



Tenable Cyber Exposure Study - NCA ECC / OTCC

Last Revised: March 29, 2024

Table of Contents

NCA ECC / OTCC Overview	3
1-3: Cybersecurity Risk Management	4
2-1: Asset Management	7
2-2: Identity and Access Management	14
Users and Groups	15
Service and Default Accounts	16
User Access Controls	18
User Accounts	19
Privileged Accounts	21
Dormant Accounts	23
Maintenance	25
2-9: Vulnerabilities Management	27
2-10: Penetration Testing	35
2-12: Cybersecurity Incident and Threat Management	37
Learn More	40

NCA ECC / OTCC Overview

The government in Saudi Arabia established the National Cybersecurity Authority (NCA) to create the Operational Technology Cybersecurity Controls (OTCC) which help fulfill the cybersecurity needs related to the development of national cybersecurity policies, governance mechanisms, frameworks, standards, controls, and guidelines. There are four main domains within the OTCC: Cybersecurity Governance, Cybersecurity Defense, Cybersecurity Resilience, and Third-Party Cybersecurity. Tenable assists organizations to proactively monitor the network to discover vulnerabilities in their environment and provide a high-level overview of an organization's vulnerability management program.

This Cyber Exposure Study provides guidance through the following primary sub-domains of the NCA OTCC:

- 1-3: Cybersecurity Risk Management
- 2-1: Asset Management
- 2-2: Identity and Access Management
- 2-9: Vulnerabilities Management
- 2-10: Penetration Testing
- 2-12: Cybersecurity Incident and Threat Management

1-3: Cybersecurity Risk Management

The OTCC sub-domain 1-3 expands on the ECC 1-5 which states:

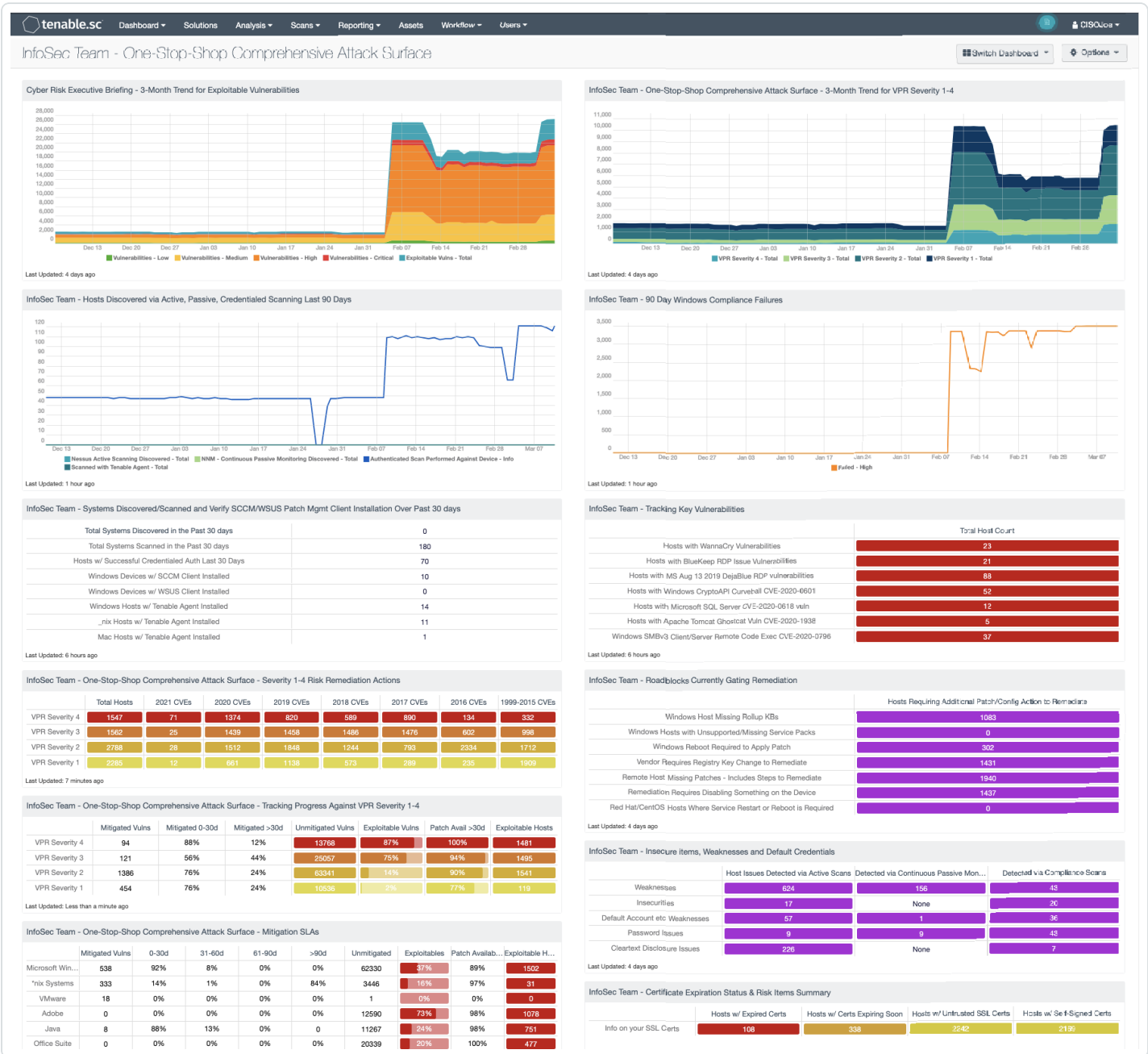
“To ensure managing cybersecurity risks in a methodological approach in order to protect the organization’s information and technology assets as per organizational policies and procedures, and related laws and regulations.”

Tenable assists organizations in following a Risk-Based Vulnerability Management (RBVM) approach. RBVM is a process that reduces vulnerabilities across the attack surface by prioritizing remediation based on the risks they pose to the organization. Unlike legacy vulnerability management, risk-based vulnerability management goes beyond just discovering vulnerabilities. RBVM provides the context needed to help organizations understand vulnerability risks with threat context and insight into potential business impact.

Legacy vulnerability management solutions weren't designed to handle the modern attack surface and the increasing threats. The attack surface is no longer just traditional IT assets, but also includes mobile devices, web apps, cloud infrastructure, containers, Internet of Things (IoT) devices and operational technology (OT) assets. In these modern networks, legacy vulnerability management tools can't deliver complete and timely insights into all of the devices across the entire attack surface. By not identifying these assets and their threat vectors, the organization has unassessed risks and which increases Cyber Exposure.

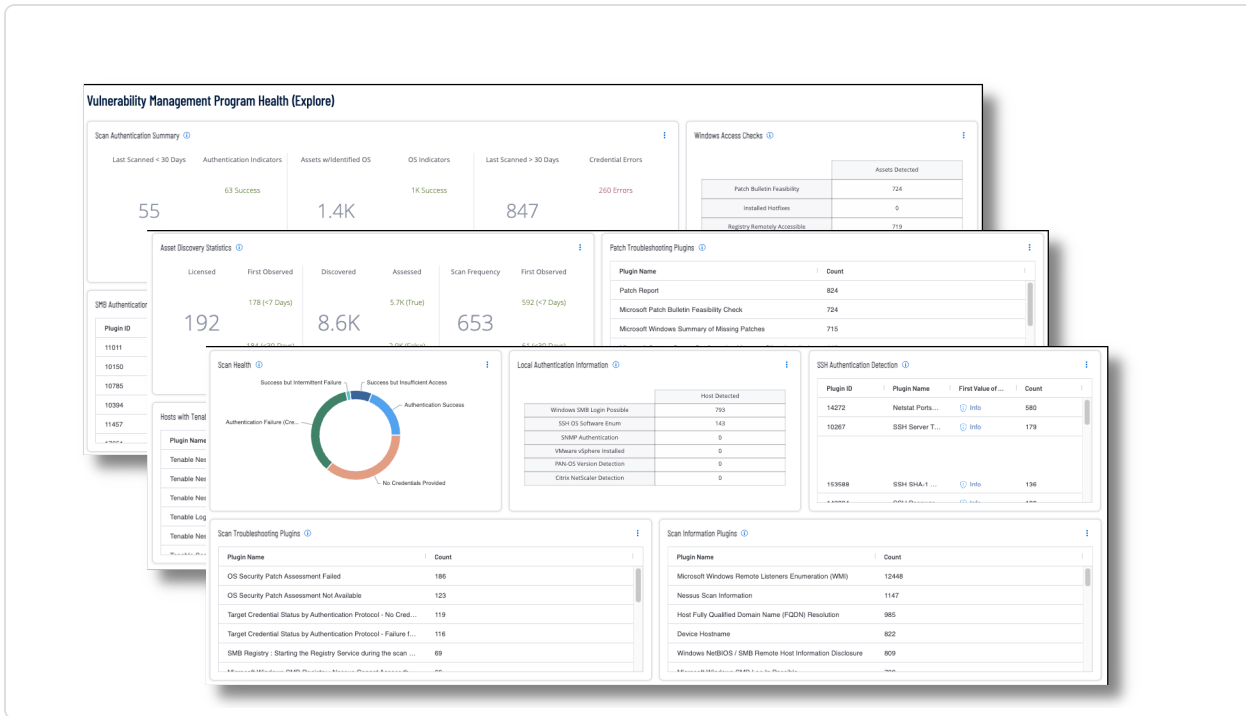
RBVM reduces guesswork, by taking a risk-based approach to vulnerability management, the security team can focus on the vulnerabilities and assets that matter most and address the organization's true business risk instead of wasting valuable time on vulnerabilities attackers may not likely exploit.

The **InfoSec Team - One Stop Shop Comprehensive Attack Surface** dashboard in Tenable Security Center helps the InfoSec team maintain a high level of awareness and vigilance. The filters and components are tailored to guide teams in detecting, predicting, and acting to reduce risk across their entire attack surface. Analysts within information security teams are empowered to analyze findings, remediate identified risks, track progress, and measure success against the organization's charter and SLAs. According to sub-domains 1-3-1-2 within the OTCC, and 1-5-4 within the ECC, risk assessments must be done periodically.



OTCC 1-3 requires risk assessments to be performed on a regular basis, and for most systems that can be actively scanned, this requirement is sustainable; however, in terms of OT devices which can be more fragile systems and cannot be actively scanned, Tenable OT Security can be used to monitor these systems for vulnerabilities and track behaviors. Tenable Vulnerability Management dashboards such as the **Vulnerability Management Program Health** dashboard, helps security operations teams ensure their scanning program is appropriately maintained for an evolving operational technology landscape aligned with business strategy.

The Output Assets filter is only available when using the Asset Summary Tool. When this tool is selected, you have the option to refine the filters to include specific Asset information.



Credentialed or agent scanning with privileged access provides the most comprehensive and accurate scanning results. Credentialed scans originate from a Tenable Nessus scanner that reaches out to the hosts targeted for scanning, while agent scans run on hosts regardless of network location or connectivity and then report the results back to the manager. Credentialed scanning is more complicated than agent scanning and requires authentication with sufficient privileges to enumerate software, installed applications, patch status, and identify configuration problems. Tenable uses multiple protocols, such as SMB, SSH, HTTPS, and SNMP, to conduct authenticated scans against assets. Analysts can drill into the summary information displayed in the dashboard to troubleshoot upstream scanning problems that can adversely impact downstream reporting to stakeholders.

Very often critical business assets are added to the environment without the knowledge of the security or IT teams. Drilling into the data for assets that are discovered but not scanned can reveal assets with a high criticality rating that are not being scanned.

2-1: Asset Management

The diverse location of assets makes the process of discover and identify assets very challenging. Understanding where critical assets are and accurately inventorying assets is the crucial first step in RBVM. Through credentialed scanning, assets can be reliably identified and attributes collected, which enables organizations to establish and validate inventory management. Tenable Vulnerability Management helps validate and collect information needed to maintain a healthy asset inventory. As assets are discovered, an organization can begin to establish an inventory, which can be used to assess and mitigate associated risks to the organization.

For domain 2-1, The National Cybersecurity Authority states:

“To ensure that the organization has an accurate and detailed inventory of OT/ICS assets in order to support the organization’s cybersecurity and operational requirements to maintain the production uptime, safe operations, confidentiality, integrity, and availability of OT/ICS assets.”

Attackers are not tied to a specific timezone and are continuously scanning the address space of target organizations, searching for new and possibly unprotected systems to be attached to the network. Transient devices, such as laptops or Bring-Your-Own-Device (BYOD) devices may be out of synchronization with security updates or already compromised providing a ripe attack vector. Often, hardware may be installed on the network one evening but not configured and patched with appropriate security updates until the following day, providing an easy target for exploitation. Devices that are not visible from the internet can be exploited by attackers who have already gained internal access and are hunting for internal pivot points.

Maintaining a comprehensive and up-to-date asset inventory is a fundamental and critical component of RBVM. Modern IT environments encompass on-premises, cloud infrastructure, mobile devices, ephemeral and transient assets, web applications, IoT devices, and more. Asset identification of all connected assets within an organization is a common baseline requirement in Essential Cybersecurity Controls (ECC) and OTCC. Maintaining an asset inventory is also the critical first step in the Discovery phase of RBVM, allowing organizations to be more proactive. This document provides guidance to establish an asset inventory.

The first step of RBVM begins with asset discovery to identify and map every asset across the environment. Devices can be detected through active scanning and analysis with Nessus Tenable OT Security to build a comprehensive list of assets and provide a clear picture of risk in the environment.

The **Asset Inventory & Discovery (SEE)** Tenable Security Center dashboard 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)

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 Point	

Last Updated: Less than a minute ago

SEE - Host Discovery - Discovery Statistics

	Nessus Scanned	ICMP (up)	ICMP (down)	NNM Discovered	FQDN Discovered	OS Discovered
System Count	3	0	0	0	3	3
<30 Days	3	0	0	0	3	3
>30 Days	0	0	0	0	0	0

Last Updated: Less than a minute ago

WAS Detection

3 Item(s) | 1 to 3 of 3 | Page 1 of 1

IP Address	DNS
10.10.10.10	hostname.domain.com
10.10.10.10	hostname.domain.com
10.10.10.10	hostname.domain.com

Last Updated: Less than a minute 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

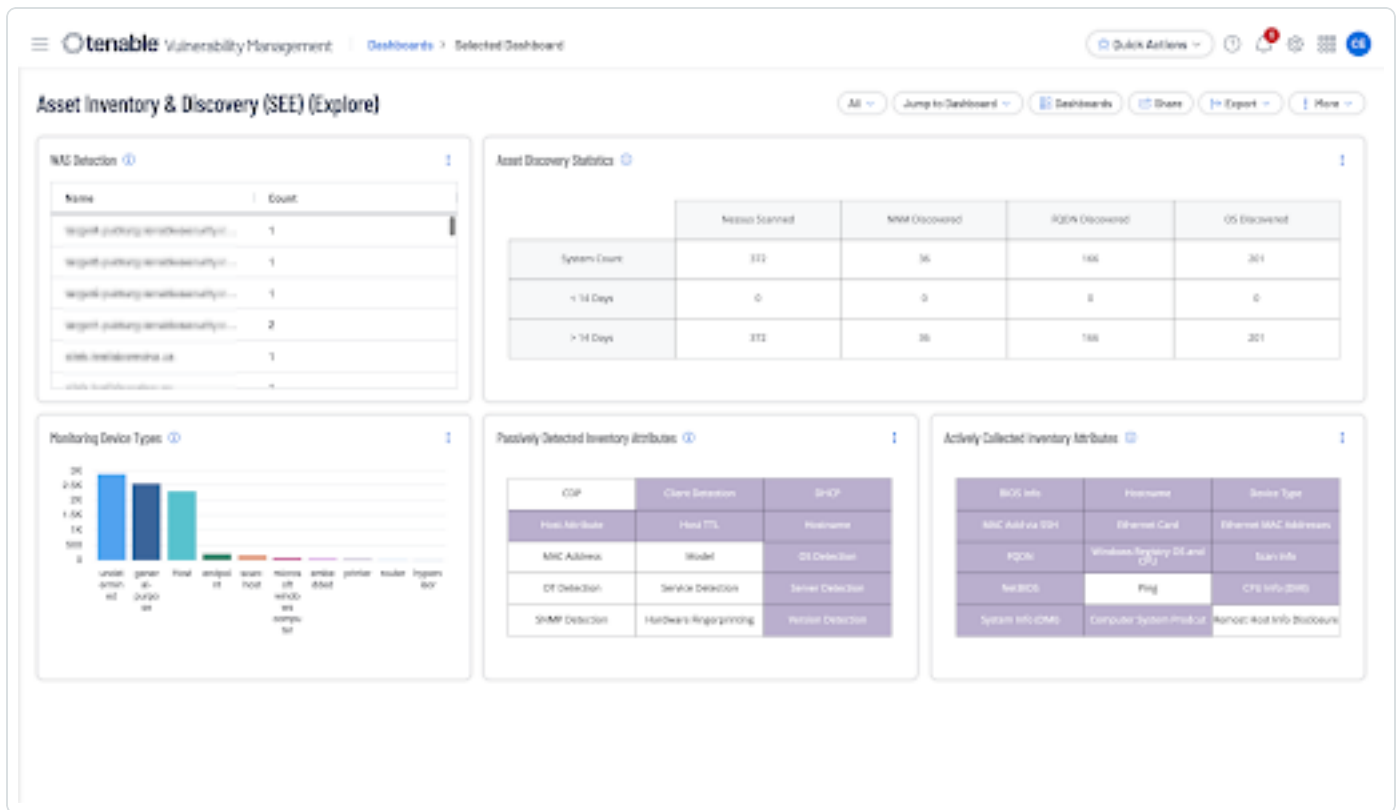
Last Updated: Less than a minute ago

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

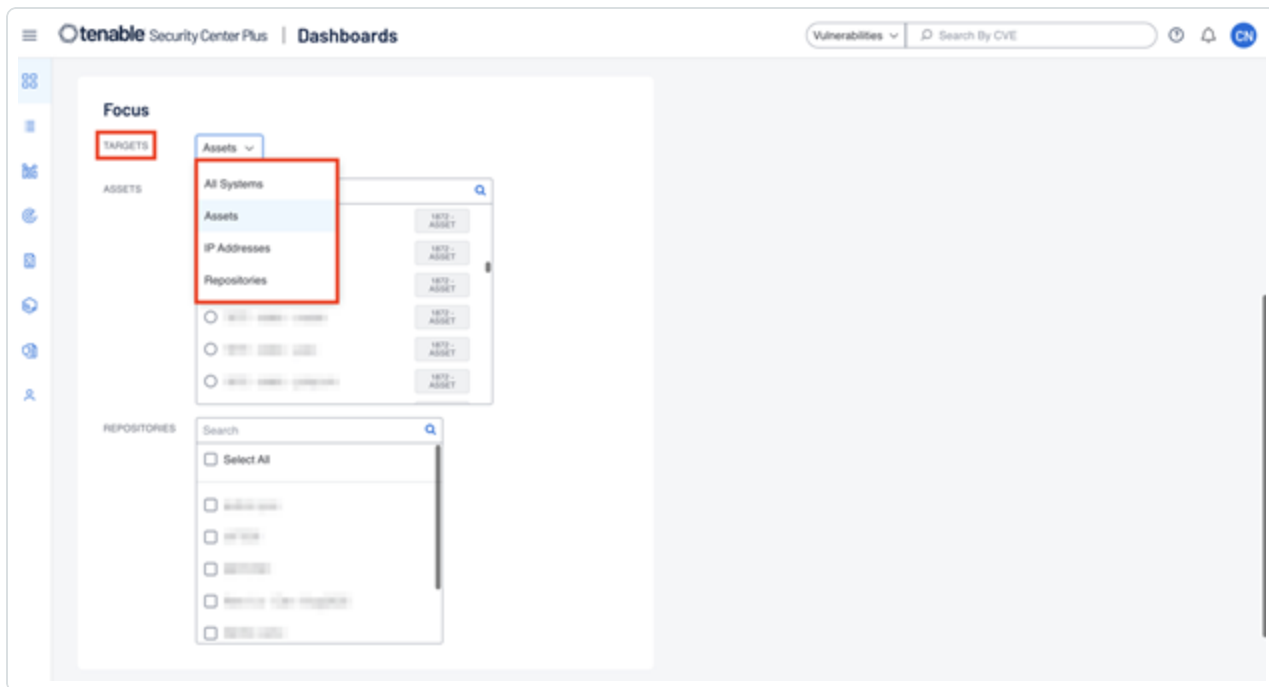
Last Updated: Less than a minute ago

An equivalent to this dashboard also exists within Tenable Vulnerability Management:

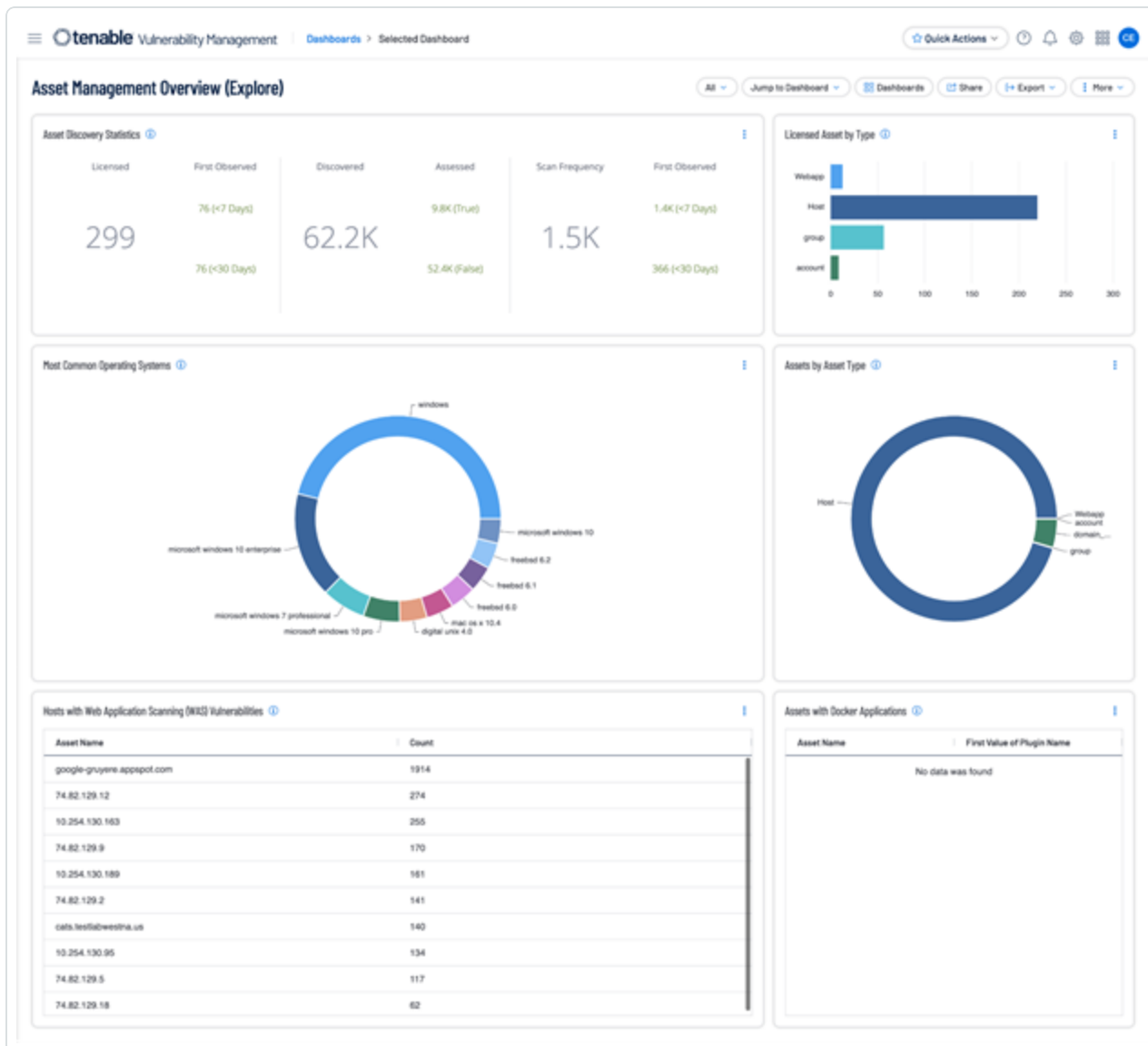


In sub-domain 2-1-1-4, asset owners must be identified and must be involved in through all the inventory and management of their assets. Oftentimes organizations have teams that focus on the detailed information relevant to the teams' assets; or operational focus areas, such as Windows, Linux, databases, or network infrastructure. The dashboard components do not require specific asset list filters to be applied before use. However, organizations with teams that focus on a specific group of assets benefit from using custom asset lists. Information security teams can visualize findings against assets that are "owned by" or "assigned to" specific teams within the organization using this method. Additionally, an Output Assets filter can be set to provide greater insight into where additional resources need to be allocated to mitigate vulnerabilities.

When adding a dashboard in Tenable Security Center from the template library, a focus can be applied to the dashboard to filter the data further. You can change the selection in the **Targets** dropdown from All Systems to Assets, IP Addresses, or Repositories:



Furthermore, organizations must know the status of critical assets to ensure they are appropriately monitored and protected based on each asset's business risk rating. The **Asset Management Overview** dashboard provides summary information about assets in the environment. This information can be leveraged by risk and security managers to ensure the organization's security program is aligned with current business goals.



According to sub-domain 2-1-1-5 of the OTCC, criticality ratings must be assigned to each asset as well as approved by their owners. Tenable assigns an Asset Criticality Rating (ACR) to each asset on the network. ACR assists in prioritizing each asset based on indicators of business value and criticality. ACR is based on several key metrics such as business purpose, asset type, location, connectivity, capabilities, and third-party data. ACRs range from 0 to 10. Assets with a low ACR are not considered business critical. Assets with a high ACR are considered to be the organization's most critical and carry the greater business impact if compromised. The ACR can also be adjusted by the user if deemed the rating needs to be different.

Another asset related metric Tenable established is the Asset Exposure Score (AES). Tenable calculates a dynamic AES for each asset on the network to represent the asset's relative exposure as an integer between 0 and 1000. A higher AES indicates higher exposure. The AES score is

derived from the current ACR (whether tenable provided or custom) and the Vulnerability Priority Ratings (VPR) associated with the asset.

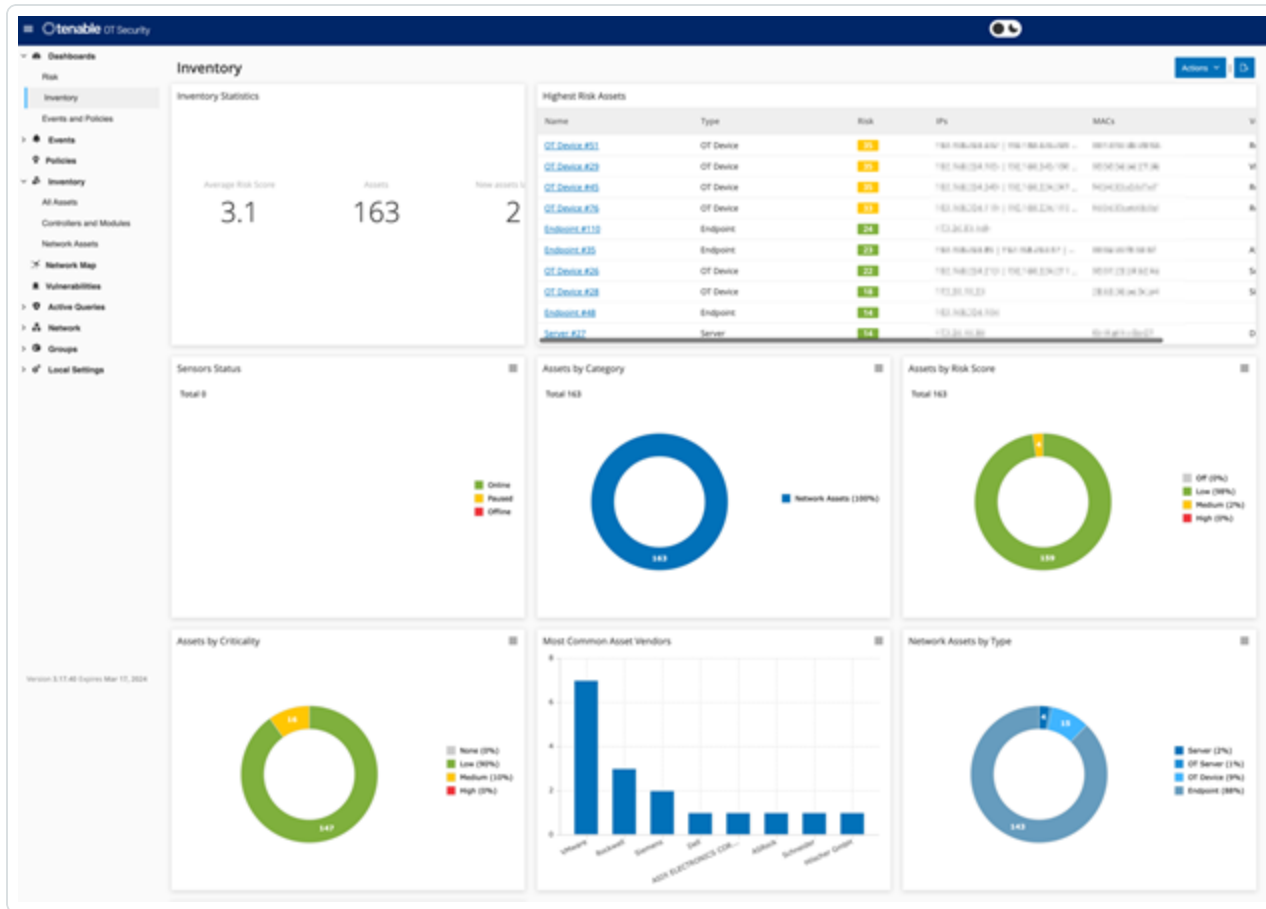
OT Security's **Automated Asset Discovery, Classification, and Management** provides an accurate, up-to-date asset inventory by continuously tracking all changes to devices. This simplifies sustaining of operational continuity, reliability, and safety. OT Security also plays a key role in planning maintenance projects, prioritizing upgrades, patch deployments, incident response, and mitigation efforts.

Name	Type	Risk Score	Criticality	IP	Category	Vendor	Family	Firmware
OT_Device_#51	OT Device	35	Medium	192.168.1.1	Network Assets	Rockwell		
OT_Device_#29	OT Device	35	Medium	192.168.1.2	Network Assets	VMware		
OT_Device_#45	OT Device	35	Medium	192.168.1.3	Network Assets	Rockwell		
OT_Device_#76	OT Device	31	Medium	192.168.1.4	Network Assets	Rockwell		
Endpoint_#110	Endpoint	24	Low	192.168.1.5	Network Assets			
Endpoint_#35	Endpoint	23	Low	192.168.1.6	Network Assets	ASIX ELECTR...		
OT_Device_#26	OT Device	22	Medium	192.168.1.7	Network Assets	Schneider		
OT_Device_#28	OT Device	18	Medium	192.168.1.8	Network Assets	Siemens		
Endpoint_#68	Endpoint	14	Low	192.168.1.9	Network Assets			
Endpoint_#88	Endpoint	14	Low	192.168.1.10	Network Assets			
Endpoint_#38	Endpoint	14	Low	192.168.1.11	Network Assets			
Server_#27	Server	14	Low	192.168.1.12	Network Assets	Dell		
Endpoint_#53	Endpoint	8	Low	192.168.1.13	Network Assets			
Endpoint_#95	Endpoint	8	Low	192.168.1.14	Network Assets			
Endpoint_#95	Endpoint	8	Low	192.168.1.15	Network Assets			
Endpoint_#82	Endpoint	8	Low	192.168.1.16	Network Assets			
Endpoint_#72	Endpoint	8	Low	192.168.1.17	Network Assets			
Endpoint_#90	Endpoint	8	Low	192.168.1.18	Network Assets			
Endpoint_#101	Endpoint	8	Low	192.168.1.19	Network Assets			
Endpoint_#103	Endpoint	8	Low	192.168.1.20	Network Assets			

All of the assets in the network are shown on the **Inventory** screen. Detailed data about each asset is shown, enabling comprehensive asset management as well as monitoring of the status of each asset and its related Events. The data shown in the Inventory screen is gathered using the OT Security Network Detection and Active Query capabilities. The All screen shows data for all types of assets. In addition, specific subsets of the assets are shown on separate screens for each of the following asset types: Controllers and Modules, Network Assets, and IoT. For each of the asset screens (All, Controllers and Modules, Network Assets and IoT), you can customize the display settings by adjusting which columns are displayed and where each column is positioned. You can also sort and filter the Asset lists as well as perform a search.

Additionally, there are three dashboards: Risk, Inventory, and Events and Policies. The dashboards contain widgets that offer an at-a-glance view of your network's inventory and security posture. You can choose a dashboard from the Main Navigation or by clicking on the Dashboards button in the

upper right corner, and selecting one from the menu that is shown. The Risk dashboard is the initial default view. However, you can change the default view to a different dashboard.



The Inventory dashboard provides visibility into the asset inventory, facilitating asset management and tracking. The Inventory dashboard shows widgets such as: Highest Risk Assets, Inventory Statistics, Assets by Risk, Controllers, and Modules by Type, Assets by Purdue Level, etc. Clicking on an asset link takes you to the corresponding asset on the Inventory screen.

2-2: Identity and Access Management

For domain 2-2, The National Cybersecurity Authority states:

“To ensure secure and restricted logical access to OT/ICS assets in order to prevent unauthorized access and allow only authorized access for users, which are necessary to accomplish assigned tasks.”

Leveraging Tenable Security Center, Tenable Vulnerability Management, and Tenable Identity Exposure 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, agentless Active Directory security solution that helps organizations analyze their complex Active Directory environment, predict what matters most to reduce risk, and eliminate attack paths before they can be exploited.

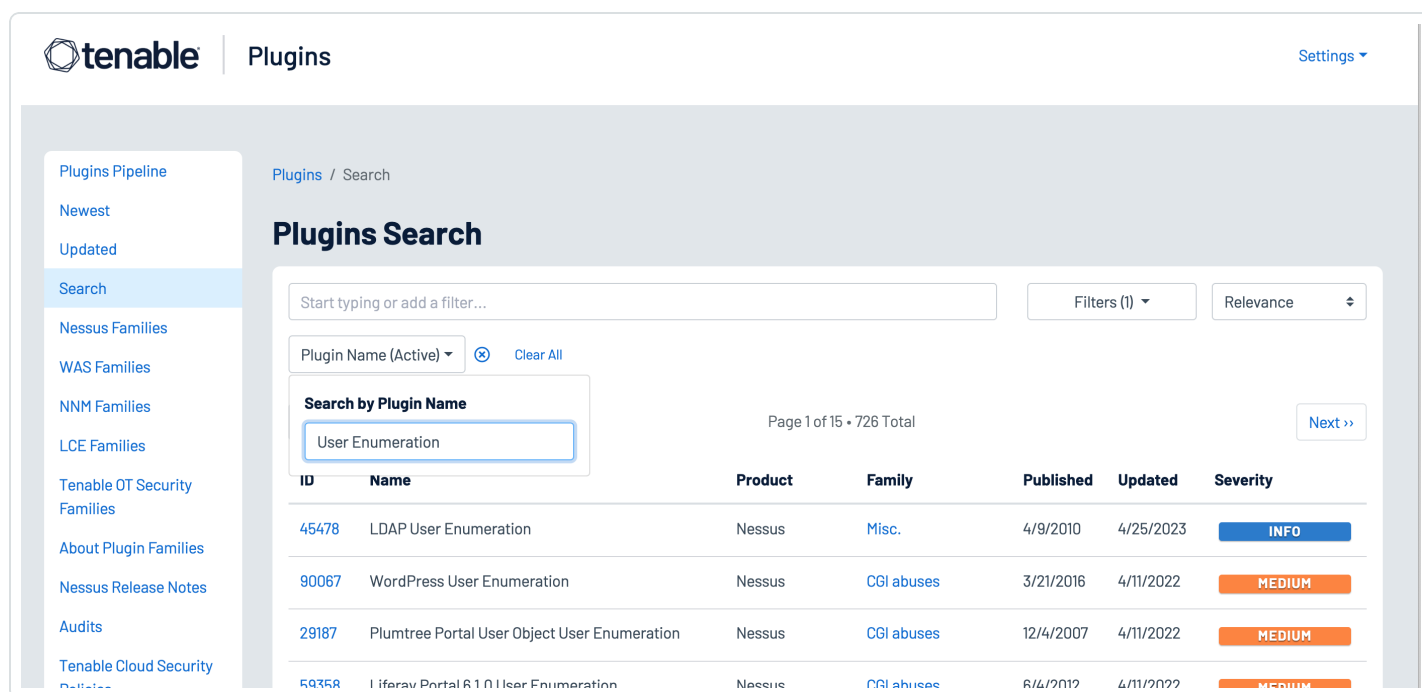
As well as expanding on ECC 2-2-3, the Identity and Access Management control in the OTCC requires the OT/ICS access management lifecycle to be separated and independent from IT. The control further talks about how certain types of accounts should be handled (e.g., service accounts, default accounts, privileged accounts, etc.).

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" can be found in the [Plugin Name](#) search using the Plugin Name filter, identify WordPress, VMware, LDAP, and other software applications that maintain user accounts:



The screenshot displays the Tenable Nessus interface for searching plugins. The search results are as follows:

ID	Name	Product	Family	Published	Updated	Severity
45478	LDAP User Enumeration	Nessus	Misc.	4/9/2010	4/25/2023	INFO
90067	WordPress User Enumeration	Nessus	CGI abuses	3/21/2016	4/11/2022	MEDIUM
29187	Plumtree Portal User Object User Enumeration	Nessus	CGI abuses	12/4/2007	4/11/2022	MEDIUM
59358	Uifera Portal 6.1.0 User Enumeration	Nessus	CGI abuses	6/4/2012	4/11/2022	MEDIUM

Service 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.

The screenshot displays the Tenable Nessus Plugins Search interface. The top navigation bar includes the Tenable logo, the word 'Plugins', and a 'Settings' dropdown. A left sidebar contains navigation links such as 'Plugins Pipeline', 'Newest', 'Updated', 'Search', and various Nessus Families. The main content area is titled 'Plugins Search' and features a search input field with the placeholder 'Start typing or add a filter...'. Below the search field, a filter dropdown is set to 'Enable Default Logins (1)', with a 'Clear All' link. A 'Yes' checkbox is checked under this filter. The search results are displayed as a table with the following data:

ID	Name	Product	Family	Published	Updated	Severity
83266	ClusterLabs Pacemaker PCS Daemon Default Password	Nessus	Misc.	5/7/2015	7/24/2018	CRITICAL
22130	Barracuda Spam Firewall Default Credentials	Nessus	CGI abuses	8/2/2006	4/11/2022	HIGH
34217	Default Password (000000) for 'admin' on WIP5000 IP Phone	Nessus	Misc.	9/16/2008	8/7/2018	CRITICAL
35649	Trend Micro InterScan Web Security Suite Default Credentials	Nessus	CGI abuses	2/12/2009	1/19/2021	HIGH
86148	Persistent Systems Radia Client Automation Agent	Nessus	Windows	9/25/2015	4/11/2022	CRITICAL

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

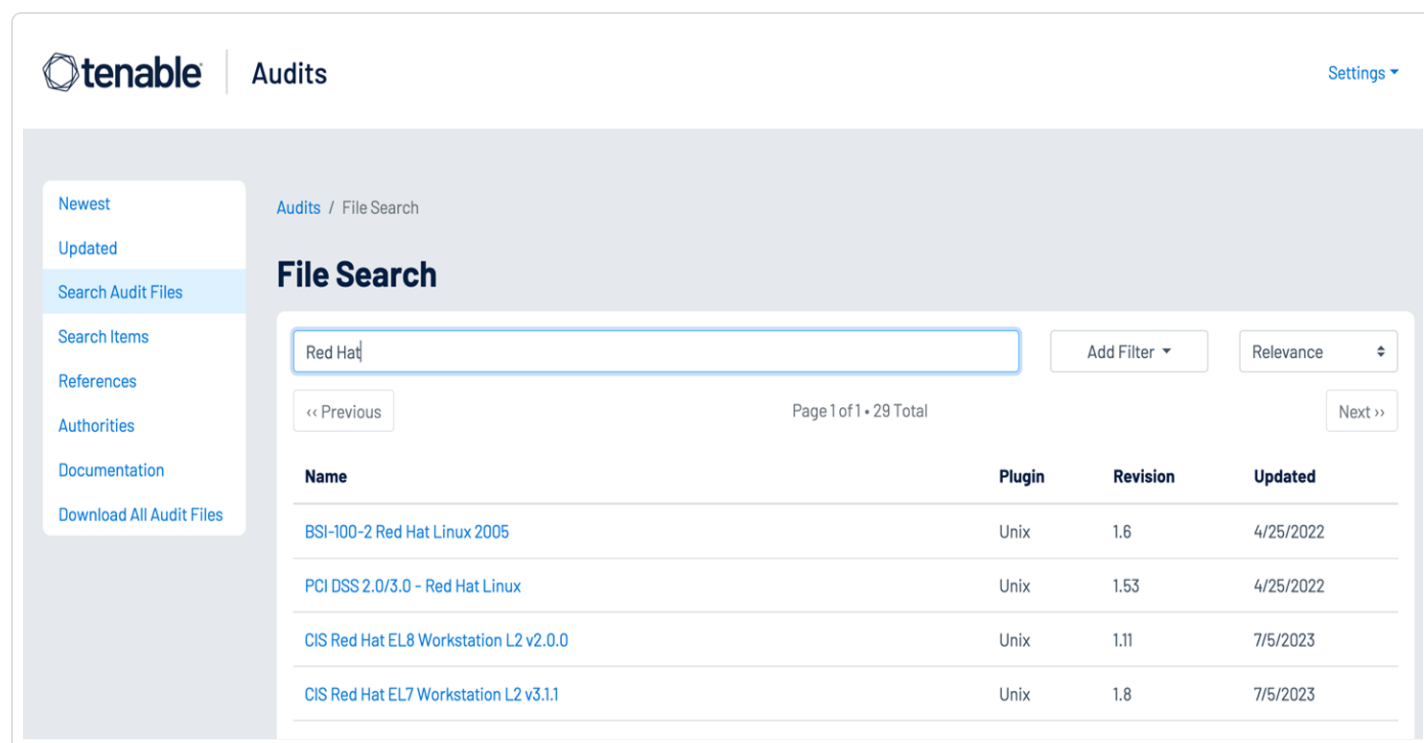
The screenshot displays the Tenable Identity Exposure interface. The top navigation bar includes the Tenable logo and 'Identity Exposure' text. On the right, there are utility icons for help, settings, notifications, and a user profile. The left sidebar is divided into 'GENERAL' (Dashboards), 'SECURITY ANALYTICS' (Trail Flow, Indicators of Exposure, Indicators of Attack, Topology, Attack Path), and 'MANAGEMENT' (Accounts, System). The main content area is titled 'Indicators of Exposure' and shows a table with one entry: 'Unsecured Configuration of Netlogon Protocol'. This entry is marked as 'Critical' and 'Not compliant', with a latest detection of '10:34:34, 2023-10-06'. Below the table, the 'Information' tab is active, showing an 'EXECUTIVE SUMMARY' that describes CVE-2020-1472 ('Zerologon') as a vulnerability allowing an unauthenticated attacker to connect to a domain controller. It also lists 'DOCUMENTS' (CVE-2020-1472 | Netlogon Elevation of Privilege Vulnerability, How to manage the changes in Netlogon secure channel connections associated with CVE-2020-1472, [MS-NRPC]: Netlogon Remote Protocol, [Blog] Zerologon: instantly become domain admin by subverting Netlogon cryptography (CVE-2020-1472)) and 'ATTACKER KNOWN TOOLS' (CVE-2020-1472 POC by Dirk-jan Mollema, Mimikatz - LsaDump Zerologon by Benjamin Delpy).

User Access Controls

Strong authentication mechanisms help validate that accounts are being used by the authorized user to read, create, modify, or delete data in accordance with business needs. The [Center for Internet Security \(CIS\)](#) provides [benchmarks](#) for a large number of Operating System platforms and applications. [Tenable Research](#) writes [audit files](#) for these benchmarks to help organizations quickly determine their alignment with the CIS recommendations. The benchmarks include guidance on access controls for both non-privileged and privileged accounts.

User Accounts

Non-privileged user accounts require strong access controls to prevent attackers from gaining local access to the network. Attackers often target user accounts to exploit weaknesses in the local network and escalate privileges. Security teams can use the [Tenable Audits Search](#) page to find audit files for their Operating System platforms, which check for common compliance requirements such as “Lock Workstations after Inactivity” and other issues.



The screenshot displays the Tenable Audits Search interface. The top navigation bar includes the Tenable logo, the word "Audits", and a "Settings" dropdown. A left sidebar contains navigation links: "Newest", "Updated", "Search Audit Files" (highlighted), "Search Items", "References", "Authorities", "Documentation", and "Download All Audit Files". The main content area is titled "File Search" and shows a search input field containing "Red Hat". Below the search bar, there are navigation buttons for "Previous" and "Next", and a page indicator "Page 1 of 1 • 29 Total". A table of search results is displayed with the following columns: Name, Plugin, Revision, and Updated.

Name	Plugin	Revision	Updated
BSI-100-2 Red Hat Linux 2005	Unix	1.6	4/25/2022
PCI DSS 2.0/3.0 - Red Hat Linux	Unix	1.53	4/25/2022
CIS Red Hat EL8 Workstation L2 v2.0.0	Unix	1.11	7/5/2023
CIS Red Hat EL7 Workstation L2 v3.1.1	Unix	1.8	7/5/2023

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:

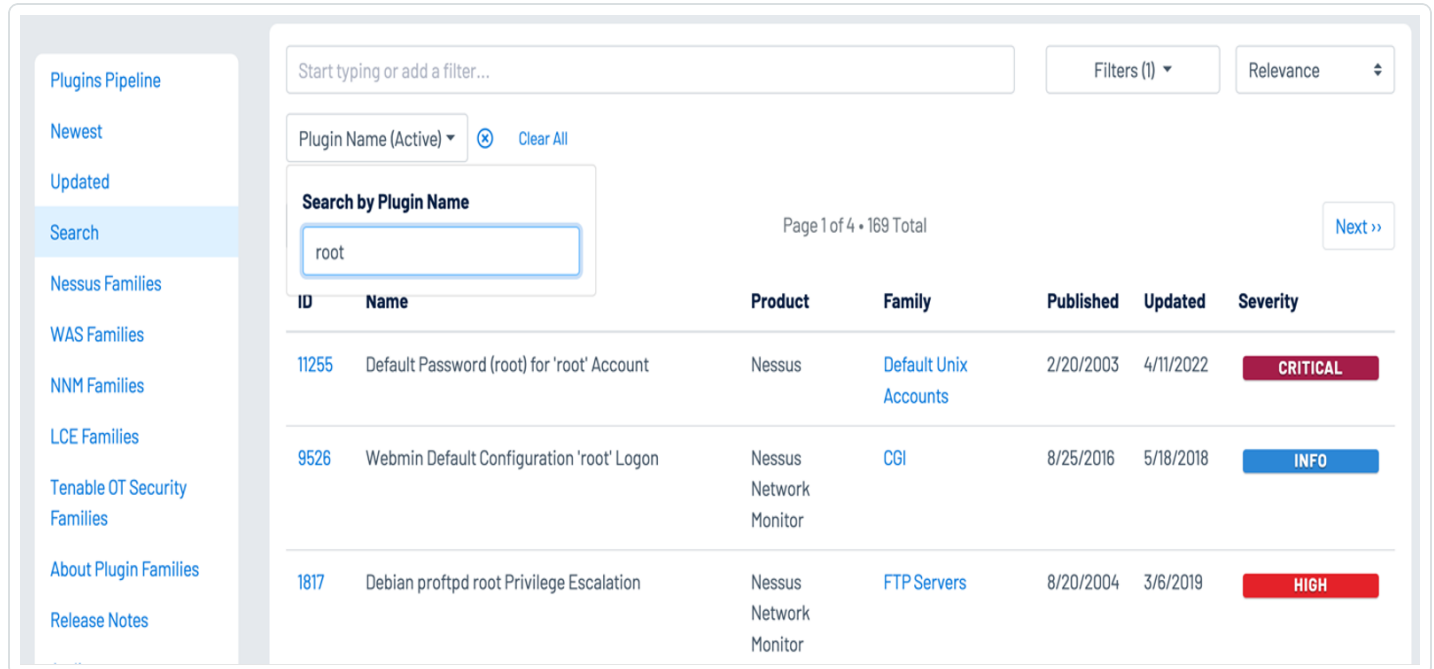
- Accounts with Never Expiring Passwords
- Application of Weak Password Policies on Users
- Dangerous Kerberos Delegation
- Account that Might Have an Empty Password

- 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.”



The screenshot shows the Tenable Nessus Plugins Search interface. On the left is a navigation menu with options like 'Plugins Pipeline', 'Newest', 'Updated', 'Search', 'Nessus Families', 'WAS Families', 'NNM Families', 'LCE Families', 'Tenable OT Security Families', 'About Plugin Families', and 'Release Notes'. The 'Search' option is selected. The main area has a search bar with 'root' entered. Below the search bar, there are filters for 'Plugin Name (Active)' and 'Clear All'. The search results are displayed in a table with columns: ID, Name, Product, Family, Published, Updated, and Severity. The table shows three results:

ID	Name	Product	Family	Published	Updated	Severity
11255	Default Password (root) for 'root' Account	Nessus	Default Unix Accounts	2/20/2003	4/11/2022	CRITICAL
9526	Webmin Default Configuration 'root' Logon	Nessus Network Monitor	CGI	8/25/2016	5/18/2018	INFO
1817	Debian proftpd root Privilege Escalation	Nessus Network Monitor	FTP Servers	8/20/2004	3/6/2019	HIGH

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

Dormant Accounts

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.









The **Active Directory Starter Scan Template** contains 10 hygiene checks that attackers often exploit while seeking to navigate their targets' Active Directory. These plugins focus on the most common attack paths, such as guessing or cracking accounts' secrets, impersonating other users, privilege escalation and lateral across domains.

Select a Template






Scanner Agent

Search 32 Results




















Vulnerability Scans (Common)

 Advanced Network Scan Configure a scan without using any recommendations.	 Basic Network Scan A full system scan suitable for any host.	 Credentialed Patch Audit Authenticate to hosts and enumerate missing updates.	 Host Discovery A simple scan to discover live hosts and open ports.
 Internal PCI Network Scan Perform an internal PCI DSS (11.2.1) vulnerability scan.	 Legacy Web App Scan Scan for published and unknown web vulnerabilities using Nessus Scanner.	 Mobile Device Scan Assess mobile devices via Microsoft Exchange or an MDM.	 PCI Quarterly External Scan Approved for quarterly external scanning as required by PCI.

Configuration Scans

 Audit Cloud Infrastructure Audit the configuration of third-party cloud services.	 MDM Config Audit Audit the configuration of mobile device managers.	 Offline Config Audit Audit the configuration of network devices.	 Policy Compliance Auditing Audit system configurations against a known baseline.
 SCAP and OVAL Auditing Audit systems using SCAP and OVAL definitions.			

Tactical Scans

 2022 Threat Landscape Report (TLR) A scan to detect vulnerabilities featured in our End of Year report.	 Active Directory Identity Use a Domain User account to query AD identity information.	 Active Directory Starter Scan Look for misconfigurations in Active Directory.	 CISA Alerts AA22-011A and AA22-047A Detection of vulnerabilities from recent CISA alerts.
 ContiLeaks Detection of vulnerabilities revealed in the ContiLeaks chats.	 GHOST (glibc) Detection Local checks for CVE-2015-0235.	 Intel AMT Security Bypass Remote and local checks for CVE-2017-5689.	 Log4Shell Detection of Apache Log4j CVE-2021-44228
 Log4Shell Remote Checks Detection of Apache Log4j CVE-2021-44228 via Remote Direct Checks	 Log4Shell Vulnerability Ecosystem Detection of Log4Shell Vulnerabilities	 Malware Scan Scan for malware on Windows and Unix systems.	 PrintNightmare Local checks to detect the PrintNightmare Vulnerability in Windows Print Spooler...
 ProxyLogon : MS Exchange Remote and local checks to detect Exchange vulnerabilities targeted by HAFNIUM.	 Ransomware Ecosystem Vulnerabilities used by ransomware groups and affiliates.	 Ripple20 Remote Scan A remote scan to fingerprint hosts potentially running the Treck stack in the ne...	 Solorigate Remote and local checks to detect SolarWinds Solorigate vulnerabilities.
 Spectre and Meltdown Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754	 WannaCry Ransomware Remote and local checks for MS17-010.	 Zerologon Remote Scan A remote scan to detect Microsoft Netlogon Elevation of Privilege (Zerologon).	

Maintenance

Every structure - physical or virtual - requires maintenance to maintain structural integrity over time. Even the most hardened infrastructure is subject to degradation with regular use. Tenable Security Center, Tenable Vulnerability Management, and Tenable Identity Exposure provide comprehensive monitoring to detect drift from the desired state.

Administrator and user activity can degrade security controls over time if the system is not maintained properly. Regular scanning of the environment using the Nessus audit files identifies drift in security controls.

The following [Indicators of Exposure](#) (IoE) in Tenable Identity Exposure can be used to identify maintenance issues in Active Directory:

- Computers Running an Obsolete OS (High)
- Disabled Accounts in Privileged Groups (Low)
- Unlinked, Disabled, or Orphan GPO (Low)

Step 1: From the **Indicators of Exposure** tab in Identity Management, search for the above listed IoEs in the search field:



Step 2: Click on one of the displayed tiles to drill down into more details:

The screenshot shows the Tenable Identity Exposure web interface. The top navigation bar includes the Tenable logo and the text 'Identity Exposure'. On the right side of the header, there are icons for help, settings, notifications, and a user profile. Below the header, the main content area is titled 'Indicators of Exposure' and 'Indicator details'. A search bar on the left contains the text 'Obsole'. The main indicator is 'Computers Running an Obsolete OS', which has a severity of 'High' and a status of 'Not compliant'. The latest detection time is '15:45:14, 2023-04-17'. The interface is divided into several sections: 'EXECUTIVE SUMMARY' with a description of OS support periods, 'DOCUMENTS' with a list of links to support articles, and 'ATTACKER KNOWN TOOLS' which is currently empty.

Using the Indicators of Exposure within Tenable Identity Exposure assists the organization in reviewing user access rights; something that must be done periodically (ECC 2-2-3-5) and in response to cybersecurity incidents, personnel roles changes or whenever there is a change in OT/ICS system architecture (OTCC 2-2-1-10).

For organizations where an on-premises solution is required Tenable Security Center is able to provide coverage along with an on-premises installation of Tenable Identity Exposure. An installation guide for Tenable Identity Exposure can be seen [here](#). Utilizing the Getting Started with AD Security dashboard (see figure 9), Tenable Security Center unifies security data from across the organization, providing a comprehensive view and understanding of the organization's overall security posture. Using a diverse deployment of Nessus scanners, administrators have complete visibility into network-connected assets with comprehensive vulnerability assessment coverage. When Active Directory concerns are identified, Tenable Security Center quickly provides alerts via workflows and notifications, which speed up incident response and vulnerability remediation. Additionally, Tenable.ad provides a comprehensive cyber exposure determination of Active Directory hosts.

2-9: Vulnerabilities Management

The objective for domain 2-9, The National Cybersecurity Authority states:

“To ensure timely detection and effective remediation of technical vulnerabilities to prevent or minimize the probability of exploiting these vulnerabilities to launch cyber-attacks against the organization.”

Understanding Cyber Exposure requires that the data collected by Tenable Vulnerability Management is trusted and verifiable. Tenable Vulnerability Management and Tenable Security Center provide several plugins that assist in determining scan status and provides a level of trust for risk managers. The **Authentication Summary** Tenable Security Center dashboard provides a clear and simplified method to track and troubleshoot authentication-related problems. The dashboard groups authentication plugins into diagnostic contexts to show administrators areas of concern to focus on.

tenable Security Center | Dashboards Vulnerabilities Search By CVE ? VT

Authentication Summary Refresh All Switch Dashboard Options

Authentication Summary - Authentication Plugin Indicator

Auth/Local Checks Issues	Authentication Status
Detected	Don't Scan Devices
Local Auth Recon	Local Checks Status
OS Identification	Port Re-check
Third-party Local Checks	Windows Access Checks
Errors in nessus.dump	

Last Updated: Less than a minute ago

Authentication Summary - Windows Access Checks

	Host Detected	Percentage of Detected Systems
Patch Bulletin Feasibility	0	0%
Installed Hotfixes	0	0%
Registry Remotely Accessible	0	0%
Registry Not Fully Accessible	0	0%

Last Updated: Less than a minute ago

Authentication Summary - Local Authentication Ratio

	Host Detected	Percentage of Detected Systems
Windows SMB Log In Possible	0	0%
SSH OS & Software Enum	0	0%
SNMP Authentication	0	0%
VMware vSphere Installed	0	0%
PAN-OS Version Detection	0	0%
Citrix NetScaler Detection	0	0%

Last Updated: 1 minute ago

Authentication Summary - Nessus Scan Summary Credentialed Summary

	Credentialed Account Percen...	Total Count per Credentials	Total Credential Scans
Credentials with Admin	-	0	0
Credentials with root	-	0	0
Credentials with Other	-	0	0
Credentials No User	-	0	0
Credentials Using SMB	-	0	0
Credentials Using SSH	-	0	0
Credentials Using SOAP	-	0	0
Credentials Undefined	-	0	0
Credentialed Checks No	100%	3	N/A

Last Updated: Less than a minute ago

Authentication Summary - Summarize local checks status

	Host Detected	Percentage of Detected Systems
Local Checks Enabled	0	0%
Local Checks Not Available	0	0%
Require Privilege Escalation	0	0%
Local Checks Not Enabled	0	0%
Local Checks Not Run	3	100%

Last Updated: Less than a minute ago

Authentication Summary - Summarize Authentication Status

	Host Detected	Percentage of Detected Systems
Authentication Success	0	0%
Insufficient Access	0	0%
Intermittent Failure	0	0%
Failure with Credentials	3	100%
No Credentials Provided	0	0%

Last Updated: Less than a minute ago

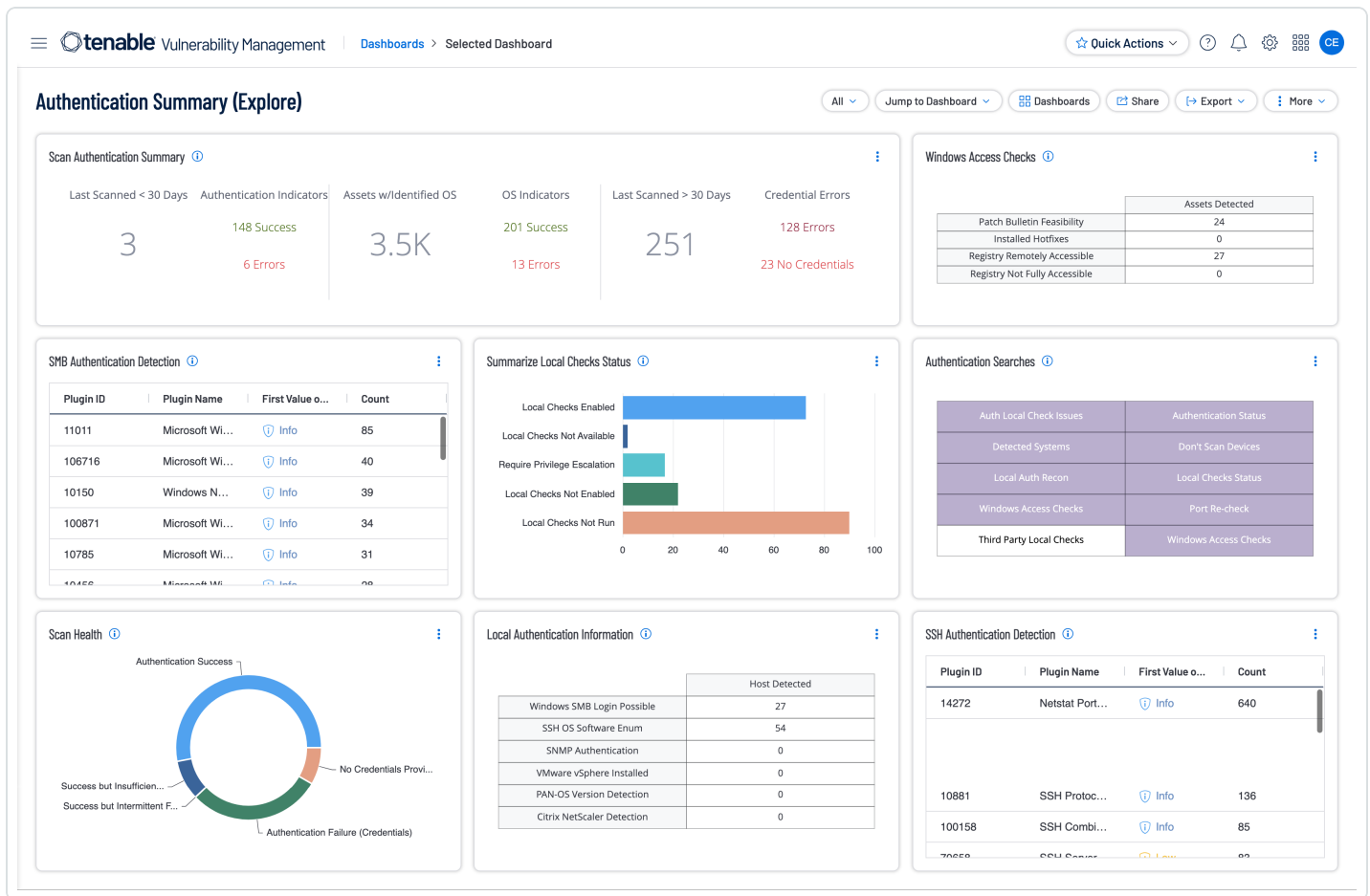
Authentication Summary - SMB Authentication Detection

Last Updated: Less than a minute ago [View Data](#)

Authentication Summary - SSH Authentication Detection

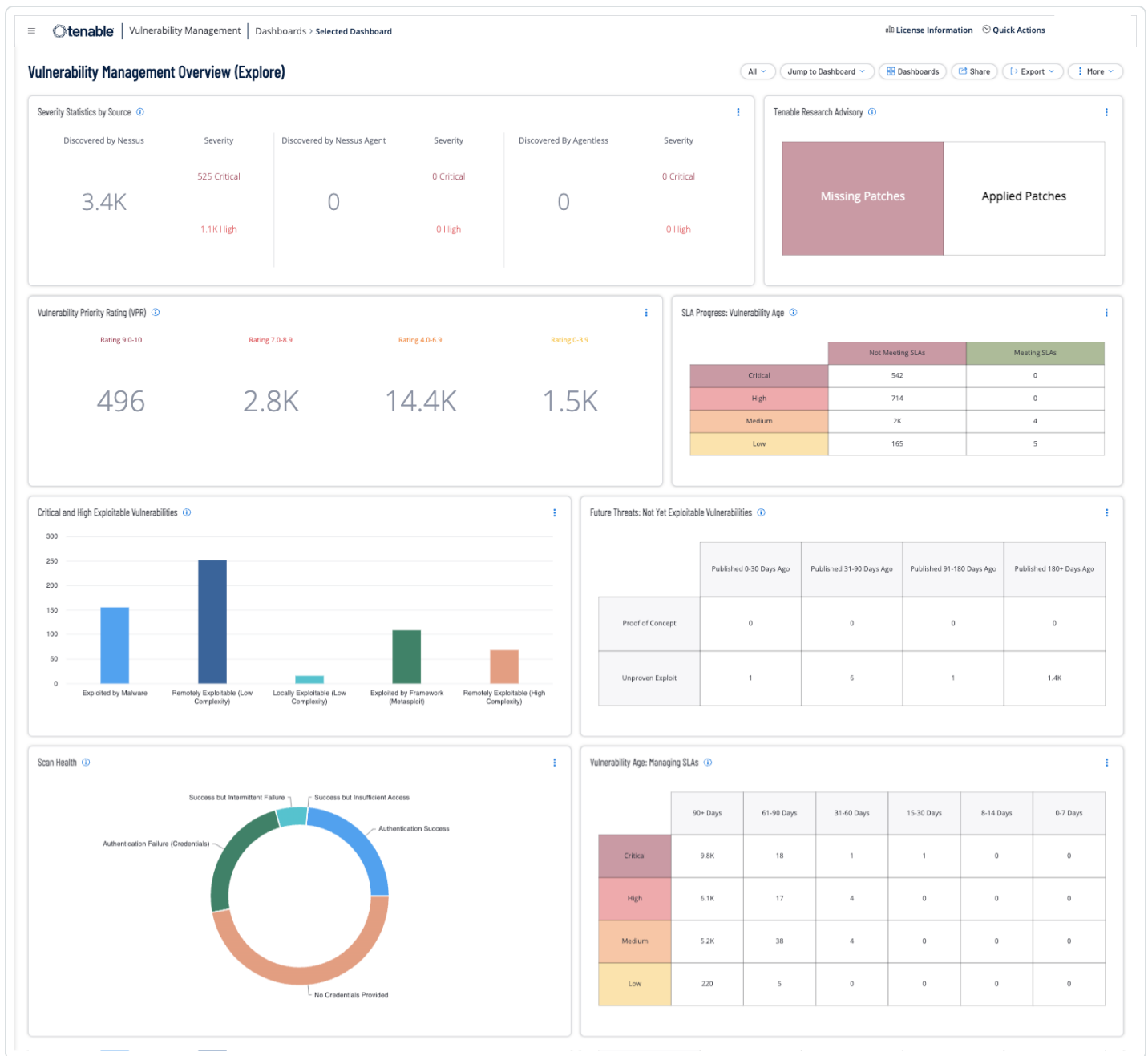
Last Updated: Less than a minute ago [View Data](#)

The **Authentication Summary (Explore)** Tenable Vulnerability Management dashboard brings together all the plugins used to verify successful authentication of assets during vulnerability scans, providing security administrators visibility into areas of concern so that the appropriate actions can be taken.



Local checks are required to ensure that scans are complete and accurate. Users enable local checks by providing credentials with elevated privileges, or administrative access, or by deploying Nessus Agents. Tenable Vulnerability Management requires privileged access to provide a comprehensive assessment of risk on an asset. The more access to a system Tenable Vulnerability Management has, the more complete the vulnerability detection.

The Vulnerability Management Overview Tenable Vulnerability Management dashboard provides executive management a summary of risk information at a glance, while enabling security analysts to drill down into technical details by clicking on the widgets.



The widgets in this dashboard provide detailed information on vulnerability severity and mitigation status. Information is provided to help Risk Managers determine compliance with Service Level Agreements. Security Analysts can use the information in the Scan Health widget to determine if scans are running as intended to ensure the accuracy of scan data. Executive Management and Security Analysts can leverage the information provided in this dashboard to ensure their vulnerability management program aligns with organizational goals.

Organizations cannot begin to fix systemic problems within their security program without first being able to analyze the data collected by the vulnerability scanning tool. OTCC 2-9 requires the

monitoring of vulnerabilities and identification of OT/ICS unsupported software. Tenable Security Center uses active and passive detection methods to bring continuous visibility and provide prioritization actions based on business risk and asset discovery.

As networks converge between Information Technology (IT) and Operational Technology (OT), organizations struggle to have complete visibility of the network. Using Tenable OT Security and Tenable Vulnerability Management or Tenable Security Center together, the complete picture of a network is visible to risk managers and CISOs. Both Tenable Vulnerability Management and Tenable Security Center are able to connect with Tenable OT Security and incorporate risk scores such as VPR and Common Vulnerability Scoring System (CVSS) vectors to fully understand risk.

Tenable Security Center has a dashboard called **Getting Started with Tenable OT Security**:

Getting Started with Tenable OT Security

Tenable OT Security - Operational Risk Rating

0-19.9	20-39.9
40-59.9	60-79.9
80-99.9	100

Last Updated: 19 hours ago

Tenable OT Security - Asset by Device Type

Communications...	General Purpose...	Generic Device...
HMI	PLC	Other Device Ty...

Last Updated: 19 hours ago

Tenable OT Security - Asset by Information Technology Device Type

	System Count	Percentage of O...
Access Point (Ac...	0	0%
IP Phone (IpPho...	0	0%
Network Device...	0	0%
Server (PoType)	0	0%
Printers (Printe...	0	0%
Storage (Storag...	0	0%
Unknown Device...	0	0%
UPS (UpsType)	0	0%
Workstations (W...	0	0%

Last Updated: 19 hours ago

Tenable OT Security - Assets by Operational Technology Device Type

	System Count	Percentage of O...
Communication...	0	0%
Engineering (Eng...	0	0%
Field Device (Fi...	0	0%
HMIs (HmiType)	0	0%
OT Servers (IcsS...	0	0%
ICS (IcsType)	0	0%
IO (IoType)	0	0%
Controllers (Pic...	0	0%
Power Supply (P...	0	0%

Last Updated: 19 hours ago

Tenable OT Security - Subnets with Linux OS



Last Updated: 19 hours ago

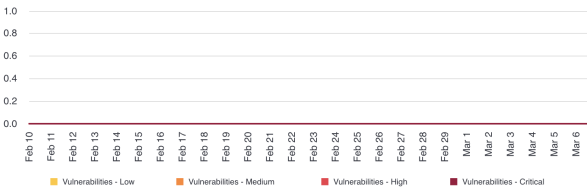
[View Data](#)

VPR Summary - Prioritization Analysis (Operational Technology)

	Low (VPR 0.0-3.9)	Medium (VPR 4.0-6.9)	High (VPR 7.0-8.9)	Critical (VPR 9.0-10)
CVSSv3 Low (0-3.9)	0	0	0	0
CVSSv3 Medium (4.0-...	0	0	0	0
CVSSv3 High (7.0 - 8.9)	0	0	0	0
CVSSv3 Critical (9.0 - ...	0	0	0	0

Last Updated: 19 hours ago

Tenable OT Security - Vulnerabilities over 25 Days



Last Updated: 19 hours ago

Tenable OT Security - Vulnerabilities by CPE Type

Application Vulns	Hardware Vulns	Operating System Vulns
-------------------	----------------	------------------------

Last Updated: 19 hours ago

Tenable OT Security - Vulnerabilities by CPE Vendor

ABB	Emerson	GE
Honeywell	Mitsubishi Electric	Omron
Rockwell	Schneider Electric	Selinc
Siemens	Wago	Yokogawa

Last Updated: 19 hours ago

Tenable OT Security - Asset Information Summary

0 Item(s) | 0 to 0 of 0 << < Page 1 of 1 > >>

Plugin ID	Name ^	Total
-----------	--------	-------

No data was found

Last Updated: 19 hours ago

[View Data](#)

Tenable OT Security - Asset by Criticality Rating

HighCriticality	MediumCriticality
LowCriticality	None/Not Defined

Last Updated: 19 hours ago

Tenable OT Security - Asset by Run Status

Running	Stopped
Fault	Backup
Other Status	Status Not Defined

Last Updated: 19 hours ago

Tenable OT Security - Assets First Seen (2019)

Q1	2019-01	2019-02	2019-03
Q2	2019-04	2019-05	2019-06
Q3	2019-07	2019-08	2019-09
Q4	2019-10	2019-11	2019-12

Last Updated: 19 hours ago

Tenable OT Security - Assets Last Seen (2019)

Q1	2019-01	2019-02	2019-03
Q2	2019-04	2019-05	2019-06
Q3	2019-07	2019-08	2019-09
Q4	2019-10	2019-11	2019-12

Last Updated: 19 hours ago

Tenable OT Security - Assets First Seen (2020)

Q1	2020-01	2020-02	2020-03
Q2	2020-04	2020-05	2020-06
Q3	2020-07	2020-08	2020-09
Q4	2020-10	2020-11	2020-12

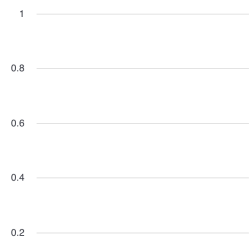
Last Updated: 19 hours ago

Tenable OT Security - Assets Last Seen (2020)

Q1	2020-01	2020-02	2020-03
Q2	2020-04	2020-05	2020-06
Q3	2020-07	2020-08	2020-09
Q4	2020-10	2020-11	2020-12

Last Updated: 19 hours ago

Tenable OT Security - Subnets with Windows OS

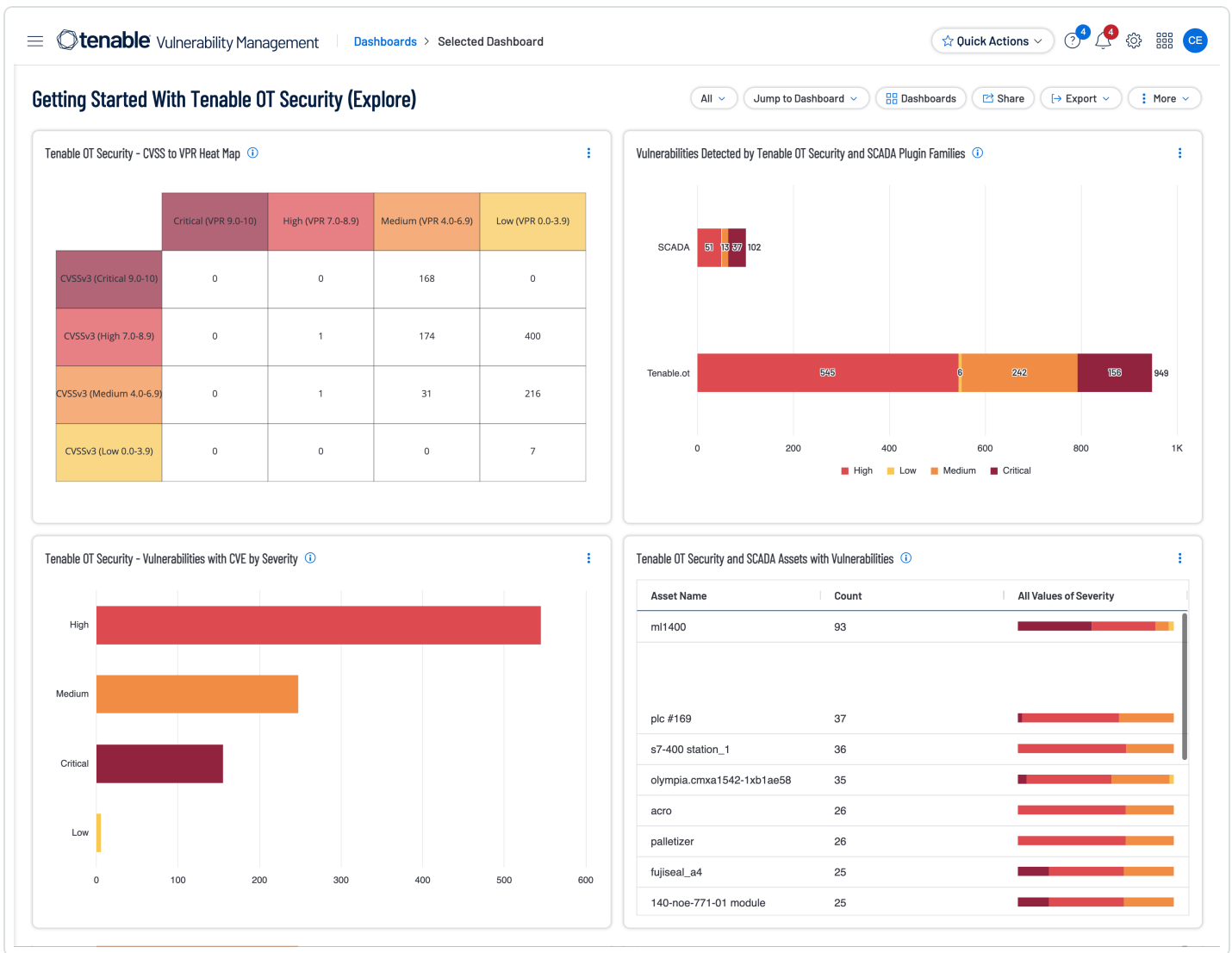


In the first row of components, the dashboard provides the added value of combining the two systems together. By showing the correlation of the Risk Ratings, CVSS, VPR, and criticality ratings, the risk managers are able to gain a clear understanding of the overall IT/OT risk.

On the left side of the dashboard there are two components that show the percentage of systems with respect to IT and OT asset classification type. Each component has a column for the system count and overall percentage. The components in the middle of the center column use the Common Platform Enumeration (CPE) detections. This attribute is part of the vulnerability plugin and can denote hardware, applications, or operating system vulnerabilities. In addition, the CPE contains manufacture information.

System managers can use this information as a starting point for vulnerability analysis and patch management efforts. In the right-hand column, there are four components that track when an asset is first discovered on the network and when last seen. These two attributes help asset managers track when new systems are detected and if the system is in current use. The bottom components use the Asset Identification plugins to show a summary of the device types detected, and the operating systems used.

Organizations are afforded the opportunity to perform risk analysis based on OT and IT data in a single unified platform with Tenable OT Security and either Tenable Vulnerability Management or Tenable Security Center. In the top row of The **Getting Started with Tenable OT Security** dashboard in Tenable Vulnerability Management, the CISO is able to quickly see the status of OT assets by the total number of assets detected, critical, and high severity vulnerabilities, and the criticality rating and run status. The criticality rating is established by default per the device type; however, this rating can be modified as needed.



As the role of the risk manager expands to include OT devices, the next row of widgets presents the data in a more vulnerability management-based view. The ring chart shows the most common vulnerabilities based on the total count of affected assets, and the matrix shows a heat map view aligning CVSS and VPR. By viewing the correlation of the Risk Ratings, CVSS, VPR, and criticality rating, risk managers are able to gain clear understanding of their overall IT/OT risk.

The Cyber Exposure Lifecycle begins with the Discovery phase, where the objective is to map and identify assets across the organization. The next two rows provide counts and summary lists of assets by discovery classifications, such as the Purdue Levels, Device Type, OT Type, and IT Type.

2-10: Penetration Testing

The objective for domain 2-10, The National Cybersecurity Authority states:

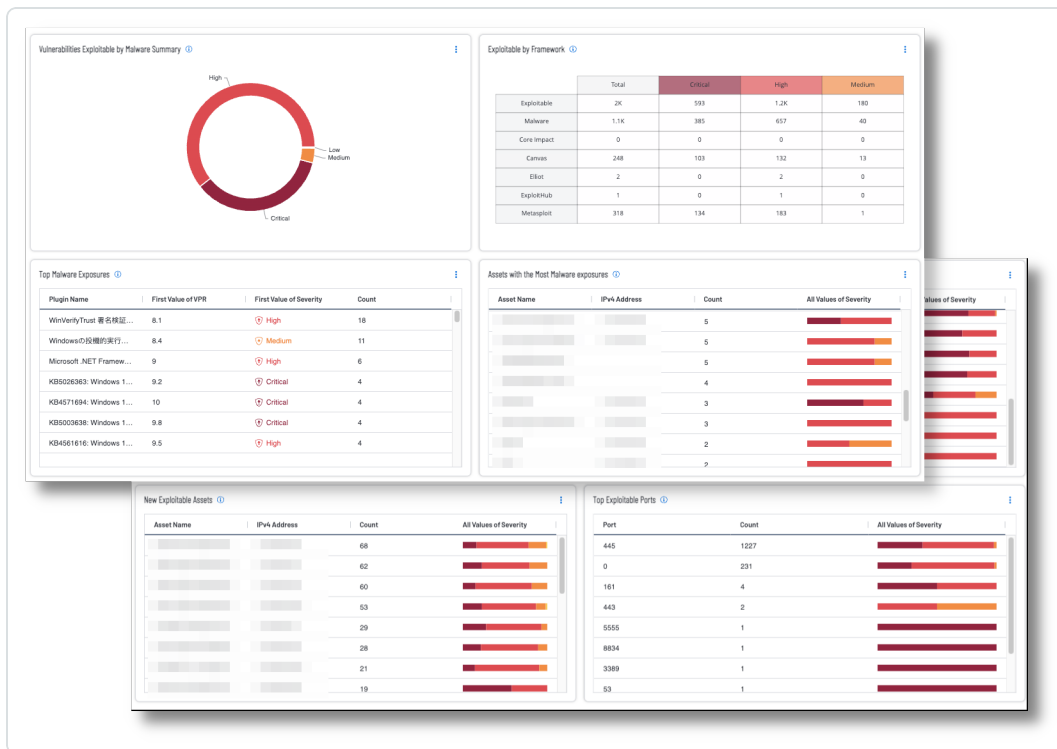
“To assess and evaluate the efficiency of the organization’s cybersecurity defense capabilities through simulated cyber-attacks to discover unknown weaknesses within the technical infrastructure that may lead to a cyber-breach.”

Having effective penetration testing can be crucial to discover weaknesses that may have passed undetected. Tenable allows an organization to identify exploitable vulnerabilities and assists a penetration testing team to effectively plan simulated cyber-attacks that discover unknown weaknesses within the technical infrastructure that may lead to a cyber-breach.

Exploits leveraged in attacks are imported into various tools and services when the attack is made public. Common exploit frameworks are easy to obtain and are used by both security researchers and malicious attackers. Security analysts can effectively reduce risk to the organization by analyzing an exploit's source tool and the most common targets. Tenable Vulnerability Management provides security operations teams a centralized view of common vulnerabilities and exploit frameworks present in the organization’s environment.

Many organizations conduct internal red team (offense) and blue team (defense) exercises to gain insight into their exposures to attackers and their ability to defend against attacks. These exercises are a great way to harden the infrastructure before an official audit or malicious attack occurs. Having detailed information about exposures in the infrastructure before commencing such exercises enables red and blue teams to more effectively uncover exposures that a sophisticated auditor or attacker would find. While exploit frameworks are a great start, they are simply tools that are only as effective as the skill of the person using the frameworks.

Using the **Pen Testing Team: One-Stop-Shop Tenable Vulnerability Management dashboard** to drill down into the Explore Findings view displays other attributes such as CPE, VPR Key Drivers, and CVSS Vectors. Each of these filters helps red and blue teams to narrow their focus and discover risks that may require prioritization over other vulnerabilities.



Vulnerabilities can also be widely exploited shortly after publication as malware authors reverse engineer the fix and develop '1-day exploits' that can be used to attack organizations. Tenable Vulnerability Management easily identifies assets most vulnerable to malware and other exploitation frameworks. This dashboard provides the necessary context to understand which assets are vulnerable to malware exploitation. Organizations can better communicate cyber risk to the business by supplying context and associated metrics.

2-12: Cybersecurity Incident and Threat Management

The objective for domain 2-12, The National Cybersecurity Authority states:

“To ensure timely identification, detection, effective management, and handling of cybersecurity incidents and threats to prevent or minimize negative impacts on an organization’s OT/ICS operation.”

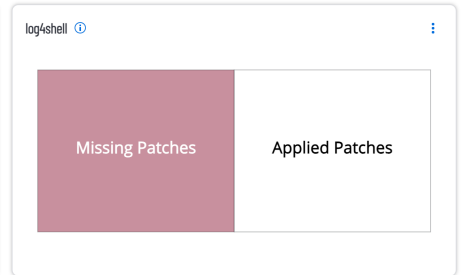
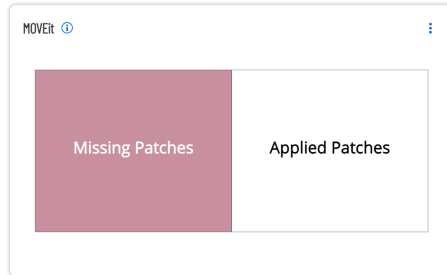
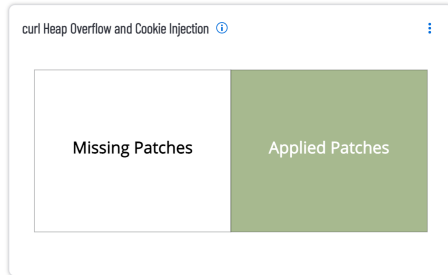
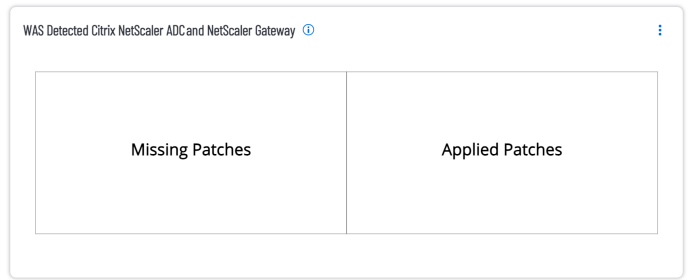
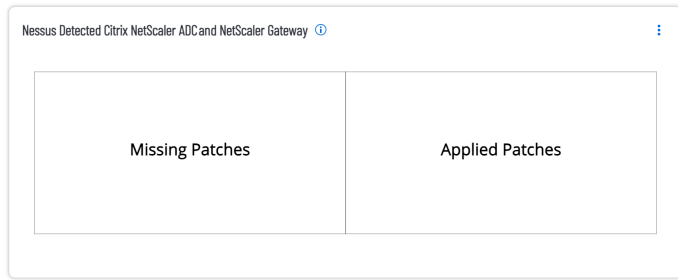
Tenable Research delivers world-class exposure intelligence, data science insights, zero-day research, and security advisories. Our Security Response Team (SRT) in Tenable Research tracks threat and vulnerability intelligence feeds to make sure our research teams can deliver sensor coverage to our products as quickly as possible. The SRT also works to dig into technical details and author whitepapers, blogs, and additional communications to ensure stakeholders are fully informed of the latest cyber risks and threats. The SRT provides breakdowns for the latest critical vulnerabilities on the Tenable blog.

When security events rise to the level of taking immediate action, Tenable - leveraging SRT intelligence - notifies customers proactively to provide exposure information, current threat details and how to use Tenable products and capabilities to accelerate remediation.

The **Tenable Research Advisories: Urgent Action** dashboards in Tenable Vulnerability Management and Tenable Security Center contain indicator style widgets to highlight any vulnerabilities related to the Tenable Research Advisories. Here, Tenable issues customer guidance that immediate remediation is of paramount importance to all affected organizations. Tenable recommends addressing missing patches as identified in the dashboard components.

Tenable Research Advisories: Urgent Action (Explore)

All Jump to Dashboard Dashboards Share Export More



Tenable Research Advisories: Urgent Action

Refresh All

Switch Dashboard

Options

Research Advisories - Nessus
Detected Citrix NetScaler ADC and NetScaler Gateway

Missing Patches Applied Patches

Last Updated: Less than a minute ago

Research Advisories - WAS
Detected Citrix NetScaler ADC and NetScaler Gateway

Missing Patches Applied Patches

Last Updated: Less than a minute ago

Research Advisories - curl Heap Overflow and Cookie Injection

Missing Patches Applied Patches

Last Updated: 17 hours ago

Research Advisories - MOVEit

MISSING PATCHES Applied Patches

Last Updated: 17 hours ago

Research Advisories - log4shell

Missing Patches Applied Patches

Last Updated: 17 hours ago

Research Advisories - PrintNightmare

Missing Patches Applied Patches

Last Updated: 17 hours ago

Research Advisories - MS Exchange ProxyLogon

MISSING PATCHES Applied Patches

Last Updated: 17 hours ago

Research Advisories - CISA Alerts AA22-011A and AA22-047A

Missing Patches Applied Patches

Last Updated: 17 hours ago

Learn More

Tenable Resources

- [InfoSec Team - One-Stop Shop Comprehensive Attack Surface](#)
- [Vulnerability Management Program Health](#)
- [Asset Inventory and Detection \(SEE\) \(Tenable Vulnerability Management\)](#)
- [Asset Inventory and Detection \(SEE\) \(Tenable Security Center\)](#)
- [Asset Management Overview](#)
- [Getting Started with Active Directory \(Tenable Vulnerability Management\)](#)
- [Getting Started with Active Directory \(Tenable Security Center\)](#)
- [Authentication Summary \(Tenable Vulnerability Management\)](#)
- [Authentication Summary \(Tenable Security Center\)](#)
- [Vulnerability Management Overview](#)
- [Getting Started with Tenable.ot \(Tenable Vulnerability Management\)](#)
- [Getting Started with Tenable.ot \(Tenable Security Center\)](#)
- [Pen Testing Team: One-Stop-Shop](#)
- [Tenable Research Advisories: Urgent Action \(Tenable Vulnerability Management\)](#)
- [Tenable Research Advisories: Urgent Action \(Tenable Security Center\)](#)

Compliance References

- [NCA - Operational Technology Cybersecurity Controls \(OTCC\)](#)
- [NCA - Essential Cybersecurity Controls \(ECC\)](#)
- [CIS Critical Security Control 7 - Continuous Vulnerability Management](#)