the exact needs of your organisation. Using customised reports, communicate with stakeholders on internal compliance, external audit and daily security activities.

Compliance reporting is available by navigating to the **Compliance** tab. On the **Compliance** dashboard, analysts have the option to select the appropriate compliance benchmark from the list.

By default, this dashboard reports compliance details for all Benchmarks combined if no option is selected.



To view details, analysts can drill down into any of the findings. In this example, drilling down into the **CIS AWS 2.0.0** item provides details on the root account.



See Also

Key Component 3: Access Control

The focus of this key component is Access Control. The focus is on limiting access to data and services based on user roles, ensuring that individuals only have access which is required to perform job functions. This key component applies to all the following in scope devices: Boundary Firewalls, Desktop Computers, Laptops, Routers, Servers, Iaas, PaaS, and SaaS devices. Some items to focus on within this key component are:

- Administrative privileges are tightly controlled and monitored
- No shared accounts, every user must have their own unique account for auditing
- Access is granted on the principles of least privilege
    - Users should have the minimum level of privileges to carry out their duties
- Strong passwords must be enforced
- Stale accounts are removed
    - User accounts should be reviewed regularly
- Use multi-factor authentication (MFA)

Leveraging Tenable Security Center (formerly Tenable.sc), Tenable Vulnerability Management (formerly Tenable.io), and Tenable Identity Exposure (formerly Tenable.ad) solutions enables organizations to close attack paths, making the organization a more difficult target to attack. Tenable solutions provide organizations the data needed to identify and evaluate exposures in the environment. Tenable Identity Exposure is a fast, agent-less Active Directory security solution that helps organizations analyse their complex Active Directory environment, predict what matters most to reduce risk, and eliminate attack paths before they can be exploited.

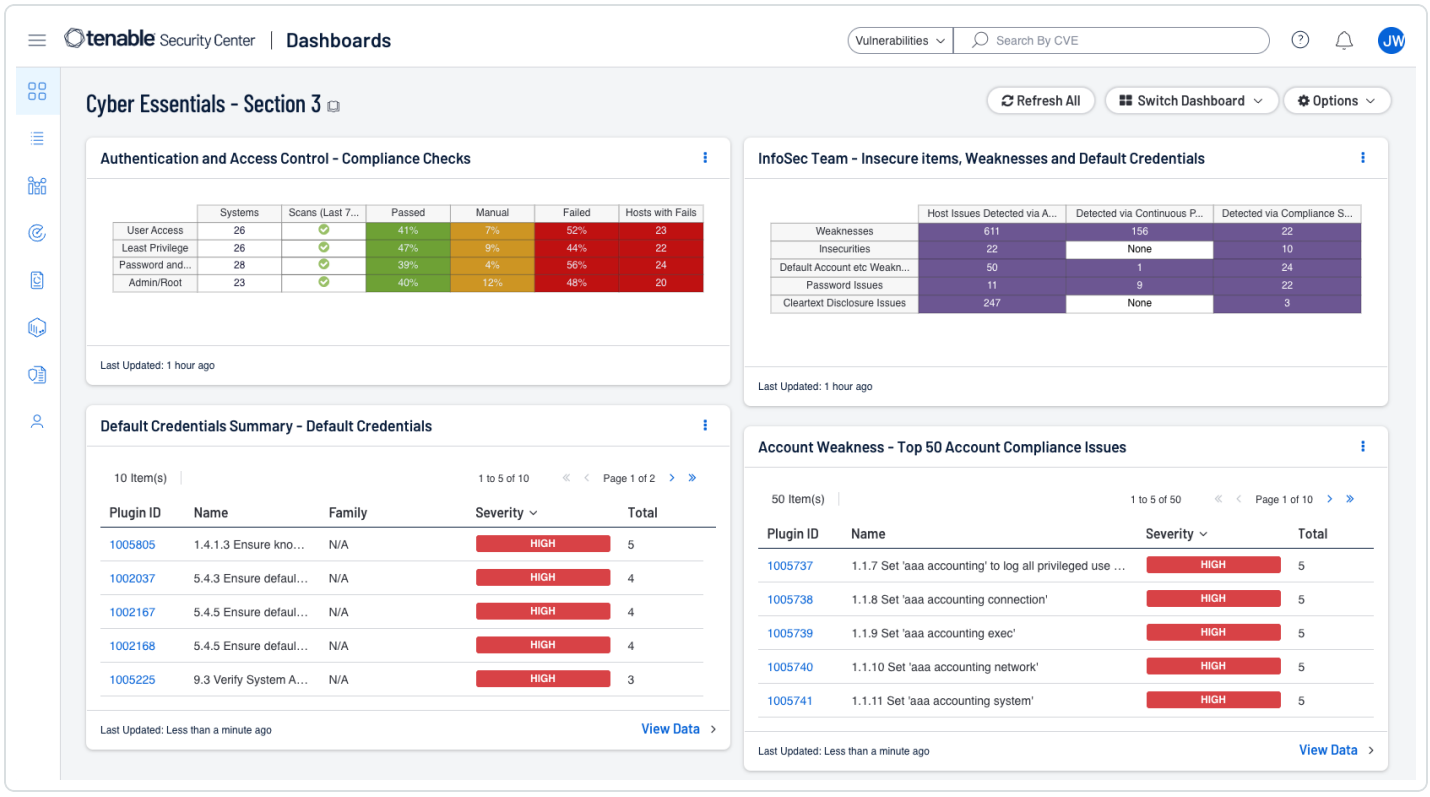
For more detailed information on Identity and Access Management, please reference the Tenable Cyber Exposure Study: Identity and Access Management.

Tenable has provided a Cyber Essentials Dashboard and Report for Tenable Security Center and Tenable Vulnerability Management for this Key Component. Those dashboards and reports can be found here by using the term “Cyber Essentials” as a search query:

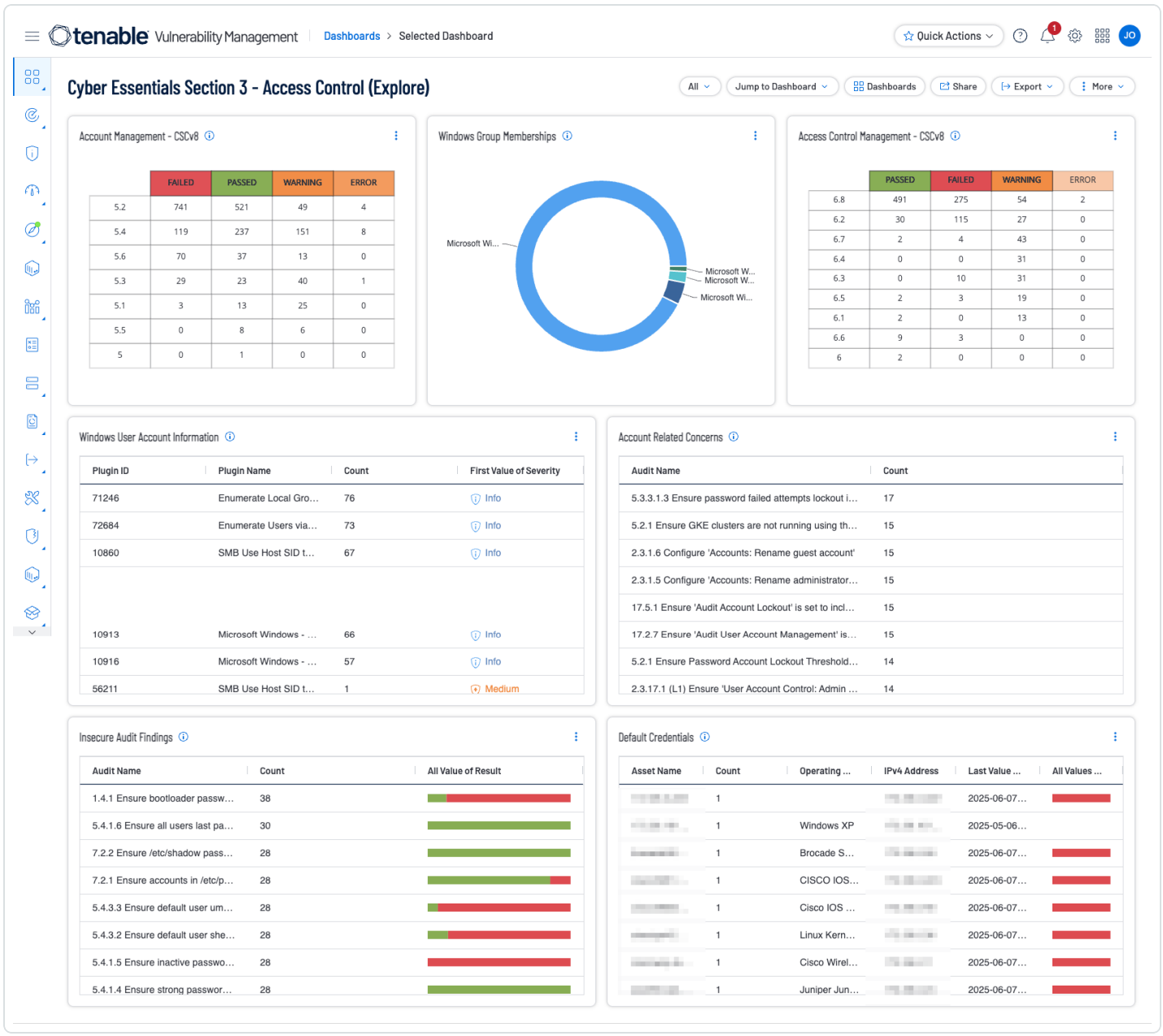
Security Center Dashboards and Reports

Vulnerability Management Dashboards and Reports

Shown below are screenshots of this section's dashboards for Security Center and Vulnerability Management.



The focus of the dashboards is around Access Control, and components and widgets support the goal of reducing an organisation's risk from the most common cyber threats. The Cyber Essentials focuses on preventing high impact attacks, such as phishing, malware infection, and unauthorised access. Strong access control can limit the number of accounts which attackers can compromise, ensuring that individuals only have access which is required to perform job functions. These dashboards assist with identification of default accounts, account weakness, and account related compliance and authentication concerns.

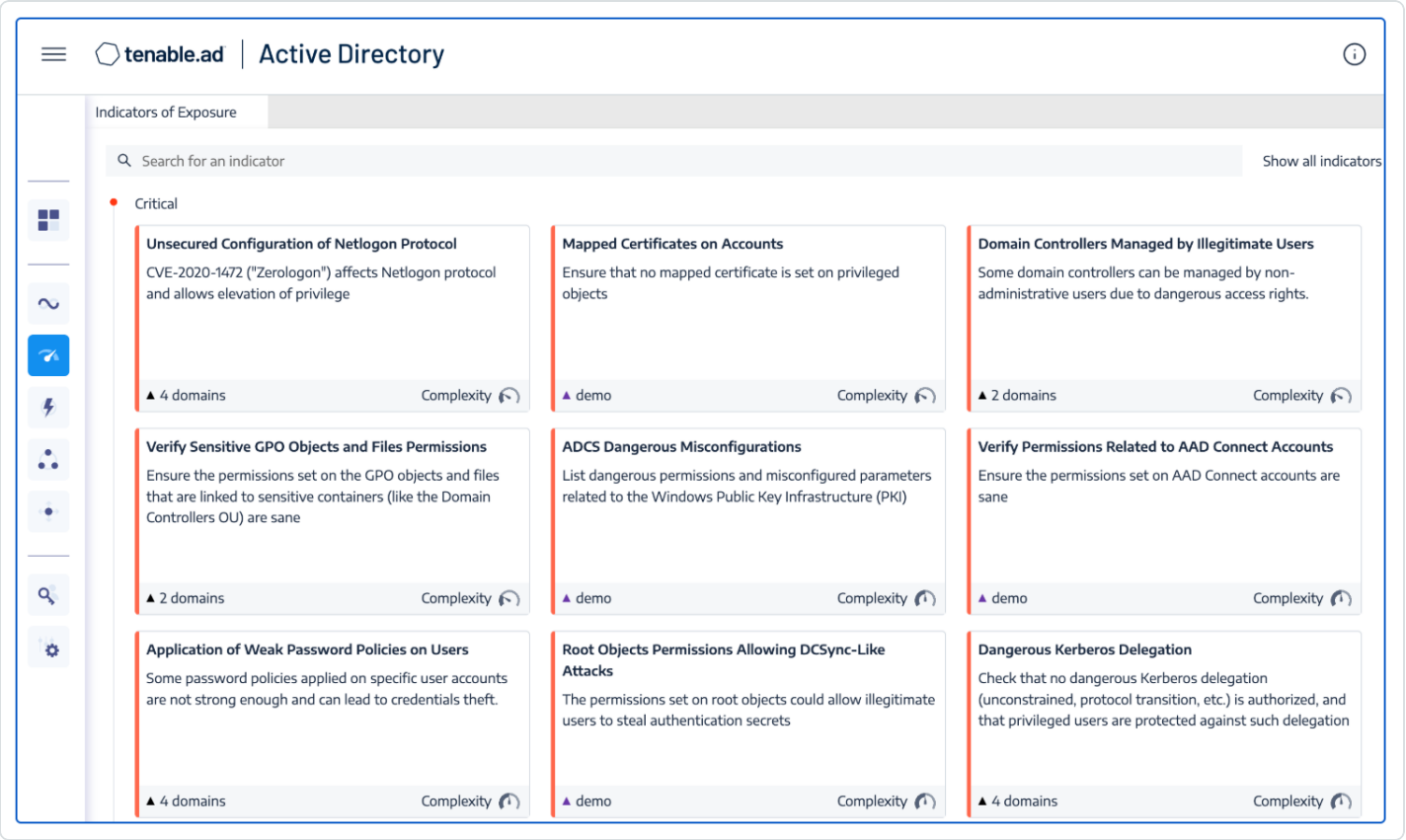


Tenable Identity Exposure

Tenable Identity Exposure provides information about an organization's Active Directory environment in an intuitive dashboard that monitors Active Directory in real-time, enabling organizations to identify at a glance the most critical vulnerabilities and recommended courses of remediation. Indicators of Exposure and Indicators of Attack discover underlying issues affecting the organization's Active Directory environment. Some of the Identity Management compliance requirements that Tenable solutions address include:

- Identify all accounts in the environment
- Ensure all active accounts are authorised
- Ensure all accounts are configured to use strong authentication controls
- Delete or disable dormant accounts
- Restrict privileged access to only authorised users
- Ensure group access is appropriately assigned
- Understand configuration exposures, such as dangerous permissions

Indicators of Exposure provides an overview of critical, high, medium, and low risk exposures identified across the organization's domains. From the landing page, security analysts can drill down for more details about which assets are exposed.



Secure Configuration Assessment Questions Directly Addressed

Questions in this section apply to: servers, desktop computers, laptops, tablets, thin clients,

mobile phones, IaaS, PaaS and SaaS. Within this section, information is provided which addresses the following questions.

A7.3. How do you ensure you have deleted, or disabled, any accounts for staff who are no longer with your organisation?

A7.8. Do you formally track which users have administrator accounts in your organisation?

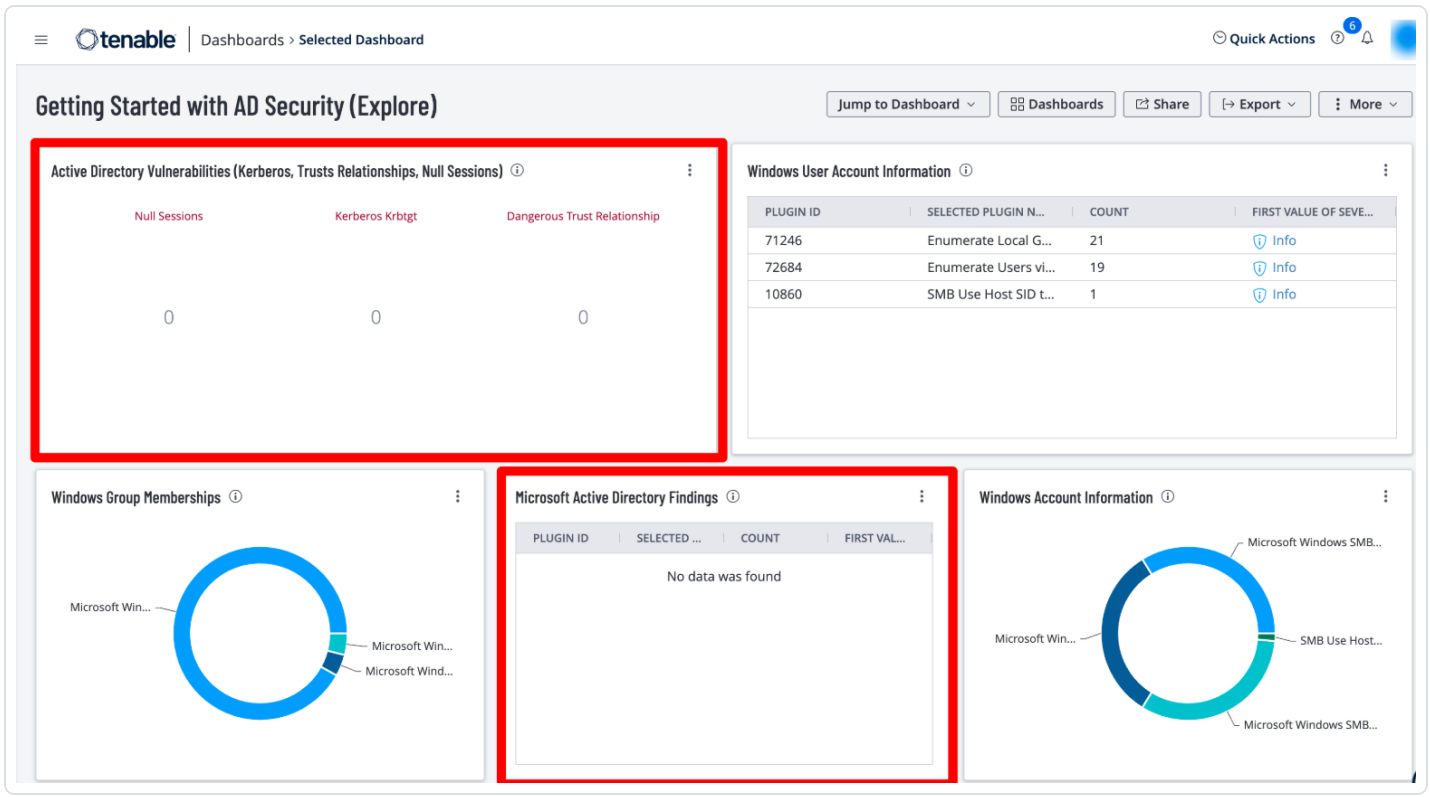
A7.9. Do you review who should have administrative access on a regular basis?

A7.11. Which technical controls are used to manage the quality of your passwords within your Organisation?

Role Based Access Control

Tenable Identity Exposure provides various methods to access the information collected through the Indicators of Exposure (IoE) and Indicators of Attack (IoA) panes. Tenable Vulnerability Management provides the ability to use the Explore Findings through the use of dashboards and reports.

The first step in taking control of the organization's Identity Management is to enumerate every user account in the environment and determine the level of access the account is granted. All user accounts must be uniquely identified and assigned to particular entities, such as users and applications.



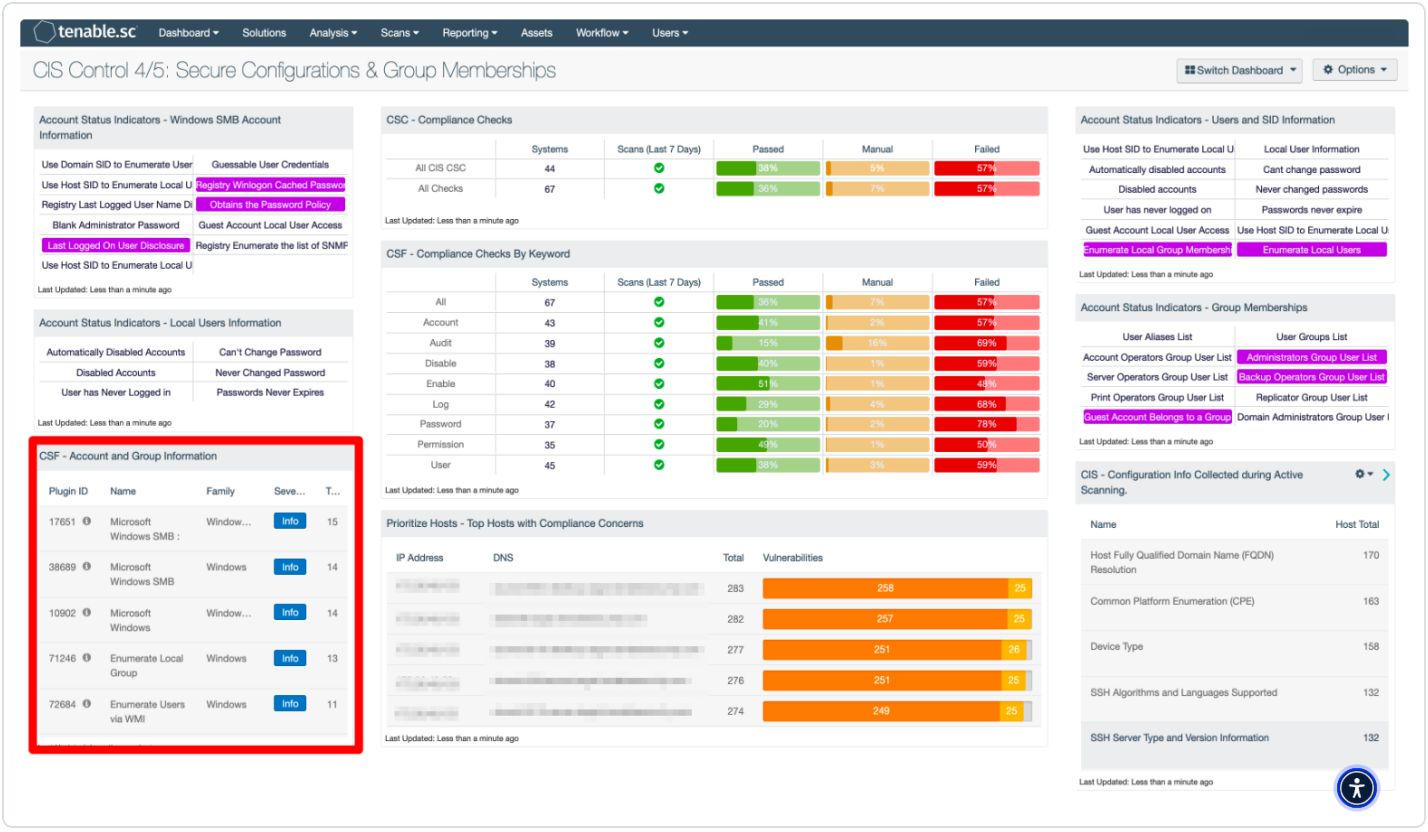
The Getting Started with AD Security dashboard in Tenable Vulnerability Management contains the following widgets to enumerate user accounts:

Windows User Account Information – This widget displays counts for user accounts and security identifiers (SID). Plugins report on potential user account vulnerabilities such as disabled accounts, accounts that have never logged in, accounts with passwords that have never changed, and more.

Windows Group Memberships – This widget displays information for Windows default groups such as administrators, server operators, account operators, backup operators, print operators, and replicator groups.

Windows Account Information – This widget displays counts related to Microsoft Windows SMB plugins that focus on user account information. Plugins focus on vulnerabilities such as SMB blank administrator passwords, SMB password policies, guest accounts, cached passwords, and more.

Organizations can use the **CSF - Account and Group Information** widget located in the **CIS Control 4/5: Secure Configurations & Group Memberships** dashboard in Tenable Security Center, which leverages plugins that enumerate Windows account information.

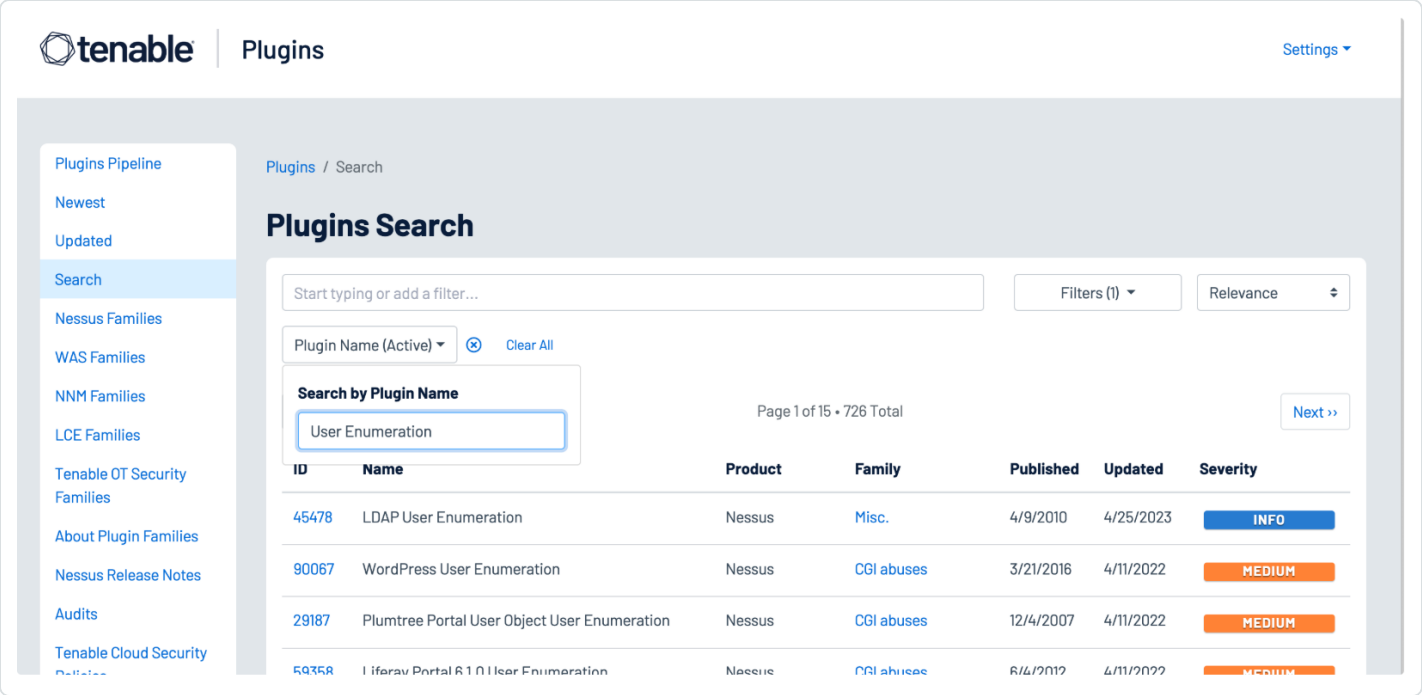


Users and Groups

While Active Directory is typically used by most organizations, there are many other accounts for non-Windows platforms that must be identified. Tenable Nessus contains a number of plugins and plugin families that help organizations enumerate users and groups on the network. The **Windows: User management** plugin family contains nearly 30 plugins that enumerate Microsoft Windows users and groups. Other useful Nessus plugins for user and group enumeration include:

- **10894 Microsoft Windows Users Group List** – This plugin uses the supplied credentials to retrieve the list of groups each user belongs to. Groups are stored for further checks.
- **126527 Microsoft Windows SAM user enumeration** – This plugin enumerates domain users on the remote Windows system using Security Account Manager.
- **95928 Linux User List Enumeration** – This plugin enumerates local users and groups on the remote host.
- **95929 macOS and Mac OS X User List Enumeration** – This plugin extracts the member lists of 'Admin' and 'Wheel' groups on the remote host.

A number of other Nessus plugins that contain the key words “User Enumeration” in a plugin name search using the Plugin Name filter identify WordPress, VMware, LDAP, and other software applications that maintain user accounts, as shown in the following image:



Active Directory accounts can be configured to escape global password renewal policies. Accounts set up in this manner can be used indefinitely without ever changing their password. Tenable recommends reviewing user and administrator accounts to ensure they are not configured to have this attribute.

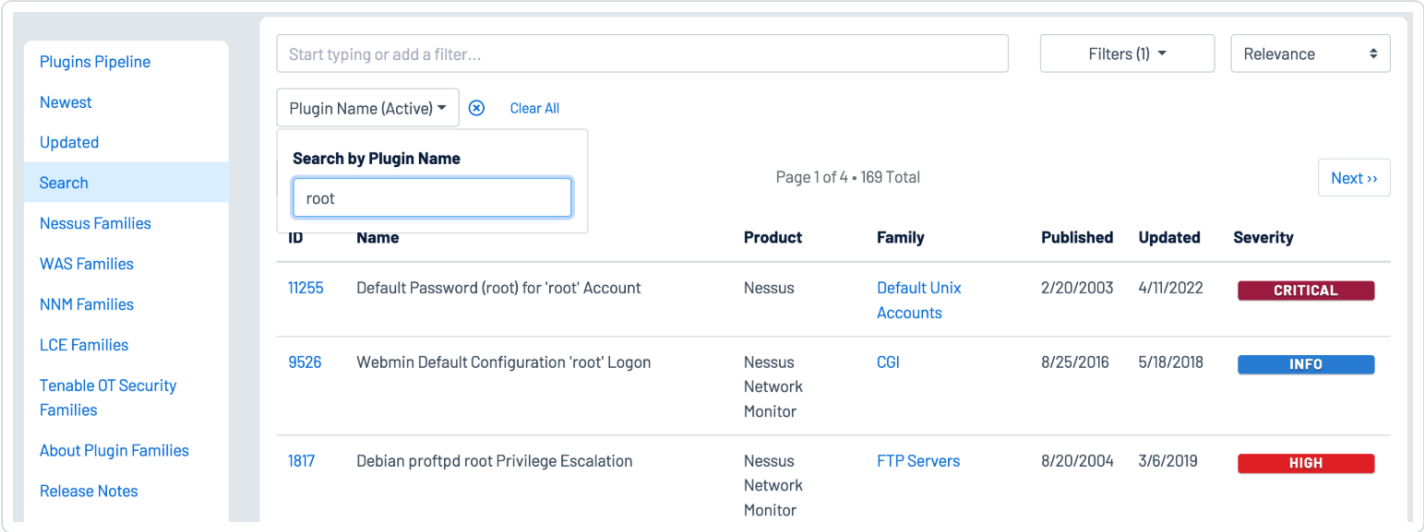
The following Indicators of Exposure (IoE) in Tenable Identity Exposure can be used to identify issues with user accounts in an organization’s Active Directory environment:

- Accounts with Never Expiring Passwords
- Application of Weak Password Policies on Users
- Dangerous Kerberos Delegation
- Account that Might Have an Empty Password
- AdminCount Attribute Set on Standard Users
- User Account Using Old Password
- Kerberos Configuration on User Account

Privileged Accounts

Most compliance standards and frameworks require privileged users to have a non-privileged account for standard user activities, such as web browsing or reading emails. Tenable Nessus and Tenable Identity Exposure provide the tools to identify settings for root and admin accounts.

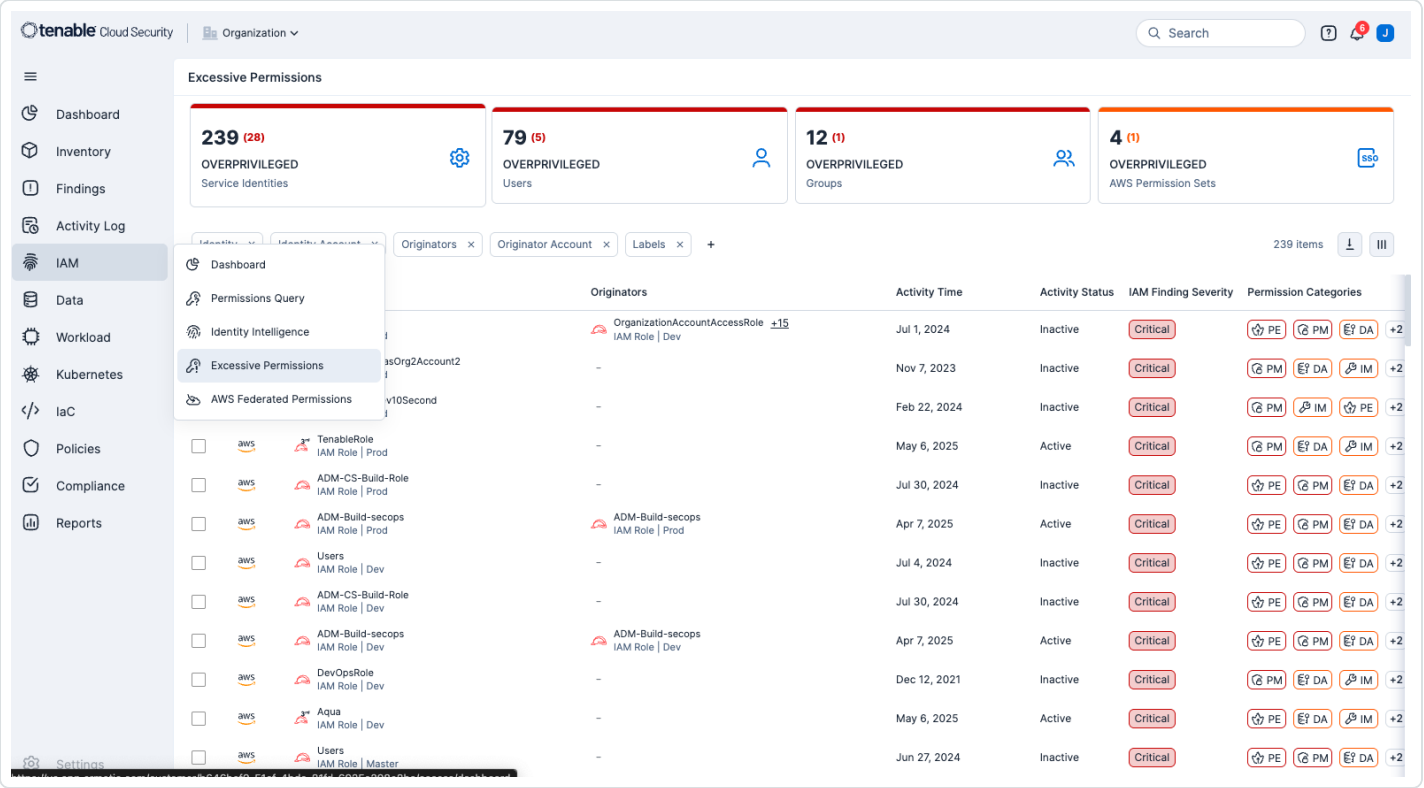
Using the Plugin Name filter on the Plugins Search page enables analysts to search for plugins with terms that identify privileged accounts such as “root,” “admin,” or “privileged,” as shown below:



The following Indicators of Exposure (IoE) in Tenable Identity Exposure can be used to identify Active Directory settings for privileged accounts:

- Mapped Certificates on Accounts
- Ensure SDProp Consistency
- Native Administrative Group Members
- Privileged Accounts Running Kerberos Services
- Potential Clear-Text Password
- Protected Users Group not Used
- Logon Restrictions for Privileged Users
- Local Administrative Account Overview Management

Tenable Cloud Security has the ability to display Excessive Permission with a single click. Drilling down into any of the results will provide an overview, details, recommendations, and remediation steps to fix the issues.



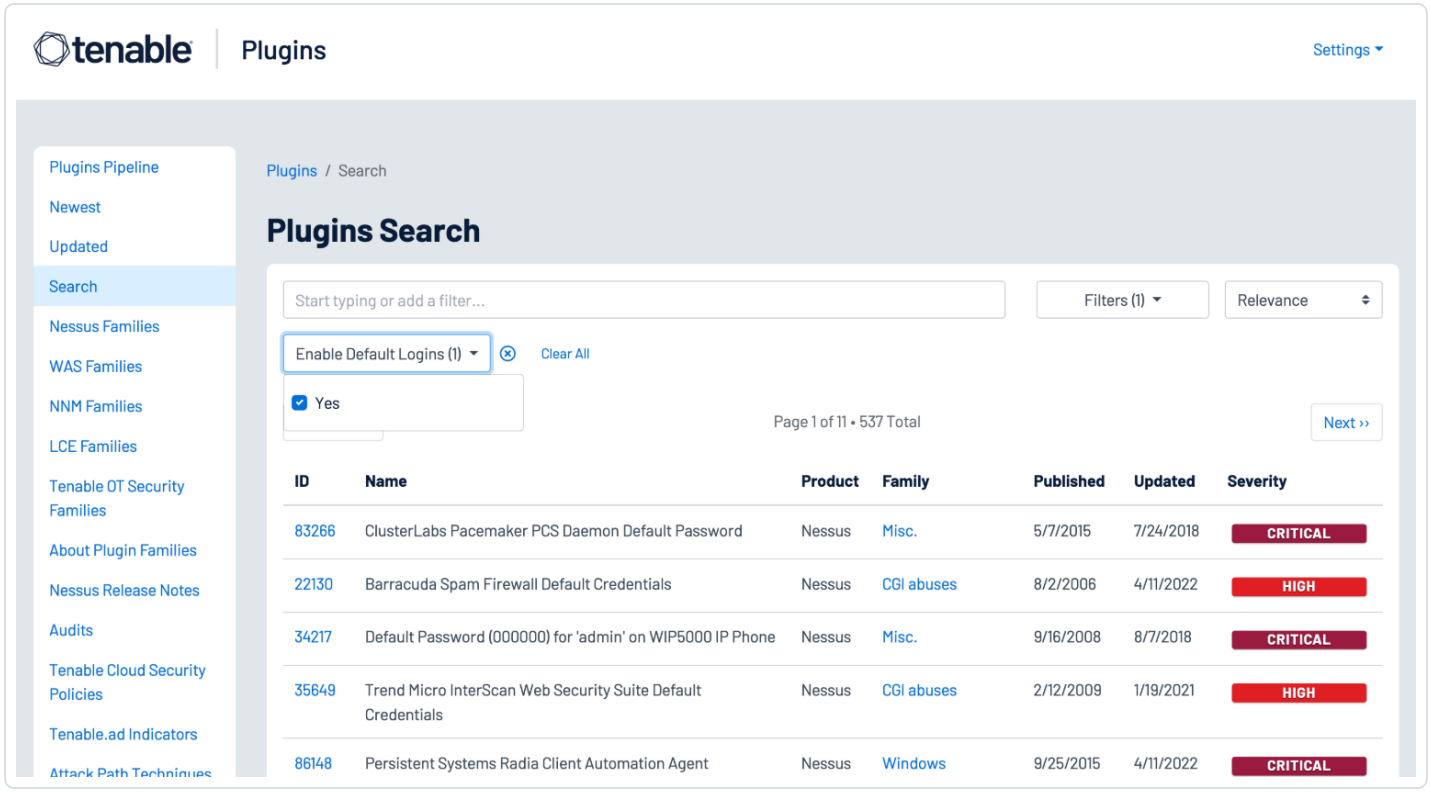
Disable Inactive and Default Accounts

Operating Systems and applications are often distributed with service and default accounts that are either not password-protected or have a default password that is well-known. Tenable Nessus and Tenable Identity Exposure help identify these accounts, enabling organizations to review and disable any unnecessary accounts to reduce the attack surface. Organizations can leverage the following Nessus plugins to enumerate service and default accounts:

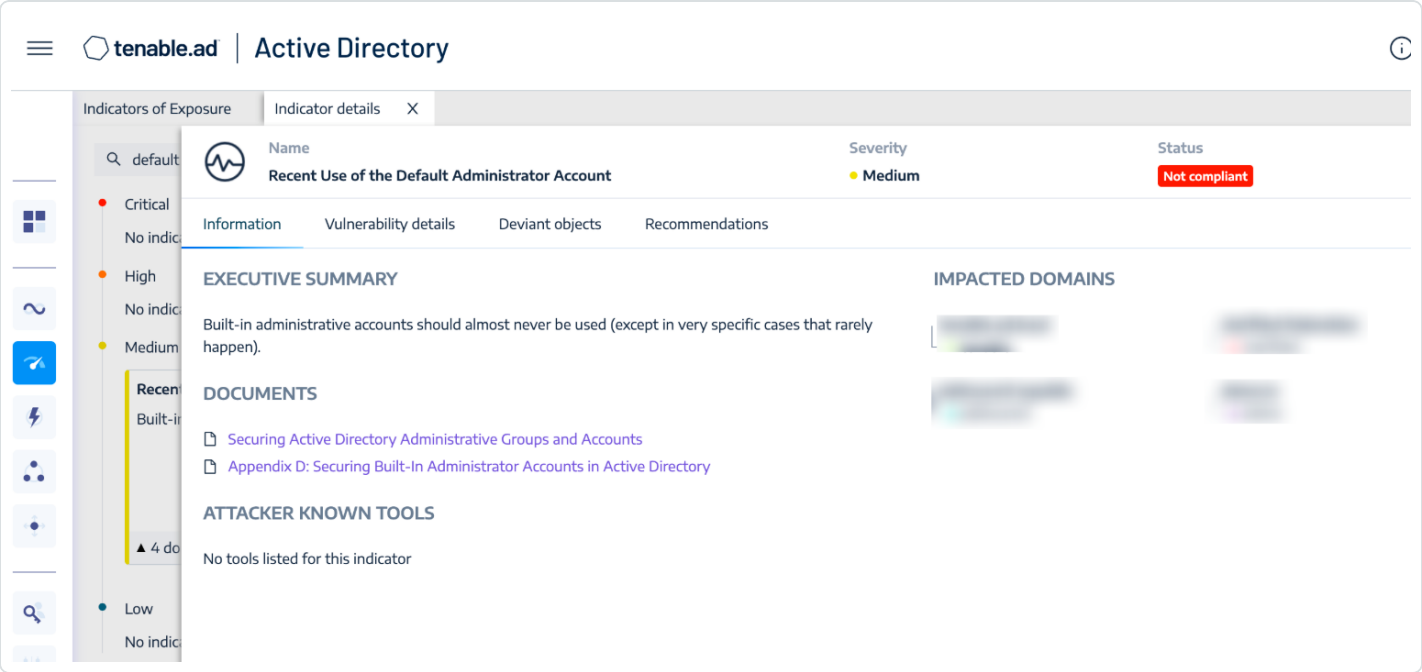
- **Plugin Family: Default Unix Accounts** – This plugin family contains over 170 Nessus plugins that check for the existence of default accounts/passwords on a number of devices. In addition, there are many plugins that check for simple passwords such as “0000”, “1234”, and more commonly identified password combinations for “root” or administrator accounts.
- **171959 Windows Enumerate Accounts** – This plugin enumerates all Windows Accounts

Several hundred plugins can be identified by searching for “Default Account” from the Nessus Plugins Search page using the Enable Default Logins filter. Nessus default account plugins are

available for Databases, Web Servers, SCADA devices, Unix/Linux devices, Cisco devices and more. Many of the plugins are associated with the Default Unix Account Nessus family, however, many are in other families as well.



In addition, Tenable Identity Exposure provides the ability to determine if a default administrator account was recently used in the environment, as shown in the image below:



Note: User accounts that have not been accessed in more than a year provide an opportunity for attackers to leverage compromised credentials and perform brute-force attacks. Nessus plugins 10915 or 10899 Microsoft Windows - Local Users Information: User Has Never Logged In displays a list of Windows accounts where the user has never logged in. The Sleeping Accounts Indicator of Exposure in Tenable Identity Exposure detects accounts that have not been accessed in over a year.

MFA

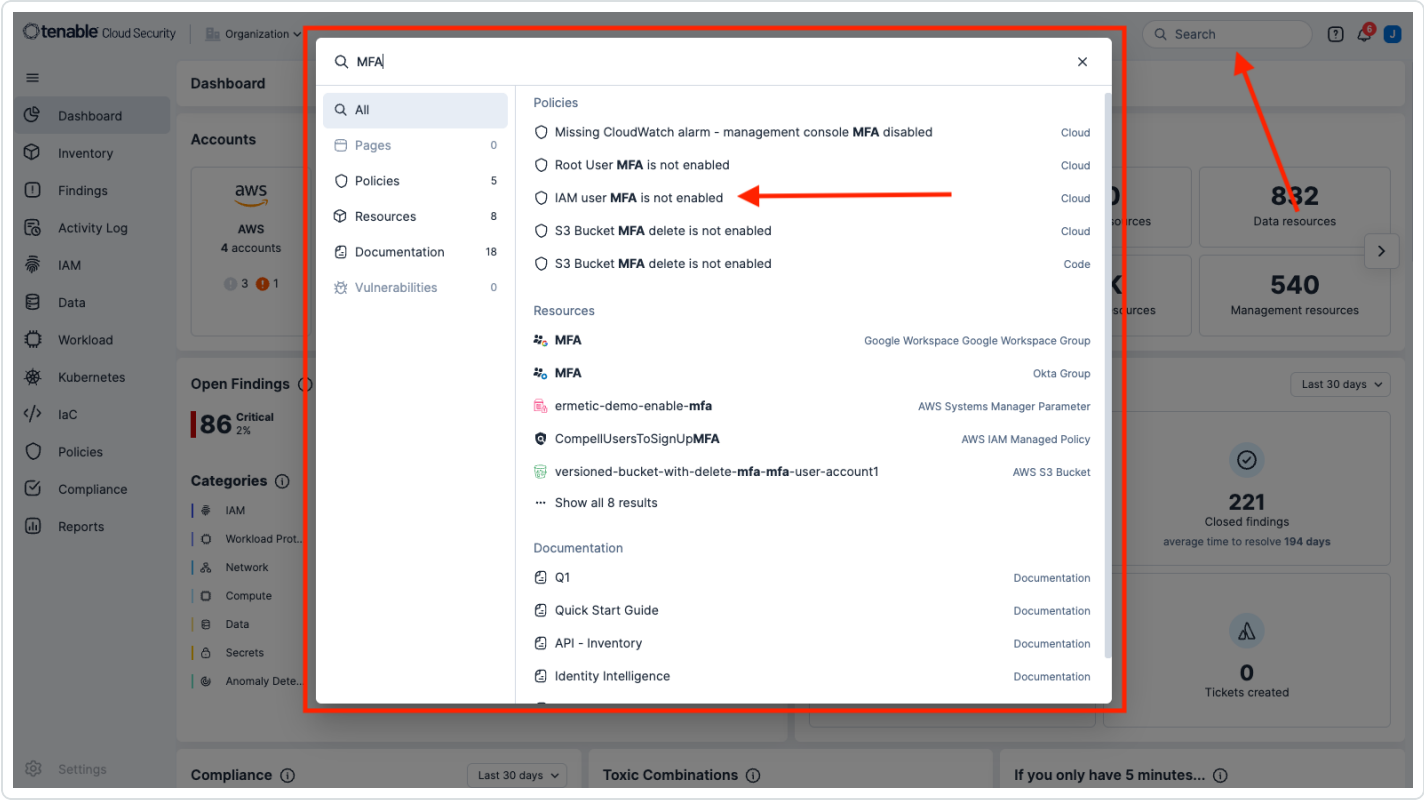
Within this section, information is provided which addresses the following questions.

A7.14. Do all of your cloud services have multi-factor authentication (MFA) available as part of the service?

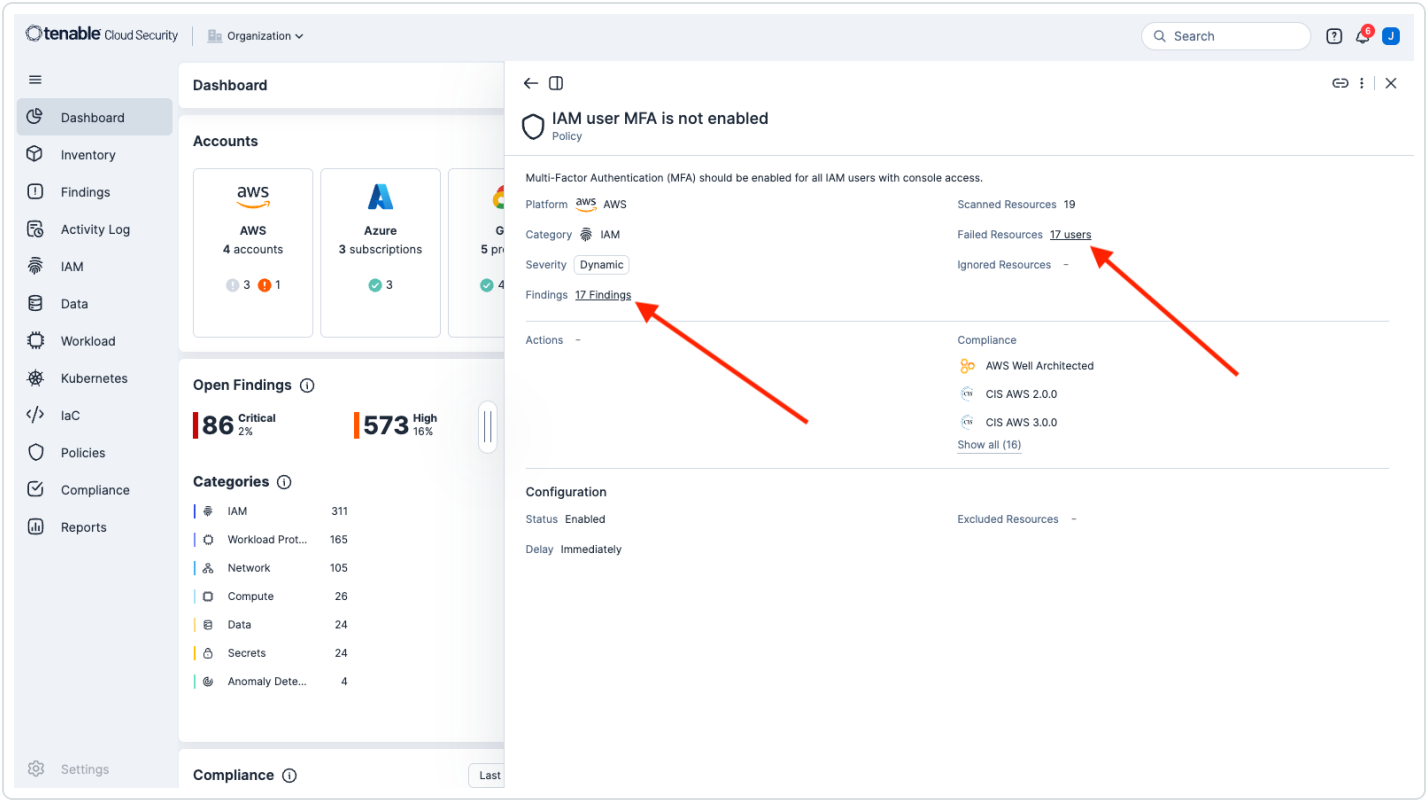
A7.16. Has MFA been applied to all administrators of your cloud services?

A7.17. Has MFA been applied to all users of your cloud services?

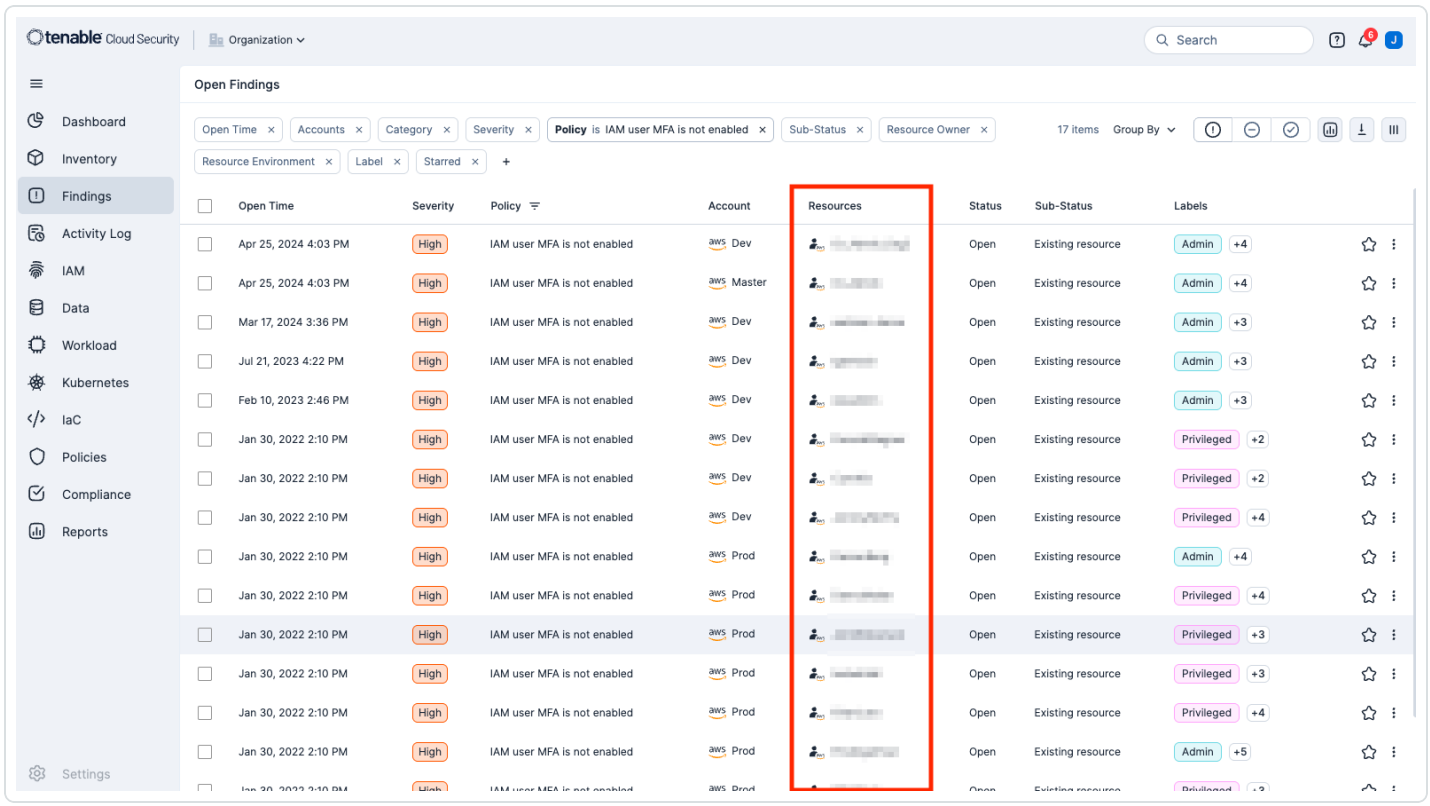
Within Tenable Cloud Security, key search terms can be entered into the search bar in the top right corner. For this example, entering MFA returns the following search results, displayed below. From these search results “IAM user MFA is not enabled” will be selected.



A new window will be opened displaying a summary of the findings. To view the users with no MFA enabled, clicking the **Failed Resources** link will open a pop up with only a user listing. For more detail, select the **Findings** link.



The Findings page is then displayed with additional information, including a column displaying each user that does not have MFA enabled (usernames pixelated for public release in this document. Normally, all usernames are clearly visible). From here analysts can continue to drill down and gather additional information on the **Open Findings** page.



See Also

- About Cyber Essentials
- Getting Started with the Scope of Assessment
- Key Component 3: Access Control
- Key Component 1: Firewalls and Internet Gateways
- Key Component 2: Secure Configuration
- Key Component 4: Malware Protection
- Key Component 5: Patch Management
- References

Key Component 4: Malware Protection

The focus of this key component is Malware Protection. Malicious software, or “malware” is software that is designed to cause harm to information systems and is one of the biggest challenges organizations face in maintaining cyber hygiene. Malware exploits weaknesses and vulnerabilities to make software or hardware perform actions not originally intended. Malware protection is one of the five key technical controls in the Cyber Essentials. This key component applies to all the following in scope devices: Boundary Firewalls, Desktop Computers, Laptops, Routers, Servers, Iaas, PaaS, and SaaS devices.

The goal is to ensure that all devices are protected from malware (viruses, worms, trojans, ransomware, spyware) which can lead to data breaches, system outages, and financial loss. The Cyber Essentials requires organizations to implement at least one of the following methods to protect against malware:

- Application Allow Listing
    - Only approved applications are allowed to run
- Anti-Malware Software
    - Traditional antivirus/antimalware tools (such as Microsoft Defender), configured to conduct regular scans, and set applications to receive automatic updates and security patches
- Sandboxing
    - Running applications in isolated environments.

Devices that can not support malware protection (such as some IoT devices) must be segregated from other systems using appropriate controls such as firewalls and/or network isolation.

Malware Protection Assessment Questions Directly Addressed

Questions in this section apply to: servers, desktop computers, laptops, tablets, thin clients,

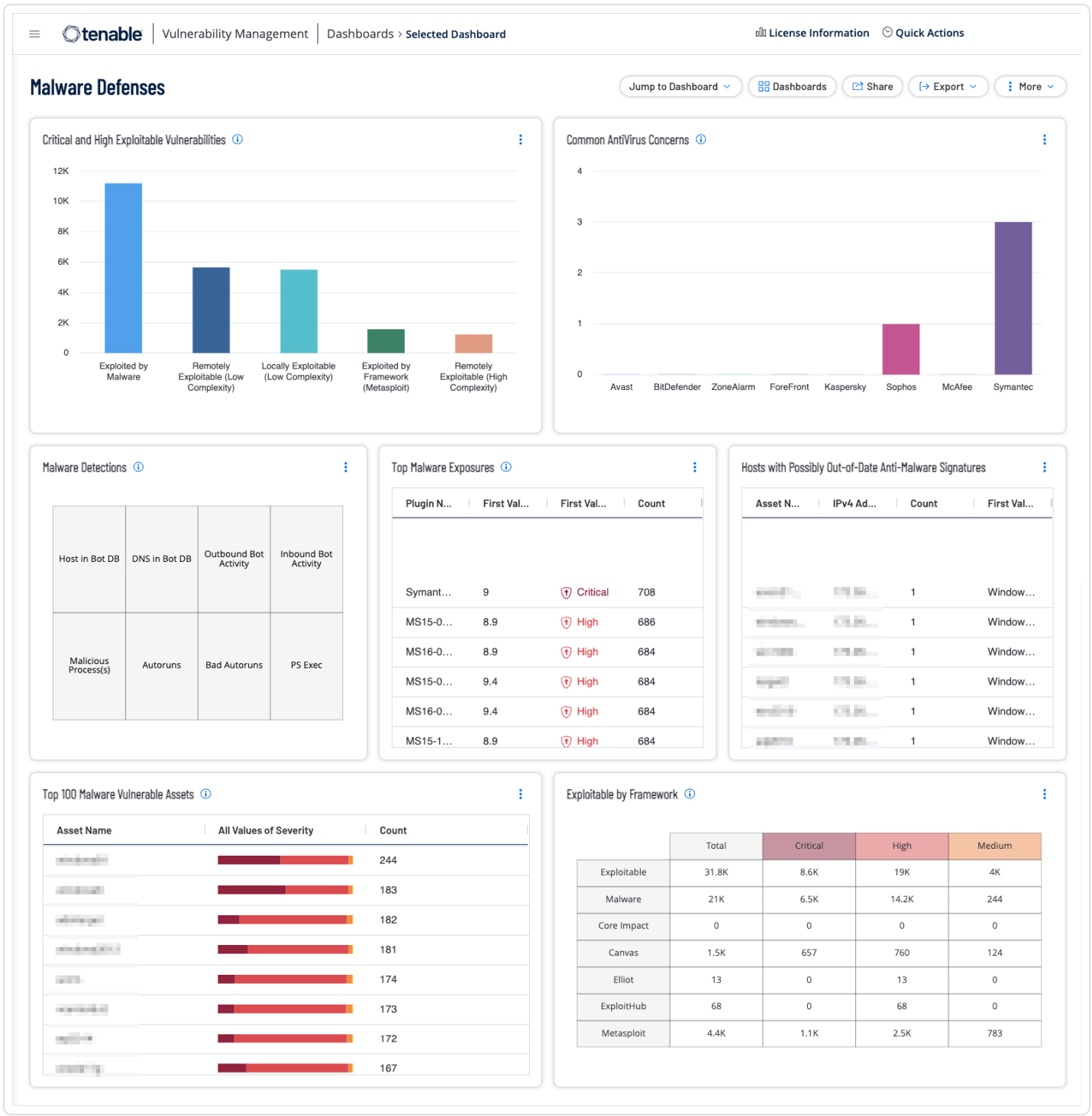
mobile phones, IaaS, PaaS and SaaS. Within this section, information is provided which addresses the following questions.

A8.1. Are all of your desktop computers, laptops, tablets and mobile phones protected from malware

A8.2.Is anti-malware software set to update in line with the vendor's guidelines and prevent malware from running on detection

Tenable Security Center and Tenable Vulnerability Management enables organizations to evaluate vulnerability data gathered from multiple active and passive scanners distributed across the enterprise. The Tenable Vulnerability Management Malware Defenses dashboard provides the necessary context to understand which assets in the organization are vulnerable to malware exploitation.

More information can be found by referring to the Malware Defences Cyber Exposure Study.



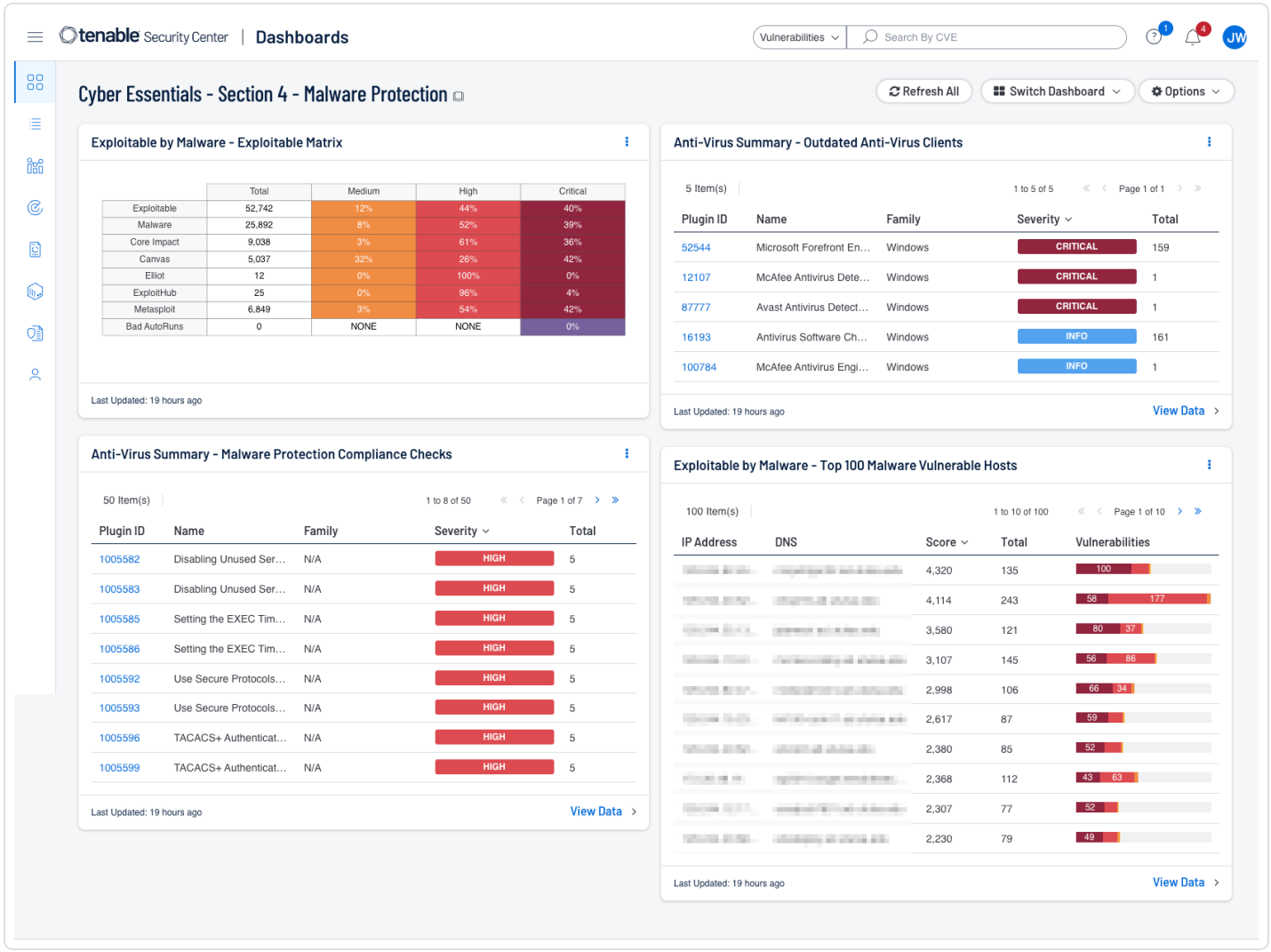
Malware threats are one of the most common and damaging cyber threats. The primary objective is to defend against threats, such as malware, viruses, ransomware, and others. Section 4 ensures you have an active protection in place for protection. Active protection helps prevent business disruptions from downtime, and costly recovery efforts. These dashboard highlight concerns that have been identified in the environment to help organisations address malware concerns.

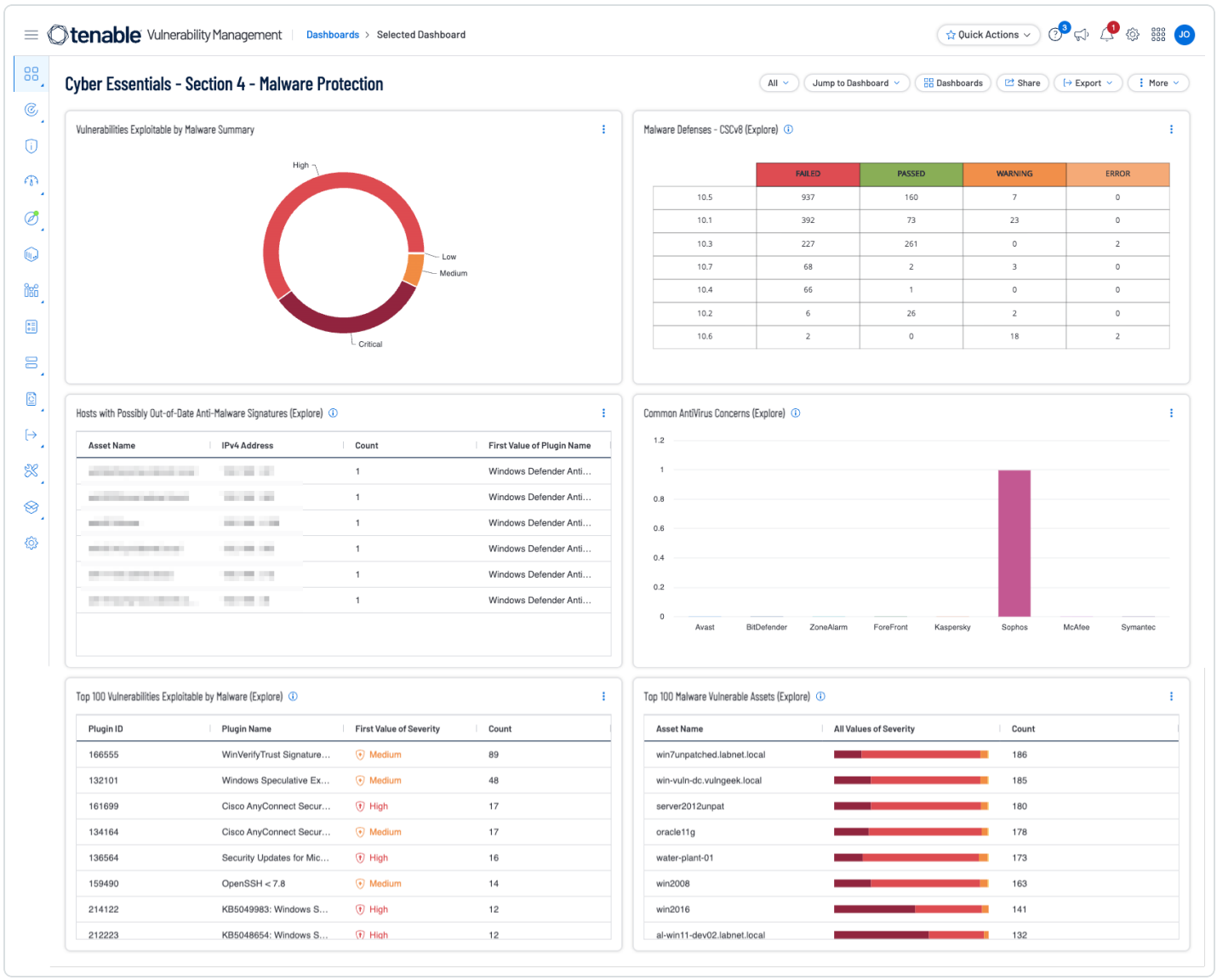
Tenable has provided a Cyber Essentials Dashboard and Report for Tenable Security Center and Tenable Vulnerability Management for this Key Component. Those dashboards and reports can be found here by using the term “Cyber Essentials” as a search query:

Security Center Dashboards and Reports

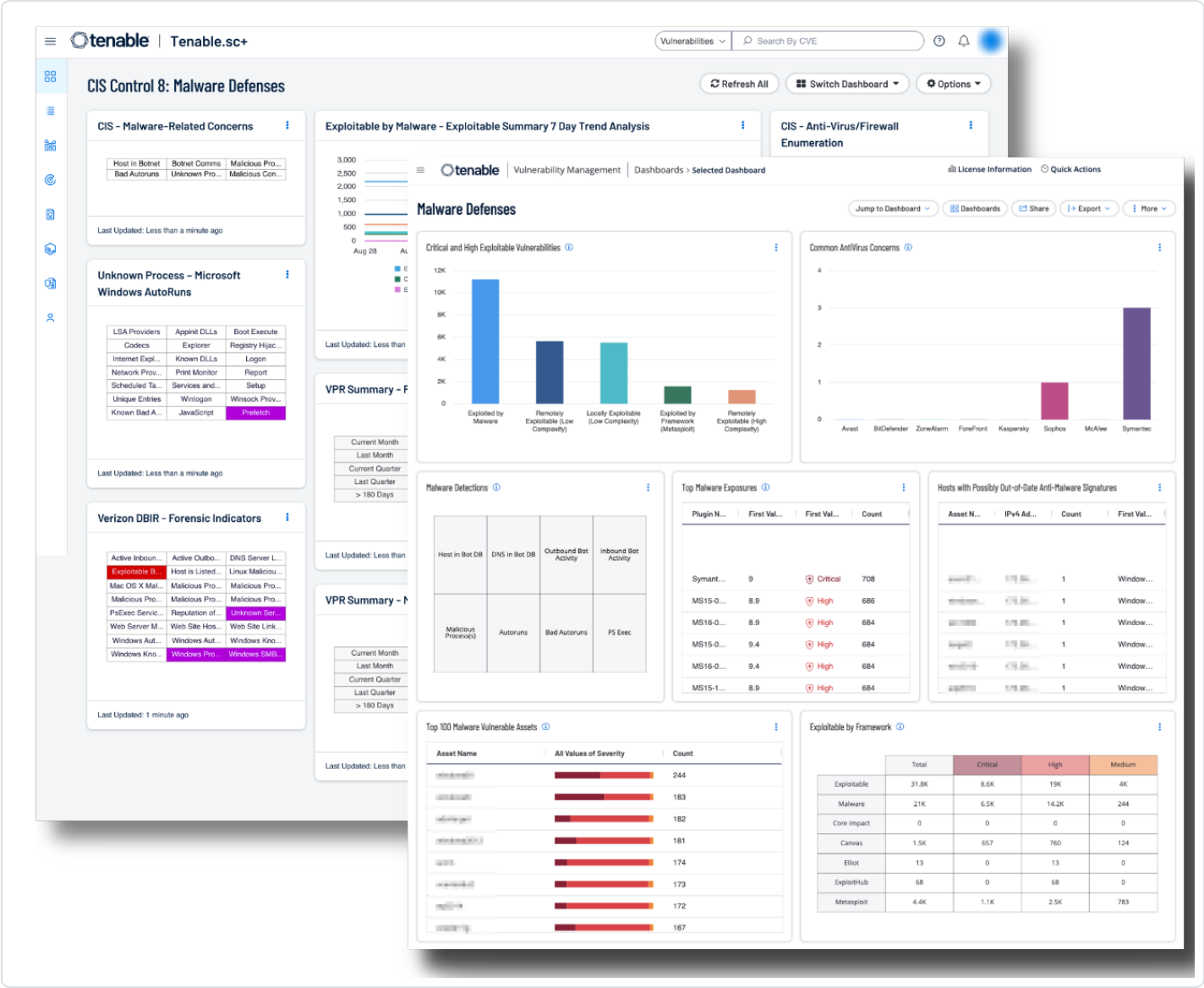
Vulnerability Management Dashboards and Reports

Shown below are screenshots of this section's dashboards for Security Center and Vulnerability Management.





Additionally, a critical part of keeping the network secure is enabling a continuous monitoring strategy and monitoring of all possible network endpoints. Information gathered from Tenable products provides organizations with a complete picture of malicious activity, malware infections, and compromised hosts. Tenable provides Malware Defense dashboards for Tenable SC (based off CIS Control 8) and Tenable Vulnerability Management which provide a detailed view of potential malware, suspicious processes, and malicious activity, enabling security analysts to easily identify malware activity on hosts. Data collected provides valuable information from devices and services on suspicious files, unauthorised logins, malicious websites, requests, and more. Systems are scanned for malicious backdoors, botnet activity, potential malware, and unknown processes. Indicators provide information on systems communicating with botnets or other malicious hosts.



Tenable Cloud

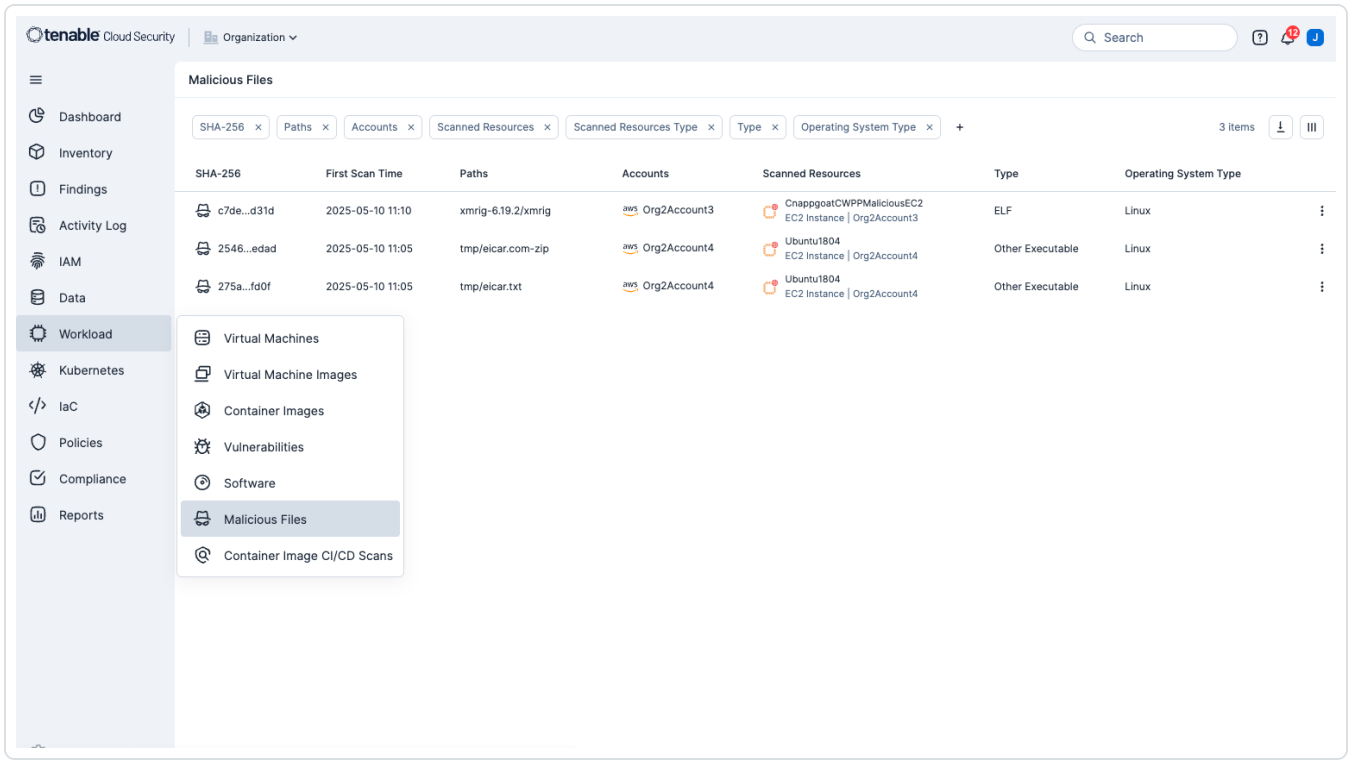
Tenable Cloud Security has unique Malware Scanning features that allow for the detection of potentially malicious files in your workloads. Tenable Cloud Security scans workloads for malicious executable files (such as a DLL), then generates a SHA-256 hash for each file. The hash is sent to a known reputation service, if the hash is known metadata about the file, combined with a reputation verdict from all supported malware engines is received.

This data is analysed and used to calculate a proprietary view on the level of maliciousness of the file. If the file is determined to exceed the threshold in terms of the number and type of vendors who deem the file to be malicious, a record of threat is created. This record is then available in the Tenable Cloud Security Console as a **malicious file** and a **finding**.

Note: Tenable Cloud Security only scans the following workload components for malicious files: Resource Types of: Virtual Machines, Container Images that are being used by workloads. Operating Systems: Linux, Windows. Cloud Providers: AWS, Azure, GCP

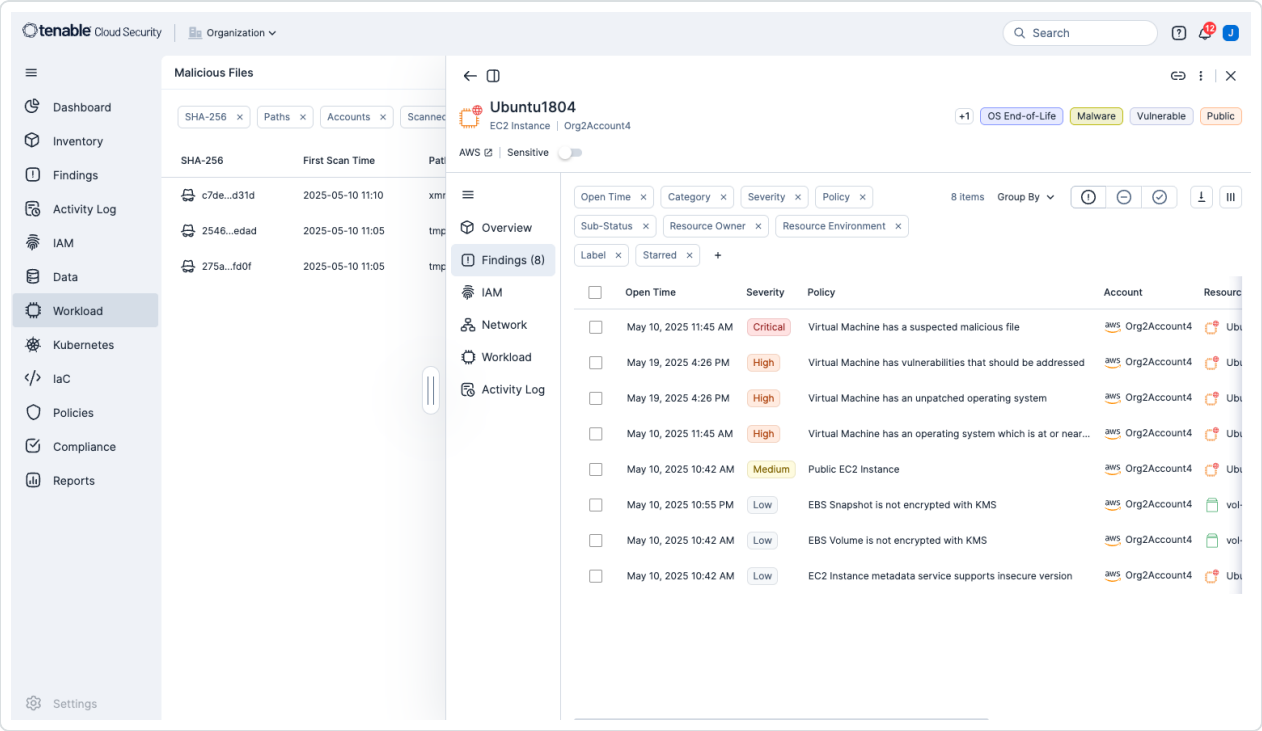
To view scan results:

1. In the Tenable Cloud Security Console, click Workload Protection > Malicious Files. The Malicious Files page displays all potentially malicious files identified by Tenable. See Malicious Files Column Data for more information.



2. Filter the table to narrow the scope of the visible data. Use the column picker on the top right of the table to choose which columns to display.
3. To mark a file as trusted, click on the three dots next to the entry and then click Mark as trusted.
4. (Optional) Export all visible data (according to any applied filters) to a CSV file.
5. Click on a SHA-256 entry to see more information about the file. The results open in a slideout panel.

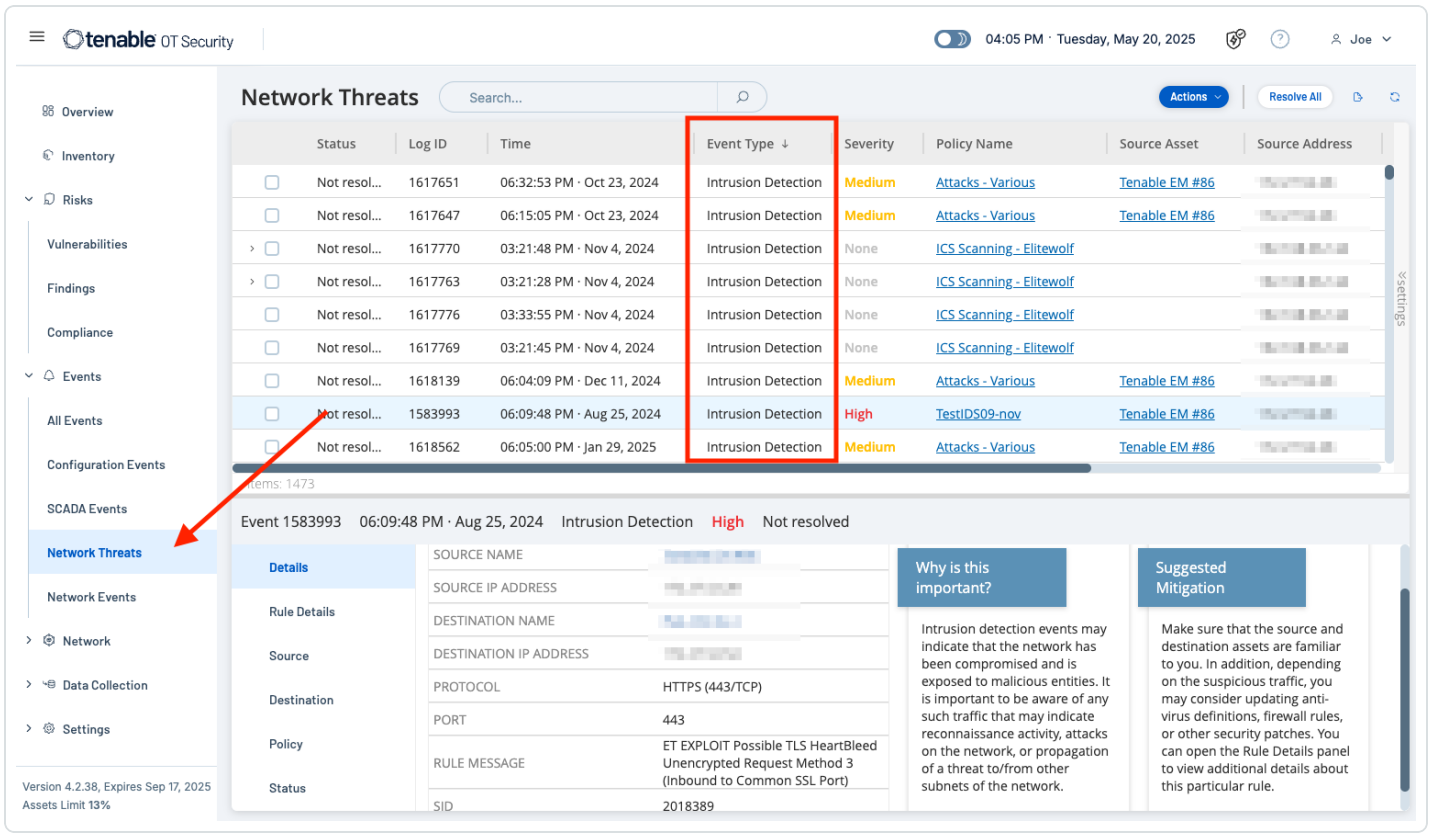
- Click Intelligence (VirusTotal) to see more details about the file on the VirusTotal site.
- To mark the file as trusted, click on the three dots next to the entry and then click Mark as trusted.



Tenable OT

Malware detection within Tenable OT is accomplished based on communications from the device and IDS Policy Events. Intrusion detection events may indicate that the network has been compromised and is exposed to malicious entities. It is important to be aware of any such traffic that may indicate reconnaissance activity, attacks on the network, or propagation of a threat to/from other subnets of the network.

From the Events tab, navigate to Network Threats to view these types of events. Filters allow analysts to focus and narrow down results.



See Also

- About Cyber Essentials
- Getting Started with the Scope of Assessment
- Key Component 4: Malware Protection
- Key Component 1: Firewalls and Internet Gateways
- Key Component 2: Secure Configuration
- Key Component 3: Access Control
- Key Component 5: Patch Management
- References

Key Component 5: Patch Management

The focus of this key component is Patch Management. Unpatched vulnerabilities create known weaknesses that attackers can readily exploit. Well known is the fact that a large number of data breaches and ransomware attacks are directly attributed to systems with known, unpatched vulnerabilities. Organizations are brutally aware of the reasons for patching, such as regulatory compliance, risk mitigation, system stability, business continuity, reputation, and customer trust. Patch management is not just a technical necessity. Patch management is a strategic imperative for protecting assets, maintaining trust, and ensuring the resilience and sustainability of the organization.

Yet there are many challenges with regards to patching that must be addressed:

- Patching is time-consuming, requiring a significant amount of time to conduct vulnerability assessments, patch deployment, and testing.
- Patching requires down time, requiring restarts, downtime. Systems can crash, application errors can occur, and the potential to disrupt business operations is often high.
- There are external factors involved such as relying on vendors to release patches, and organizations having limited access to equipment and resources.

This key component applies to all the following in scope devices: Boundary Firewalls, Desktop Computers, Laptops, Routers, Servers, Iaas, PaaS, and SaaS devices. The goal is to ensure that all devices are kept up to date with the latest security patches, reducing the risk of exploitation to known vulnerabilities. The Cyber Essentials requires organizations to:

- Apply security patches promptly (within 14 days of release). This applies to all operating systems, applications, and firmware (routers/firewalls).
- Remove and Replace all unsupported and outdated software. End-of-Life software must not be used unless the software is isolated and mitigation controls and/or compensating controls are in place.
- Automatic updates are enabled where possible

Patch Management Assessment Questions Directly Addressed

Questions in this section apply to: servers, desktop computers, laptops, tablets, thin clients,

mobile phones, IaaS, PaaS and SaaS. Within this section, information is provided which addresses the following questions.

A6.2.1 Please list your internet browser(s) The version is required.

A6.2.2 Please list your malware protection software The version is required

A6.2.3 Please list your email applications installed on end user devices and servers. The version is required.

A6.2.4 Please list all office applications that are used to create organisational data. The version is required.

A6.3. Are any of the in-scope software or cloud services unlicensed or unsupported?

A6.3.1 If yes to A6.3, please list the unsupported or unlicensed software or cloud services.

A6.4. Are all high-risk or critical security updates and vulnerability fixes for operating systems and router and firewall firmware installed within 14 days of release?

A6.5. Are all high-risk or critical security updates and vulnerability fixes for applications (including any associated files and extensions) installed within 14 days of release?

A6.6. Have you removed any software installed on your devices that is no longer supported and no longer receives regular updates or vulnerability fixes for security problems?

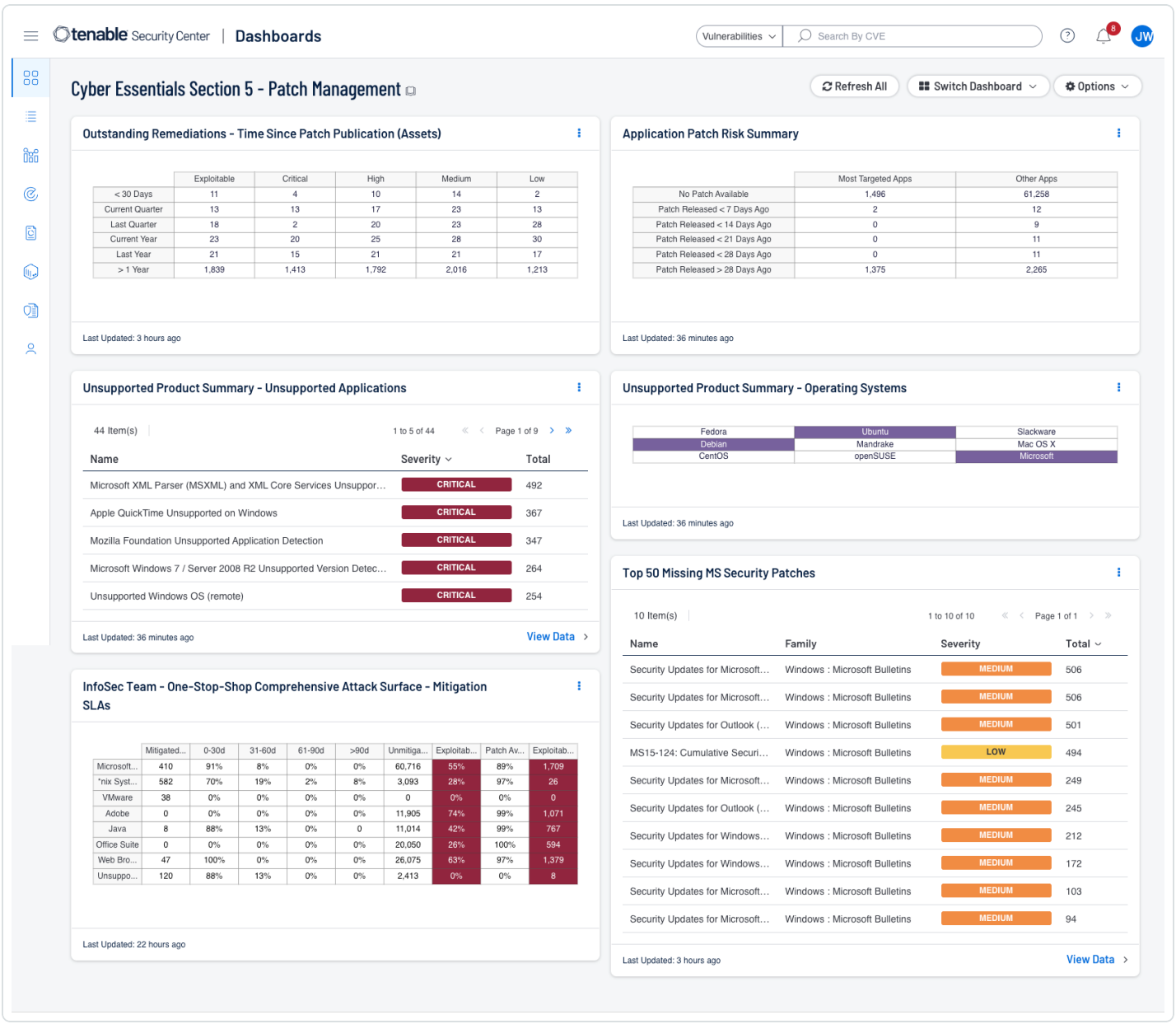
The Cyber Essentials - Section 5 Dashboard assists organizations by presenting a selection of widgets and components that track how application patching is currently being implemented by the organisation. Data provided includes patch rates, current vulnerabilities, and if the vulnerability can be patched or exploited for Operating Systems, and Applications in general. Missing Microsoft Security Updates are also displayed.

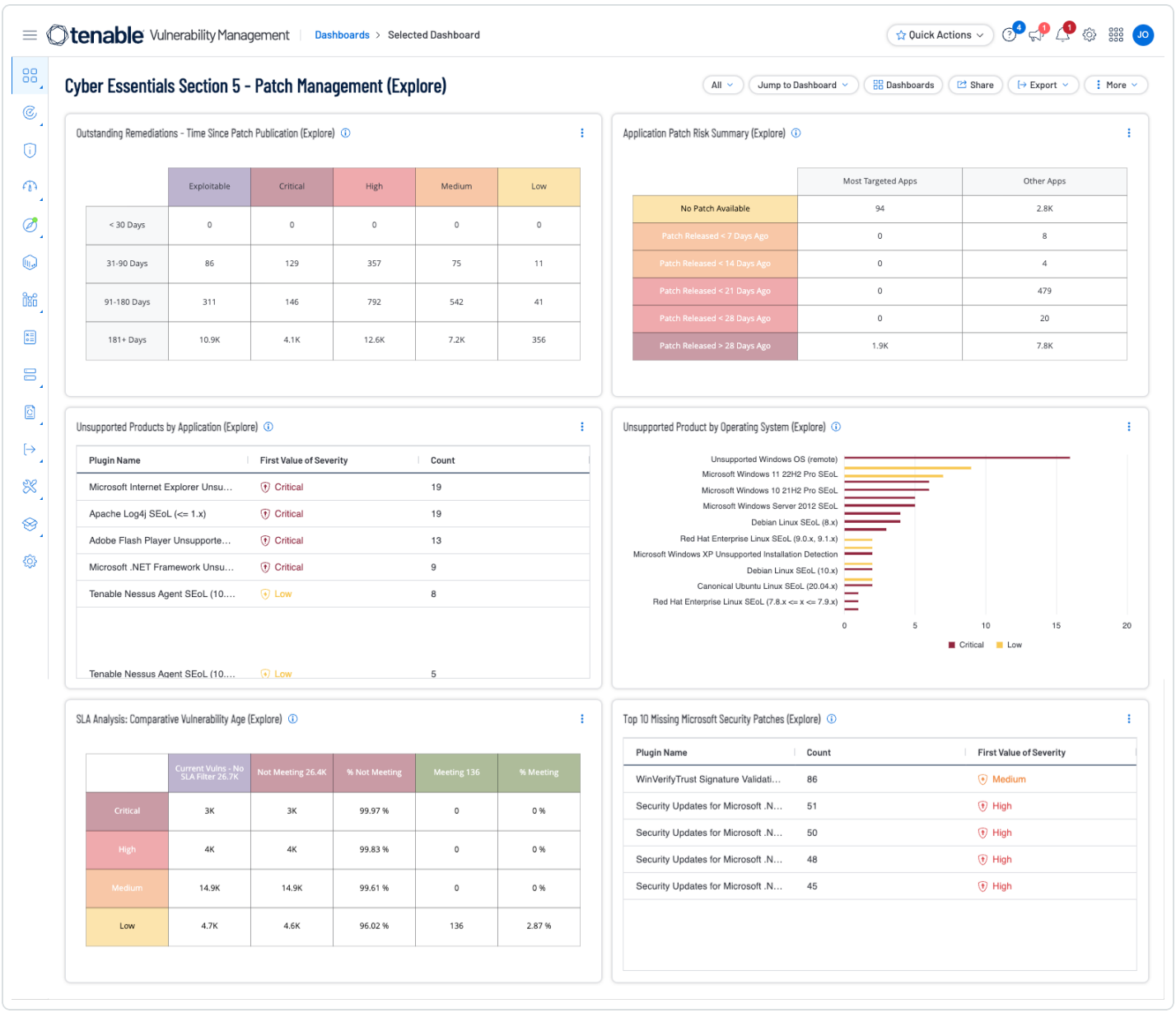
Tenable has provided a Cyber Essentials Dashboard and Report for Tenable Security Center and Tenable Vulnerability Management for this Key Component. Those dashboards and reports can be found here by using the term “Cyber Essentials” as a search query:

Security Center Dashboards and Reports

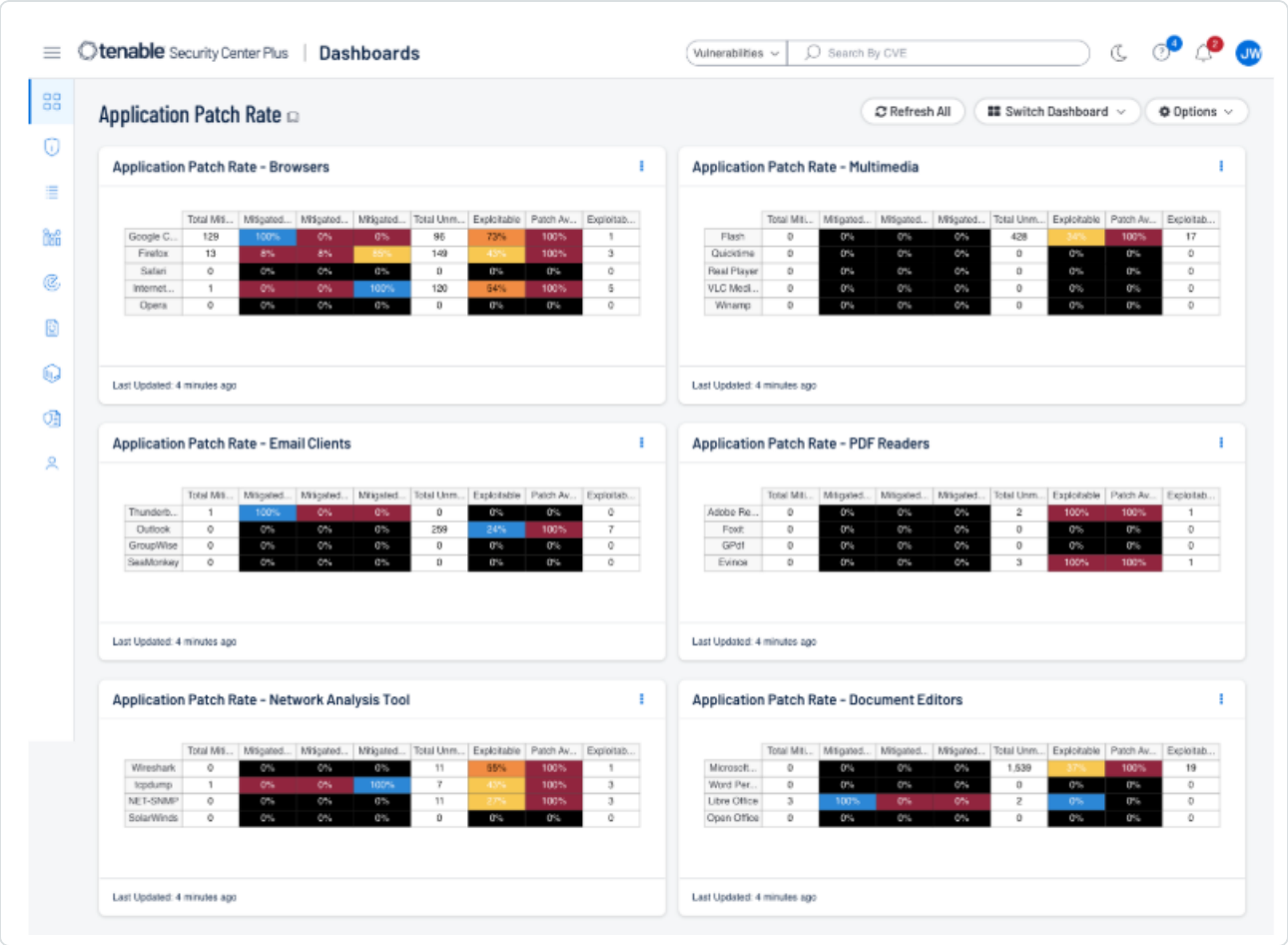
Vulnerability Management Dashboards and Reports

Shown below are screenshots of this section's dashboards for Security Center and Vulnerability Management.


tenable Security Center | Dashboards
Vulnerabilities
Search By CVE
Cyber Essentials Section 5 - Patch Management
Refresh All
Switch Dashboard
Options
Outstanding Remediations - Time Since Patch Publication (Assets)
Exploitable Critical High Medium Low
< 30 Days 11 4 10 14 2
Current Quarter 13 13 17 23 13
Last Quarter 18 2 20 23 28
Current Year 23 20 25 28 30
Last Year 21 15 21 21 17
> 1 Year 1,839 1,413 1,792 2,016 1,213
Last Updated: 3 hours ago
Application Patch Risk Summary
Most Targeted Apps Other Apps
No Patch Available 1,496 61,258
Patch Released < 7 Days Ago 2 12
Patch Released < 14 Days Ago 0 9
Patch Released < 21 Days Ago 0 11
Patch Released < 28 Days Ago 0 11
Patch Released > 28 Days Ago 1,375 2,265
Last Updated: 36 minutes ago
Unsupported Product Summary - Unsupported Applications
44 Item(s)
1 to 5 of 44
Page 1 of 9
Name Severity Total
Microsoft XML Parser (MSXML) and XML Core Services Unsuppor… CRITICAL 492
Apple QuickTime Unsupported on Windows CRITICAL 367
Mozilla Foundation Unsupported Application Detection CRITICAL 347
Microsoft Windows 7 / Server 2008 R2 Unsupported Version Detec… CRITICAL 264
Unsupported Windows OS (remote) CRITICAL 254
Last Updated: 36 minutes ago
View Data
Unsupported Product Summary - Operating Systems
Fedora Ubuntu Slackware
Debian Mandrake Mac OS X
CentOS openSUSE Microsoft
Last Updated: 36 minutes ago
Top 50 Missing MS Security Patches
10 Item(s)
1 to 10 of 10
Page 1 of 1
Name Family Severity Total
Security Updates for Microsoft… Windows : Microsoft Bulletins MEDIUM 506
Security Updates for Microsoft… Windows : Microsoft Bulletins MEDIUM 506
Security Updates for Outlook (… Windows : Microsoft Bulletins MEDIUM 501
MS15-124: Cumulative Securi… Windows : Microsoft Bulletins LOW 494
Security Updates for Microsoft… Windows : Microsoft Bulletins MEDIUM 249
Security Updates for Outlook (… Windows : Microsoft Bulletins MEDIUM 245
Security Updates for Windows… Windows : Microsoft Bulletins MEDIUM 212
Security Updates for Windows… Windows : Microsoft Bulletins MEDIUM 172
Security Updates for Microsoft… Windows : Microsoft Bulletins MEDIUM 103
Security Updates for Microsoft… Windows : Microsoft Bulletins MEDIUM 94
Last Updated: 3 hours ago
View Data
InfoSec Team - One-Stop-Shop Comprehensive Attack Surface - Mitigation SLAs
Mitigated... 0-30d 31-60d 61-90d >90d Unmitiga... Exploitab... Patch Av... Exploitab...
Microsoft... 410 91% 8% 0% 0% 60,716 55% 89% 1,709
*nix Syst... 582 70% 19% 2% 8% 3,093 28% 97% 26
VMware 38 0% 0% 0% 0% 0 0% 0% 0
Adobe 0 0% 0% 0% 0% 11,905 74% 99% 1,071
Java 8 88% 13% 0% 0 11,014 42% 99% 767
Office Suite 0 0% 0% 0% 0% 20,050 26% 100% 594
Web Bro... 47 100% 0% 0% 0% 26,075 63% 97% 1,379
Unsuppo... 120 88% 13% 0% 0% 2,413 0% 0% 8
Last Updated: 22 hours ago



The Application Patch Rate Dashboard for Tenable Security Center presents an additional view of how application patching is currently being handled by the organization. The data provided includes the patch rates, current vulnerabilities, and if the vulnerabilities can be patched and exploited. The colors of the cells within the Application Patch Rate dashboard will change based on the percentage of patches applied. When 95% of vulnerabilities are mitigated the color will be blue. The color will be green for more than 75%, yellow for more than 50%, orange for more than 25%, and red when less that 25% of the vulnerabilities are patched. The total of the 3 columns will total 100%. When the majority of patches applied is in the forth column, a serious review of the patch management system should be conducted, because patches are taking longer than 30 days to be applied.



There is no set timetable to resolve vulnerabilities that fits every situation. SLAs can vary from organization to organization, and even vary between business units within the organization. Tenable recommends aligning SLAs with technology or business objectives, starting with the most important assets.More information on SLAs and Remediation can be found in the SLAs and Remediation section of the Cyber Exposure Study titled Cyber Insurance Report.

Once the highest priority vulnerabilities are identified, operations team needs to take the appropriate action to effectively manage the risk. For each vulnerability, there are three response options – remediate, mitigate, or accept. Which action is chosen for each should be in line with what was previously determined during the initial discovery phase, as you developed a comprehensive understanding of the environment. More information on Tracking and Reporting SLA Progress can be found within Tenable Documentation.

More details on Patch Management, including Operating System and Application Patch Management can be found in the Patch Management section of the Vulnerability Management Cyber Exposure Study

Getting Started with SLAs

Once the highest priority vulnerabilities are identified, operations team needs to take the appropriate action to effectively manage the risk. For each vulnerability, there are three response options — remediate, mitigate, or accept. Which action is chosen for each should be in line with what was previously determined during the initial discovery phase, as you developed a comprehensive understanding of the environment. But to be sure we're clear on our terminology, here's how we define each of them:

Remediate

Oftentimes, remediation is used interchangeably with patching. And in some cases, patching may be all that's required. Something important to note is that typically, applying a patch is just one part of what's required to remediate a vulnerability. The asset may also require removal or rebuilding the operating system, specific software components may need to be upgraded, or there could be a configuration error that needs to be corrected. Once the vulnerability is verified to have been fully remediated, the amount of risk associated with the vulnerability is fully removed from the environment.

Mitigate

Mitigation employs other technologies to reduce the risk of a given vulnerability. This is different from remediation because with mitigation nothing has really been done to actually fix the vulnerability itself. Instead, organizations are accounting for other mitigating factors that neutralise some or all of the risk posed by the vulnerability. For example, organizations may have firewall rules in place that effectively block an exploit from accessing sensitive data. To account for this mitigating factor, organizations would reduce the severity of the vulnerability accordingly.

Accept

Risk acceptance is consciously deciding not to take any action at all. This may be done for a variety of reasons. For example, during the discovery phase, management may have determined some assets are so business-critical they can't afford to take them down for maintenance unless the vulnerability is also business-critical. In other cases, the cost of the fix may be greater than the cost associated with a successful exploit. Regardless of the reason, when organizations choose to accept risk, the VM platform may allow you to remove the risk score from reports or set the score to "0." However, organizations need to understand that while the vulnerability may no longer be immediately visible, the actual risk still remains in your environment.

Note: If you're in an industry subject to regulatory compliance, don't be tempted to develop an assessment plan around passing audits. Limiting assessments to assets that are within audit scope often causes other business-critical systems to be ignored. Remember passing an audit doesn't mean you're secure.

These actions should align with the organizational plans established during the discovery phase of the risk-based VM lifecycle when the business environment was mapped, along with IT policies, and procedures.

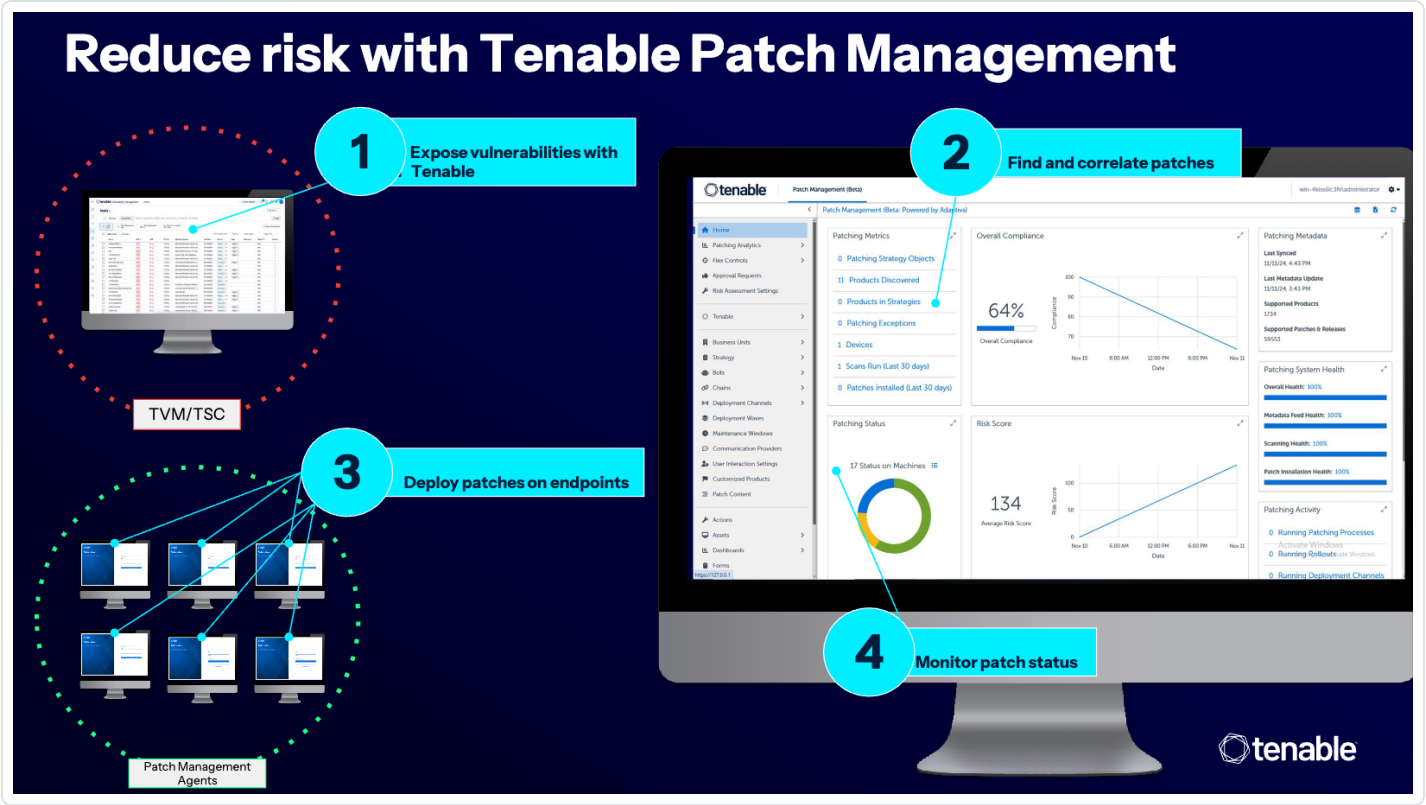
Tenable Vulnerability Management contains the Fundamental Cyber Hygiene Report Card dashboard, which can be reviewed here. As vulnerabilities are identified, remediation must be prioritised and tracked in accordance with organizational goals and Service Level Agreements (SLAs). Reviewing remediated vulnerabilities and the remediation timeframe provides valuable information to the organization on the effectiveness of the risk remediation program.

More information on how Tenable Vulnerability Management and Tenable Security Center can assist can be found in the Tracking and Reporting SLA Progress section of the Tenable Vulnerability Management Cyber Exposure Study.

Tenable Patch Management

For customers that would like to have a patch requirement solution, or are required to have a patch management solution tied into the vulnerability management program, Tenable offers Tenable Patch Management. Patch Management allow organizations to:

- Correlate vulnerabilities to patches
- Easily tracks remediation compliance status with dedicated dashboards
- Allows teams to determine how and where remediation actions are deployed
- And maximises ROI by leveraging autonomous patching with customizable guardrails around approval workflows, version control, device type, and more.



Note: Tenable Patch Management requires Tenable Vulnerability Management, Tenable Security Center, or Tenable One and is not available as a standalone product.

More information on Tenable Patch Management is available here.

References:

Cyber Essentials Self-Assessment Preparation Booklet

IASME Consortium Ltd.

Cyber Essentials: Requirements for IT infrastructure v3.2

National Cyber Security Centre - a part of GCHQ

Cyber Essentials Plus Test Specification v3.2

National Cyber Security Centre - a part of GCHQ

See Also

References

Cyber Essentials Self-Assessment Preparation Booklet

IASME Consortium Ltd.

Cyber Essentials: Requirements for IT infrastructure v3.2

National Cyber Security Centre - a part of GCHQ

Cyber Essentials Plus Test Specification v3.2

National Cyber Security Centre - a part of GCHQ

See Also

- About Cyber Essentials
- Getting Started with the Scope of Assessment
- References
- Key Component 1: Firewalls and Internet Gateways
- Key Component 2: Secure Configuration
- Key Component 3: Access Control
- Key Component 4: Malware Protection
- Key Component 5: Patch Management