Tenable Cyber Exposure Study — NIS 2 Directive

Last Revised: July 17, 2025

Table of Contents

NIS 2 Directive

In an effort to elevate the cybersecurity resilience of European Union (EU) member states, the Directive on the security of Network and Information Systems (NIS) was established in 2016 and revised in 2023 (NIS 2). NIS 2 fosters cross-border collaboration to enhance information flow on incidents, threats, and vulnerabilities. This initiative complements existing EU regulations, such as the General Data Protection Regulation (GDPR), Cybersecurity Act, Digital Operational Resilience Act (DORA), and the Cyber Resilience Act.

As the threat landscape changes, so should organisations, to better identify and mitigate emerging threats. The evolution from NIS to NIS 2 is aimed to bolster the EU's resilience to cyber threats. The EU introduced the NIS 2 Directive in December 2022, addressing previous issues and to fortify cybersecurity. NIS 2 broadens the scope, introduces more robust incident reporting, introduces potential sanctions, mandates training and emphasises use of encryption.

Overall, the scope of the original NIS remains intact, and NIS 2 adds eight new sectors, and simplifies identification with a new size-cap rule encompassing Essential and Important Entities. Keep in mind that under NIS 2 organisations fall into the scope of being Essential Entities with over 250 employees and an annual turnover above 50 million EUR, or a balance sheet over 43 million EUR. Alternatively, Important Entities have over 50 employees and an annual turnover or balance sheet above 10 million EUR.

EU member states must implement the NIS 2 Directive by **October 17, 2024**. Organisations within the scope must comply by October 18, 2024. Early preparation is essential to meet obligations promptly. Non-compliance may result in administrative fines, temporary management suspension, and reputational damage.

If you have identified that your organisation is within the scope of the NIS 2 Directive you should review and audit your vulnerability management program. Organisations within scope must adhere to Chapter IV, Article 21 of the NIS 2 Directive for cybersecurity risk management and reporting obligations. It underscores a systematic, risk-based approach to minimise cyber incidents and outlines essential security measures all organisations must implement to safeguard their network and information systems.

This Cyber Exposure Study provides guidance on leveraging Tenable products in support of NIS 2 Article 21, Cybersecurity Risk-Management Measures. Tenable provides the ability to comprehensively conduct risk management & reporting activities required by NIS 2.

The NIS 2 measures supported by Tenable are:

- Article 21(2)(a): Risk Analysis and Information System Security: Cyber Risk-Based Approach.
- Article 21(2)(b): Incident Handling: Incident Management and Reporting
- Article 21(2)(c): Business Continuity: Business Continuity Process and Technology
- Article 21(2)(d): Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers.
- Article 21(2)(e): Network and Information Systems Security, including Vulnerability Handling and Disclosure: Preventative Network and Information Vulnerability Management
- Article 21(2)(f): Policies and Procedures for Testing Cybersecurity Risk Management Measures: Policy Definition and Testing
- Article 21(2)(g): Basic Cyber Hygiene Practices and Cybersecurity Training: Cyber Hygiene
- Article 21(2)(h): Policies and procedures regarding the use of cryptography, and where appropriate encryption
- Article 21(2)(i): Access Control Policies and Asset Management: Asset Discovery and Access Control
- Article 21(2)(j): Use of Multi-Factor Authentication or Continuous Authentication Solutions: MFA

Getting Started

Develop a thorough analysis of whether or not your organisation is within the scope of the NIS 2 Directive. After this is done, you should follow the national discussion regarding the NIS 2 Directive to get a better picture of how it will be implemented into your national law.

If you have identified that your organisation is within the scope of the NIS 2 Directive, you should review and audit your vulnerability management program. Risk-based vulnerability management is a proactive approach to cybersecurity that considers the likelihood of a vulnerability being exploited and the potential impact of events when deciding which vulnerabilities to remediate.

Risk-based vulnerability management also includes detailed documentation and reporting of identified vulnerabilities, their associated risks, and the steps taken to address them. This information is critical for the incident reporting requirements of NIS 2.

As the deadline for transposing the NIS 2 Directive into national law approaches on October 17, 2024, organisations falling under its purview must proactively prepare for compliance. Unlike EU regulations, NIS 2, being a directive, is not directly binding, but sets a minimum standard. However, when your country implements national regulation attached to NIS 2, your organisation must take steps to be compliant to local law. Each country creates their own regulations attached to NIS 2 and these vary from country to country.

Following these five crucial steps to navigate the complexities and ensure a smooth transition:

1. Involve your top management. The success of any compliance initiative relies on the backing of your organisation's leaders.

2. Understand the Scope. Figuring out the scope of NIS 2, your systems that fall under this scope, and the challenges in achieving compliance are the first steps to achieving NIS 2 compliance.

3. Study the NIS 2 security requirements. Familiarise yourself with Article 21 of the Directive, outlining the main NIS 2 requirements. Ensure your organisation addresses the ten security measures mandated by NIS 2, ranging from risk analysis to multi-factor authentication. These 10 requirements are covered in depth within this document.

4. Conduct gap analysis. Once you've identified the scope and requirements of NIS 2, you're ready to compare them to the existing security measures implemented in your organisation. Gap analysis bridges any existing gaps between the current state of compliance and the desired one.

5. Allocate the necessary resources. Successful implementation of the NIS 2 Directive requirements involves allocating the resources needed, including money, people, and technology.

How Tenable Helps

While the above steps can help you begin to navigate the complexities that this new directive brings, an effective exposure management program helps organisations gain visibility across the modern attack surface, focuses efforts to prevent likely attacks, and accurately communicates cyber risk, supporting optimal business performance.

Tenable products provide useful detection and collection tools that identify and inventory the network, identify the attack surface, and provide the ability to communicate the findings to executive leadership and operation teams on a single platform. As assets on the network are inventoried, the exposure management team is able to gain visibility across the network and clearly identify the modern attack surface. Allowing the asset owners and support teams to focus efforts to prevent the most likely attacks, and accurately communicate cyber risk to executive leadership.

This study covers the methods used by Tenable products to support and guide customers in the following areas:

1. **Vulnerability Management:** Tenable's solutions help organisations identify and address vulnerabilities in their network and information systems. This is crucial for complying with NIS 2, which requires organisations to implement measures to manage and mitigate cyber risks.
2. **Risk Assessment:** Conducting risk assessments and evaluating the effectiveness of their cybersecurity risk management measures.
3. **Continuous Monitoring:** Leveraging different scanner capabilities to continuously network and supporting systems, and provide information needed for an effective incident response initiative.
4. **Incident Detection and Response:** The data collected from is often leveraged as evidence of malicious activity or as timeline artefacts used during the incident response investigation. Additionally by identifying the attack surface, customers are able to establish risk mitigation strategies and avoid incents all together.
5. **Compliance and Reporting:** The reporting and analysis tools provide organisations the ability to demonstrate compliance with various cybersecurity regulations.
6. **Security Hygiene Practices:** The ability to quickly identify the state of the organisation cyber hygiene is crucial in establishing and maintaining the NIS 2 certification.

7. **Identity and Access Control:** The framework to ensure that the right users have the appropriate access to the organisation's resources.

This document also assists organisations to map NIS 2 to other standards, specifically, ISA IEC 62443, ISO 27001, and NIST CSF by presenting corresponding cross-reference information. This document provides readers with a set of key points in each topic area. The following mapping serves as guidance:

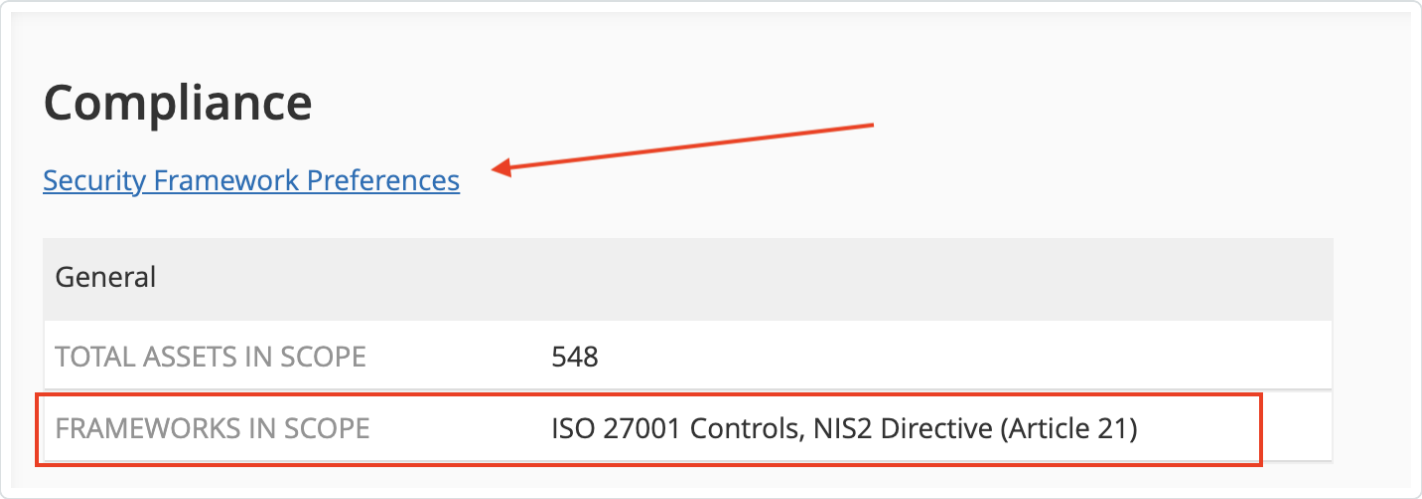
Many organisations already comply with ISO 27001. The ISO 27001 is an international standard and widely used across the world. The standard was also referred to in the ENISA official guidelines. While the concepts change with NIS 2, the recommended information security standards and control frameworks will likely not change dramatically. For this reason, this guide includes specific cross-reference information between the NIS 2 articles and ISO 27001, NIST CSF, and ISA/IEC 62443.

The cross-reference includes the following information:

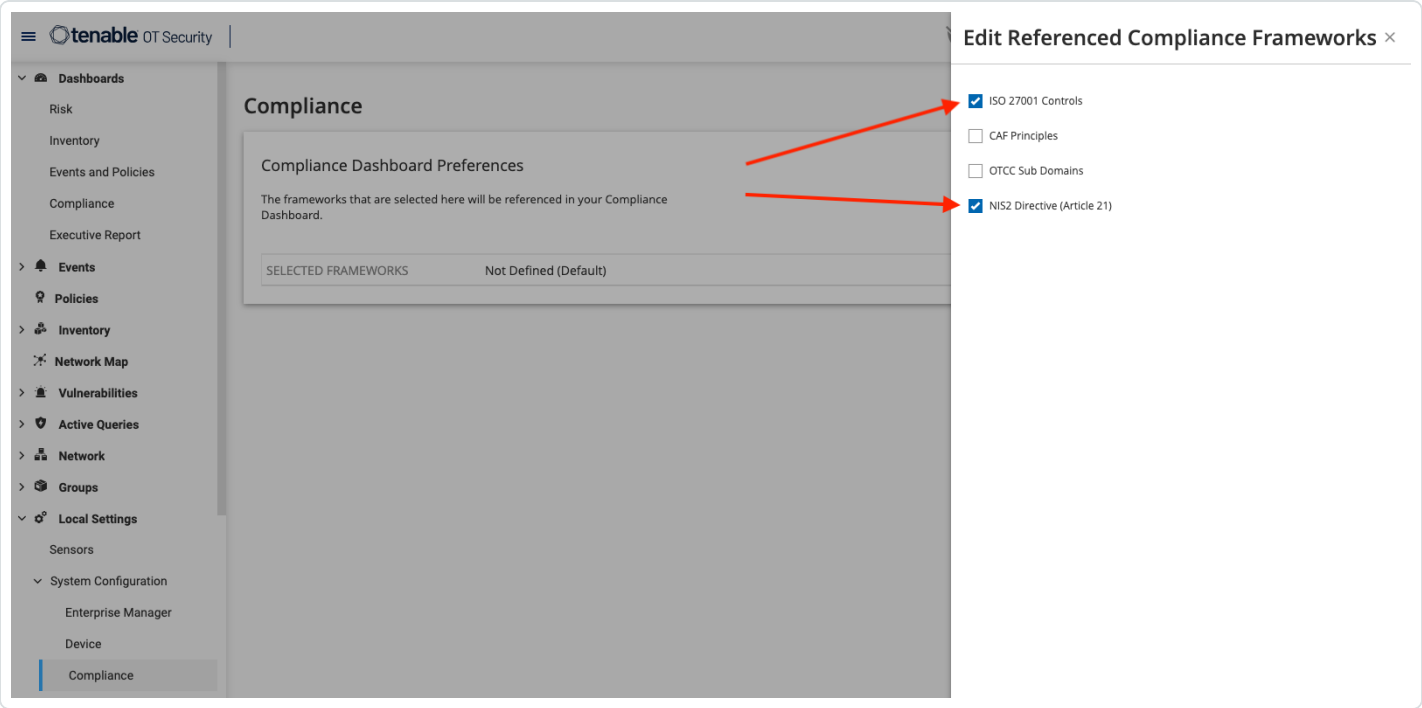
- The article name.
- **SECURITY DOMAIN** — The primary Cyber Security Domain.
- **SECURITY SUB-DOMAIN** — The secondary Cyber Security Domain.
- **SECURITY MEASURE** — The action that needs to be taken.
- **CROSS REFERENCES** — Cross-references to ISO 27001, NIST CSF, and ISA/IEC 62443.
- Relevant Tenable information to assist and provide guidance.

Tenable OT and Framework Mapping Preferences

Operational Technology (OT), includes hardware and software systems that monitor and control industrial equipment and processes. Many of these systems were traditionally isolated, but are now becoming integrated with IT networks, making them more vulnerable to cyber attacks. Securing these devices requires comprehensive strategies, and continuous monitoring. Tenable OT, beginning with version 3.19 SP1, contains compliance mapping to the NIS 2 Framework, specifically Article 21, and ISO 27001 to assist organisations meet compliance standards, traditionally only available to other IT devices. To enable this option, select the Security Framework Preferences link as shown below.



Once selected you will be prompted to choose the appropriate Framework.



Vulnerability Management

Vulnerability Management is the process of identifying, assessing, reporting, managing, and remediation of vulnerabilities across the organisation on an on-going basis. Article 21(2)(e) addresses Network and Information Systems Security, including, acquisition, development, maintenance, and vulnerability handling and disclosure. Organisations can map NIS 2 to other

standards, such as ISA IEC 62433, ISO 27001, and NIST CSF via the Cross-Reference notes. This document provides readers with a key aspect in addressing specific requirements within the topic area.

Key Aspects of Vulnerability Management

Tenable utilises Risk-based Vulnerability Management (RBVM) to take the guesswork out of which vulnerabilities you should tackle first. RBVM gives organisations clear answers to reduce the time and effort in navigating through a never-ending vulnerability backlog.

RBVM is a process that reduces vulnerabilities across your attack surface by prioritising remediation based on the risks they pose to your organisation. Unlike legacy vulnerability management, risk-based vulnerability management goes beyond just discovering vulnerabilities. This unique approach helps organisations understand vulnerability risks with threat context and insight into potential business impact.

Risk-based vulnerability management uses machine learning to correlate asset criticality, vulnerability severity, and threat actor activity. This helps organisations cut through vulnerability overload so they can focus on the relatively few vulnerabilities that pose the most risk to your enterprise. Article 21, paragraph 2, section e, references Network and Information Systems Security, including Vulnerability Handling and Disclosure. This section specifically addresses preventative network and information vulnerability management.

Preventative Network and Information Vulnerability Management

Several sections within the NIS 2 may be best suited to fall into the Vulnerability Management category. Those include:

- Article 21(2)(e) Network and Information Systems Security, including Vulnerability Handling and Disclosure
- Article 21(2) (d): (d) Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers.
- Article 21(2)(g) Basic Cyber Hygiene Practices and Cybersecurity Training
- Article 21(2)(a) Risk Analysis and Information System Security

The Cyber Hygiene, Section (g), and Risk Analysis, Section (a), are special topics and therefore will be discussed in more detail in the Security Hygiene Practices, and Risk Assessment section of this guide.

Knowing what hosts are on your network is the starting point to any vulnerability assessment. The diverse location of assets makes discovery and identification a challenge. Understanding where critical assets are and accurately inventorying assets is the crucial first step in Risk-Based Vulnerability Management (RBVM). Through credentialed scanning, assets can be reliably identified and attributes collected, which enables organisations 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 organisation can begin to establish an inventory, which can be used to assess and mitigate associated risks to the organisation.

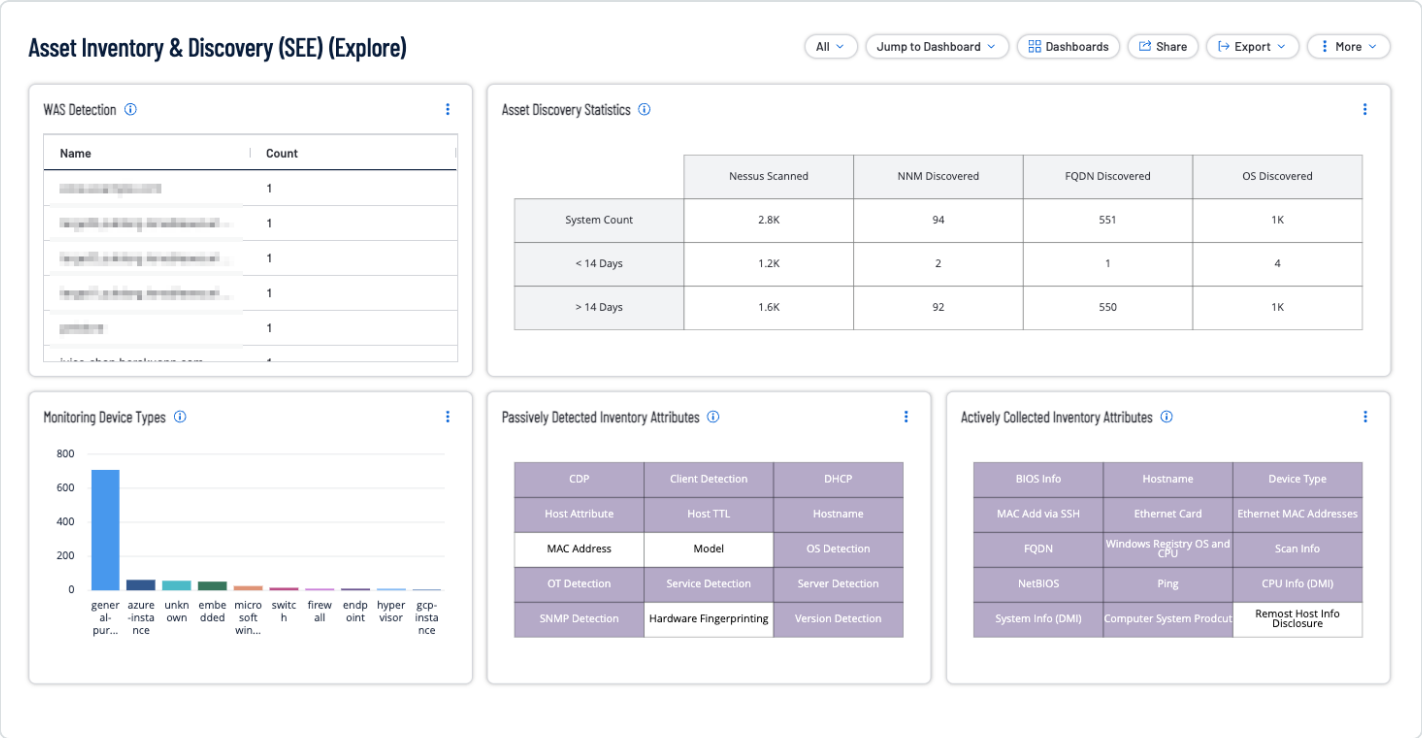
Attackers are not tied to a specific timezone and are continuously scanning the address space of target organisations, searching for new and possibly unprotected systems to be attached to the network. Transient devices, such as laptops or Bring-Your-Own-Device (BYOD) devices may be out of synchronisation 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.

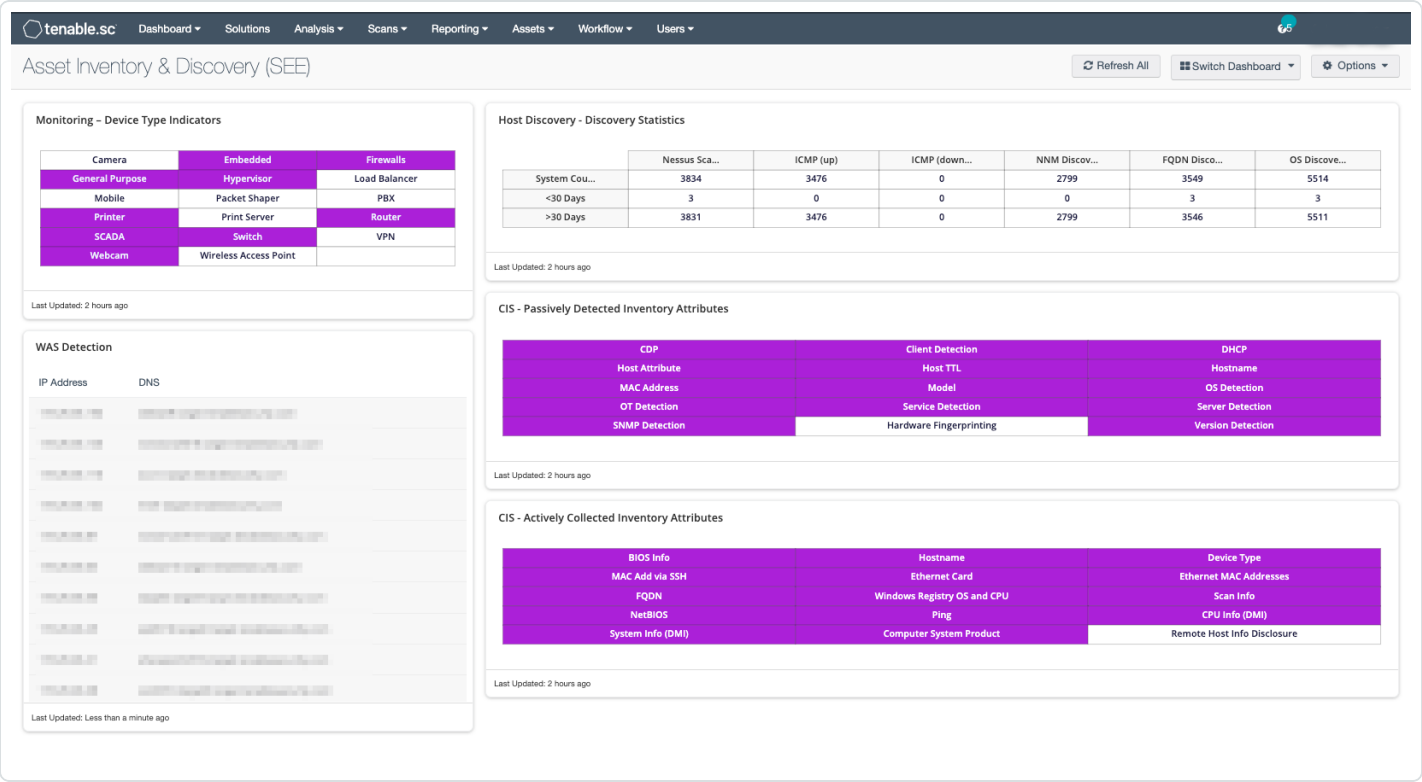
Maintaining a comprehensive and up-to-date asset inventory is a fundamental and critical component of RBVM. Modern IT environments encompass on-premises, cloud infrastructure, mobile devices, ephemeral and transient assets, web applications, IoT devices, and more. Asset identification of all connected assets within an organisation is a common baseline requirement in a number of security standards. Maintaining an asset inventory is also the critical first step in the Discovery phase of RBVM, allowing organisations 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 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)



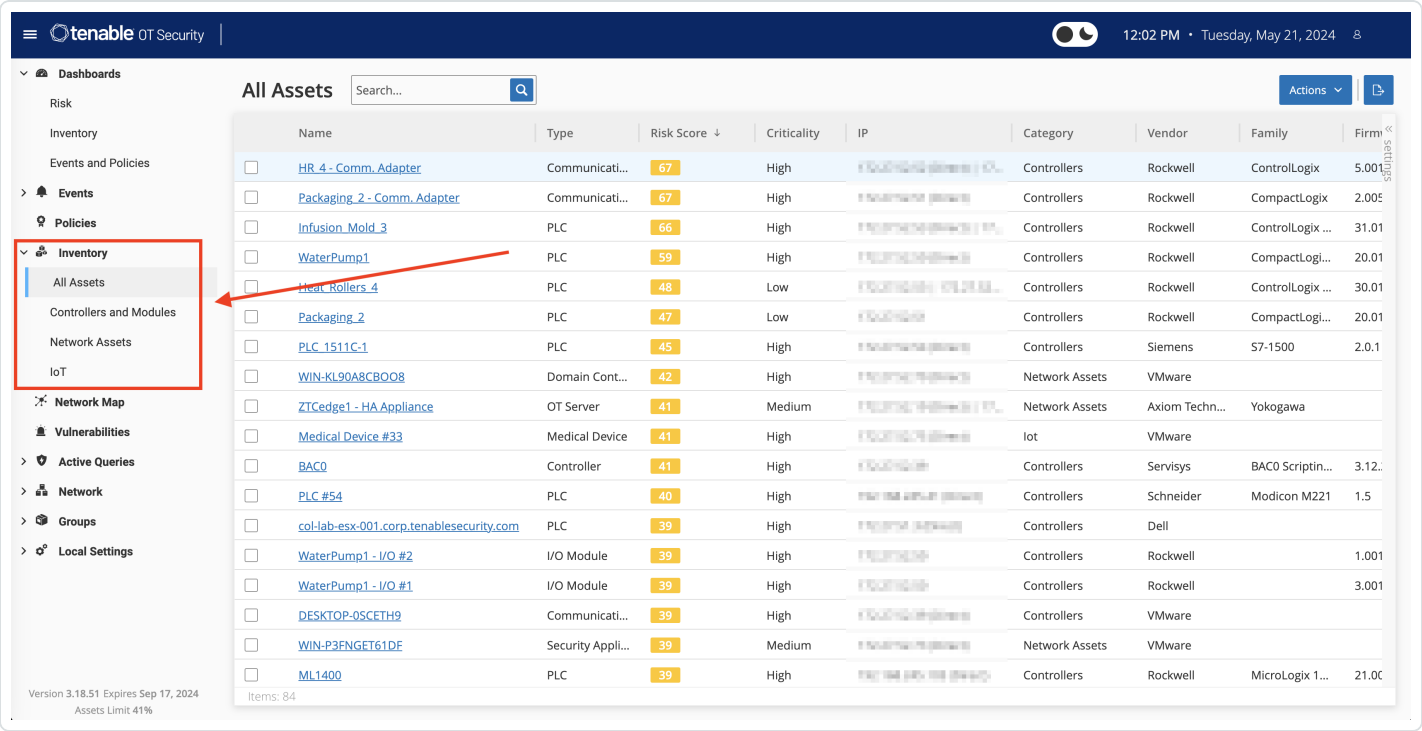


For more information on Asset Discovery and Classification see the [Asset Inventory and Discovery Cyber Exposure Study](#).

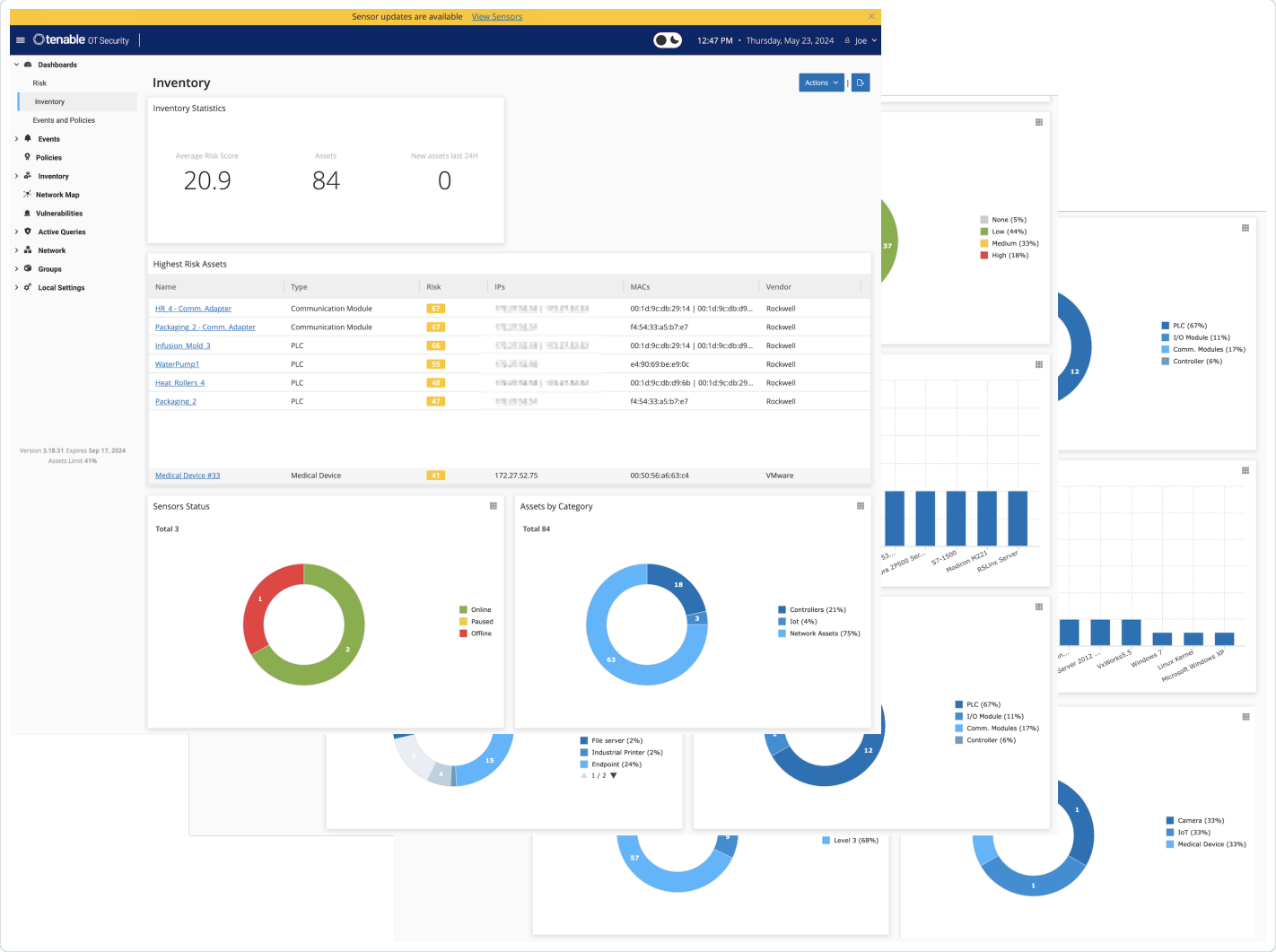
Tenable OT

For organisations with industrial controls, 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**.

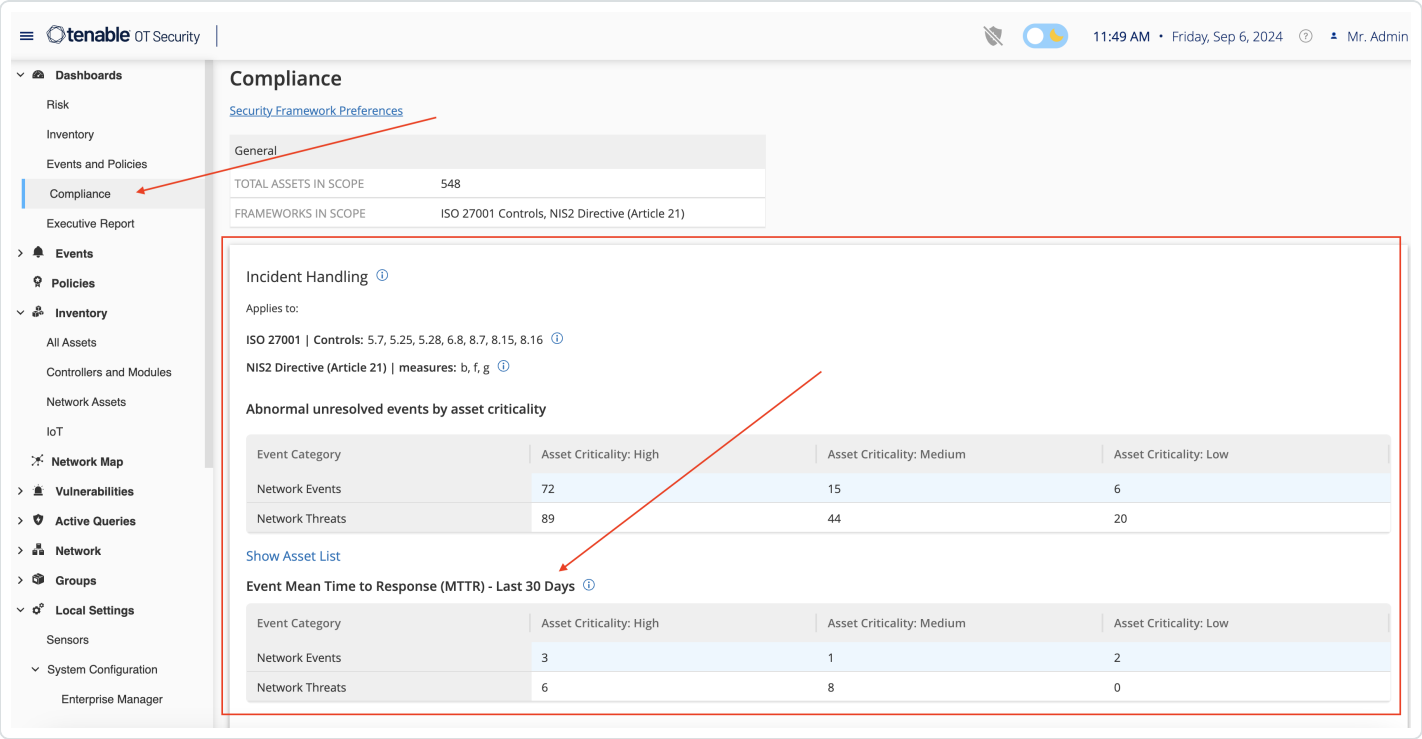


Tenable OT provides three in product dashboards that display assets in groupings such as by **Category, Vendor, Module Type, Purdue Level**, and more, facilitating asset management and tracking. Tenable OT Security provides a complete visibility of assets across the environment (IT and OT). A service 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.



The Vulnerability Handling widget for Tenable OT, located on the compliance dashboard assists in the process of identifying, assessing, reporting, and remediating vulnerabilities. Using this widget, analysts can focus first on assets that have the potential to impact on business operations.

Mean time to Respond (MTTR) is a critical key performance indicator (KPI). A shorter MTTR indicates a more efficient incident resolution process. Minimising downtime and disruptions is crucial for maintaining productivity and service availability. From a Vulnerability Management perspective, OT security personnel can utilise the MTTR for each vulnerability severity within scope, track improvements, and measure SLAs and progress over time. Key items displayed are severity results, high risk assets and MTTR/SLA.



For more information on using Tenable OT Security reference the documentation for your organisation's version here: [Getting Started with Tenable OT Security](#).

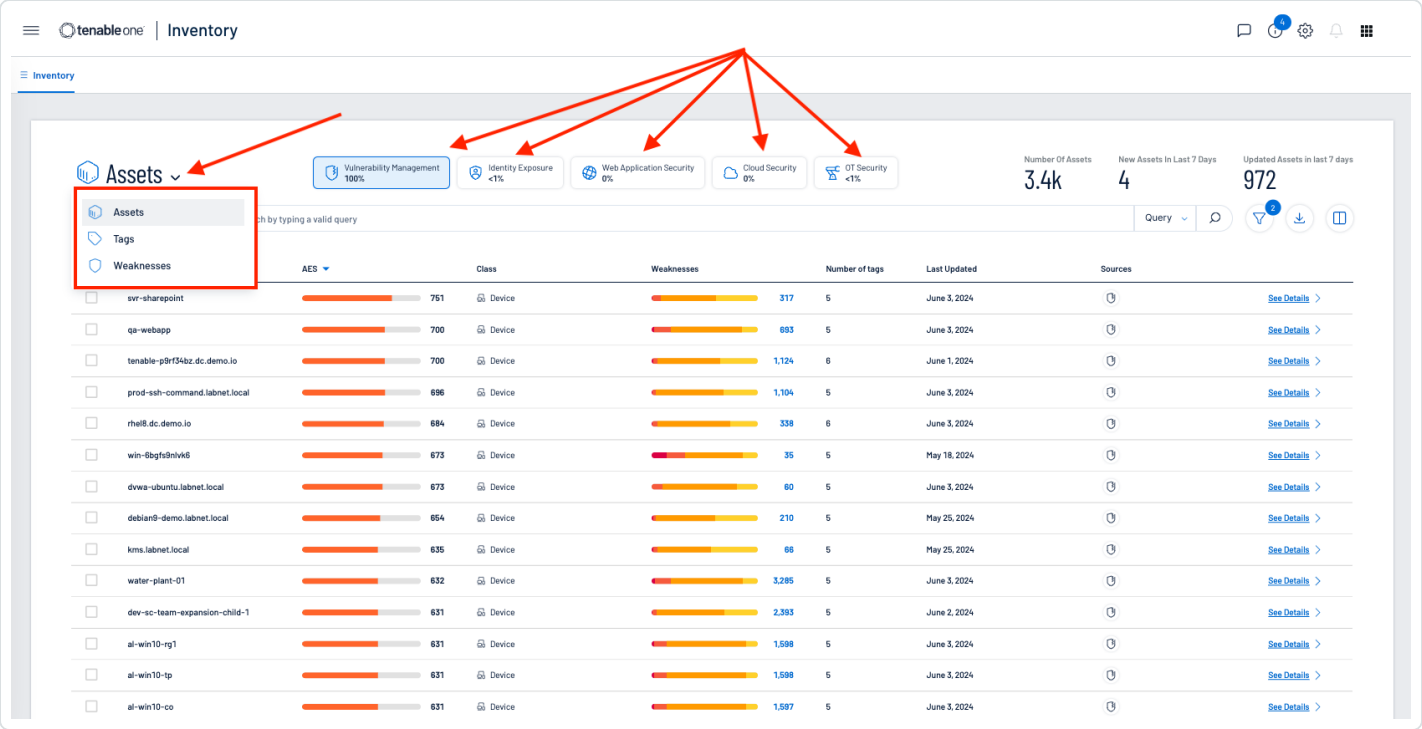
Tenable One

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.

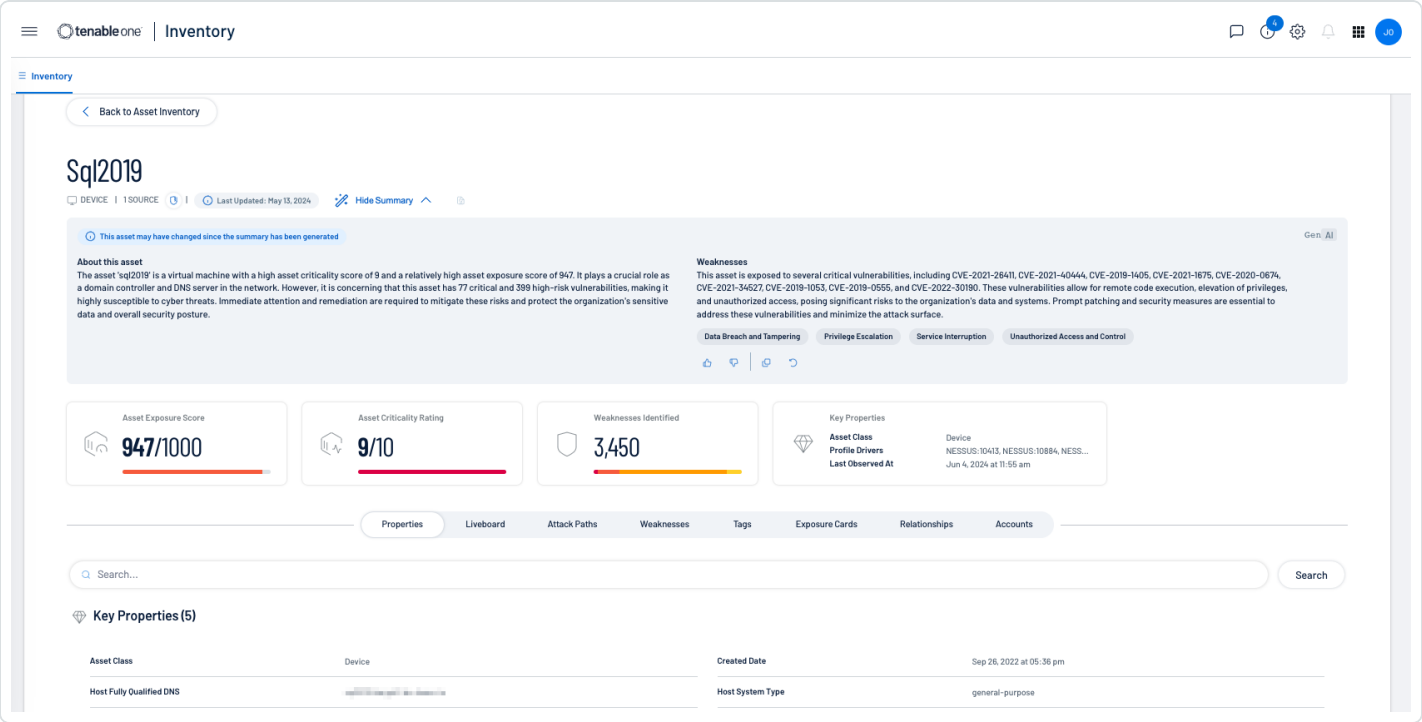
Tenable One Asset Inventory provides a comprehensive view of all assets across the entire attach surface. Sensors pull data from multiple applications across the platform, providing details on all known systems. At the highest level on the Asset Inventory page is shown the Number of Assets identified, New Assets identified in the last 7 days, and assets that have been updated in the last 7 days. Buttons allow you to select any combination of assets (Vulnerability Management, Identity Exposure, Web Application Security, Cloud Security, OT Security).

Displayed in the main body of the page is the **Asset**, **the Asset Exposure Score, Class of device, Weakness, Tags, Last Update Date, Source, and Details**. Selecting the Asset drop-down also allows all assets to be displayed by Tag or by Weakness. Weakness is a Common Vulnerability and Exposure (CVE), which is a reference method for publicly known vulnerabilities, maintained by the MITRE Corporation, and funded by the US National Cyber Security Division and the US Department

of Homeland Security. Assets can be grouped together, or displayed separately within Vulnerability Management, Identity Exposure, Web Application Security, Cloud Security, and OT Security, by selecting (or deselecting the corresponding icon).



Drilling down into the Asset details provides a wealth of information, including insights into the assets properties, **Attack Paths, Weaknesses, Exposure Cards, Relationships, and Accounts**. For more information on Tenable One features and benefits, go here.



Once an organisation has determined NIS 2 compliance is required, based on size or categorization as an Essential or Important Entity, steps must be taken to ensure compliance with a number of Articles. In an effort to make compliance with the NIS 2 as easy as possible, this document links NIS 2 articles to pre-established Standards and Security Domains.

Article 21(2)(e): Network and Information Systems Security, including Vulnerability Handling and Disclosure

NIS 2 Article 21(2)(e) references security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure.

Security domains define how information is classified, categorised, or administered. The following Security Domains, Sub-Domains, and Measures are related to NIS 2 Article 21(2)(e), and can assist organisations already using other standards and frameworks to comply with NIS 2.

SECURITY DOMAIN: Governance and Ecosystem

SECURITY SUB-DOMAIN: Information System Security Governance & Risk Management

SECURITY MEASURE: Information system security indicators.

In an effort to foster higher consistency and reliability across multiple frameworks and the NIS 2, Article 21(2)(e) can be associated with the ISO 27001, NIST CSF, and ISA/IEC 62443 utilising the

following cross-references for vulnerability handling and disclosure. The following cross-references cover the processes and procedures related to asset management, software management, risk management strategies, data security, and the business environment.

CROSS REFERENCES:

The ISO 27001 references sections within Planning, Support, Performance Evaluation, and Annex A, specifically the following sections:

- ISO 27001 (6.2, 7.1, 7.2, 9, A.12.1.3)

The NIST CSF references the following sections within Identify and Protect.

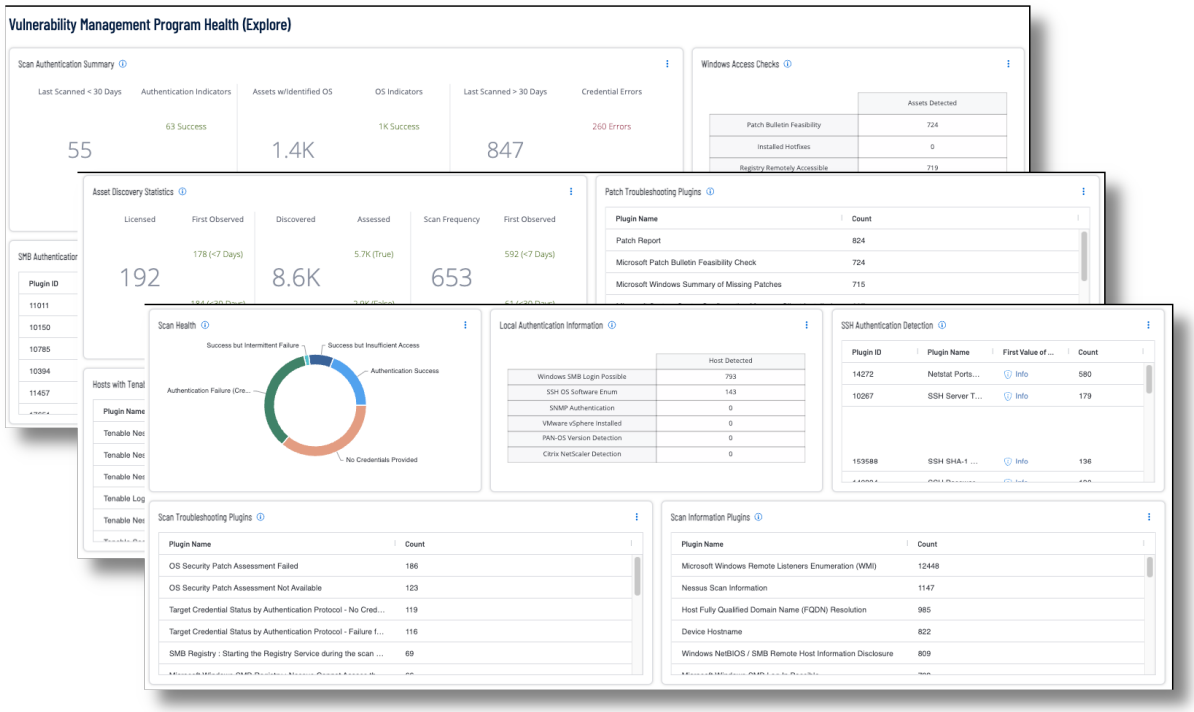
- NIST CSF (ID.AM -5, ID.RM-2, 3, PR.IP -7,8, PR.DS -4, ID.BE -5)

The ISA/IEC 62443 references the following sections within System Integrity, and Data Confidentiality.

- ISA/IEC 62443 (SR 3.4, SR 4.1)

Measurable metrics that provide insights into an organisation's security posture are important indicators in determining the effectiveness of an organisation's vulnerability management program. These indicators may relate to the risk management organisation's performance, the maintaining of resources in secure conditions, the number of unpatched systems, or the severity ratings of vulnerabilities.

When managing the effectiveness of a vulnerability assessment program within the organisation, dashboards such as the **Vulnerability Management Program Health** dashboard, for Tenable Vulnerability Management, shown in the following image, helps security operations teams ensure their scanning program is appropriately maintained for an evolving operational technology landscape aligned with business strategy.



There are many factors that can adversely affect the scope and accuracy of scan data, such as failed credentials, network problems, or licence limitations. This dashboard provides security analysts comprehensive information to monitor the health of their scanning program.

Analysts can drill into the summary information displayed in the dashboard to troubleshoot upstream scanning problems that can adversely impact downstream reporting to stakeholders.

For additional in-depth information related to Vulnerability Management, see [the Vulnerability Management Cyber Exposure Guide](#).

Audit and Accreditation

An IT Security Audit is a comprehensive assessment of an organisation's infrastructure and security posture. The definitive method to find and identifying vulnerabilities within an organisation's network is by conducting authenticated scanning. Authenticated scanning can be defined by connecting to a system and providing credentials in order to gain access to the system. Nessus scans systems by using different network protocols (SSH, SMB, HTTPS, SNMP, etc.) in order to gain access to the remote target asset. For example, logging in to a remote host via SSH using a username and password is a method of authentication. Each remote asset is able to authenticate

using several protocols. Assets with more than one authenticatable protocol, for example Windows server running a SQL server, could report both authentication success and failure.

Optionally, Tenable Nessus Agents can also be utilised. Tenable Nessus Agent scans use lightweight, low-footprint programs that are installed locally on hosts. Tenable Nessus Agents collect vulnerability, compliance, and system data, and report that information back to Tenable Nessus Manager or Tenable Vulnerability Management for analysis. Tenable Nessus Agents are designed to have minimal impact on the system and the network, giving you the benefit of direct access to all hosts without disrupting your end users.

Understanding this fact during analysis is key to understanding if the system was successfully scanned or not. While in many cases the successful authentication of an asset may seem binary, there are many examples of successfully scanned systems with authentication failures. The system administrator should review all the failures and understand the services which are enabled on the asset for a complete analysis. The following Security Domains, Sub-Domains, and Measures are related to authentication, and can assist organisations already using other standards to comply with NIS 2. Specifically, information systems security audit and accreditation are the main elements to focus on here.

NIS 2 Article 21(2)(e) references security in network and information systems acquisition, development and maintenance, including audits within vulnerability handling and disclosure.

Security domains define how information is classified, categorised, or administered. The following Security Domains, Sub-Domains, and Measures are related to NIS 2 Article 21(2)(e), and can assist organisations already using other standards and frameworks to comply with NIS 2.

SECURITY DOMAIN: Governance and Ecosystem

SECURITY SUB-DOMAIN: Information System Security Governance & Risk Management

SECURITY MEASURE: Information system security audit (and accreditation)

In an effort to foster higher consistency and reliability across multiple frameworks and the NIS 2, Article 21(2)(e) can be associated with the ISO 27001, NIST CSF, and ISA/IEC 62443 utilising the following cross-references for information security audits and accreditation. The following cross-references cover the processes and procedures related to audits and accreditation, assisting organisations meet the requirements of authenticated/credentialed scans, by confirming that scans are successful.

CROSS REFERENCES (Audit Related):

The ISO 27001 references sections within Planning, Operations, Performance Evaluation, Improvement, Organisational, and Technological Controls, specifically the following items

- ISO 27001 (6, 8, 9.2, 9.3, 10, A.5.1.2, A.12.7.1, A.18.2)

The NIST CSF references the following sections within Identify, and Detect.

- NIST CSF (ID.GV -3, 4, ID.RA-1, 3, 4, 5, 6, ID.RM-1, 2, 3, DE.CM -8, DE.DP -5, ID.SC -4, PR.AC-1, PR.PT -1, PR.IP -7, 12, RS.IM -1, 2, RC.IM -1, 2)

The ISA/IEC 62443 references the following sections within Policies and Procedures.

- ISA/IEC 62443 (SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12)

NIS 2 Article 21(2)(e) references security in network and information systems acquisition, development, and maintenance, including accreditation of vulnerability audits.

CROSS REFERENCES (Accreditation Related):

The ISO 27001 references sections within Planning, Operations, Performance Evaluation, Improvement, and Organisational Controls, specifically the following items:

- ISO 27001 (6.1, 8, 9.2, 10.1, A.12.1.1, A.12.7.1)

The NIST CSF references sections within Identify and Detect.

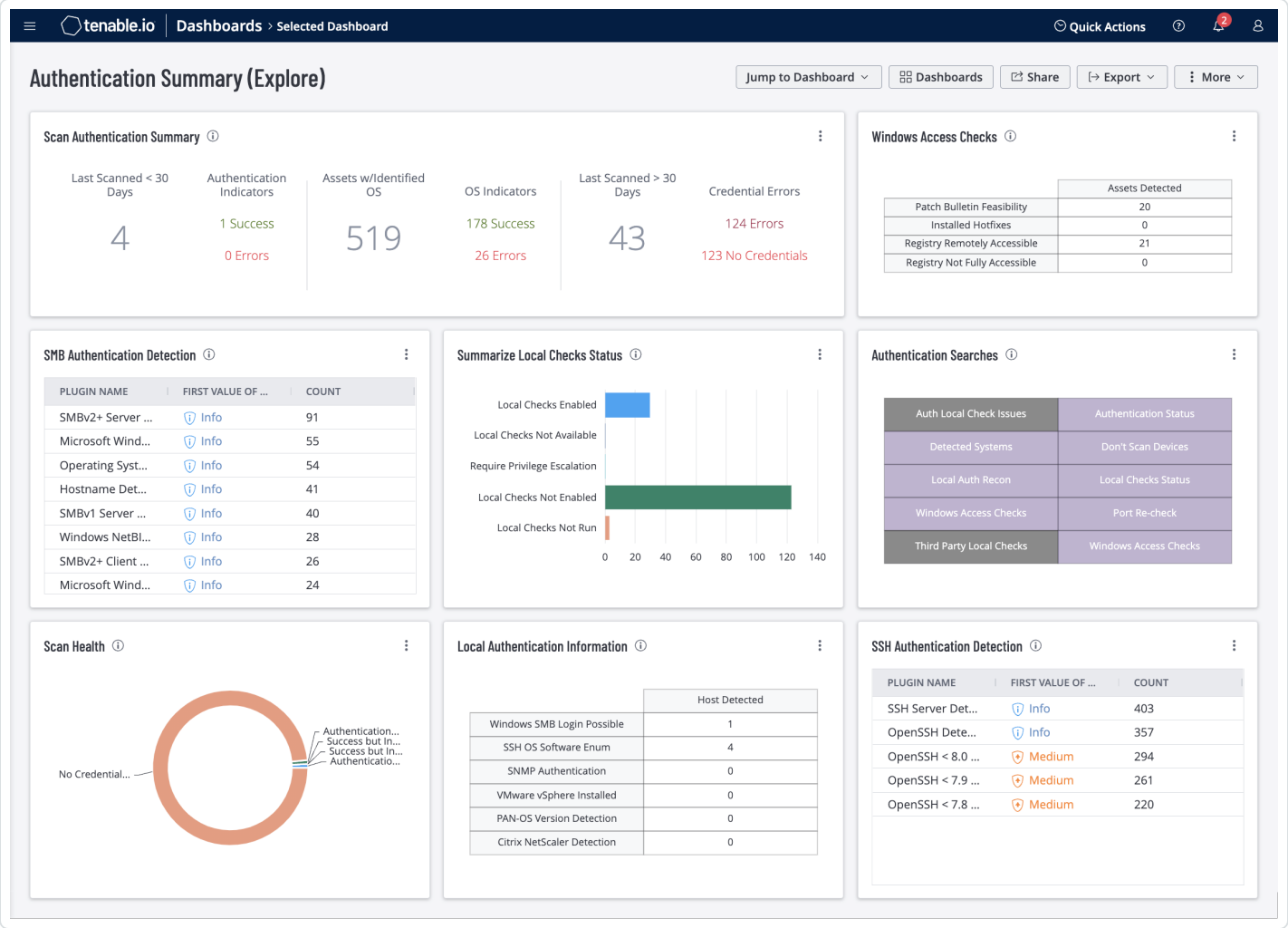
- NIST CSF (ID.RA-1, 3, 4, 6, ID.RM-1, 2, 3, ID.SC -1, RS.IM -1, 2, PR.IP -7, 12, PR.PT -1, DE.CM -8, RS.MI -3)

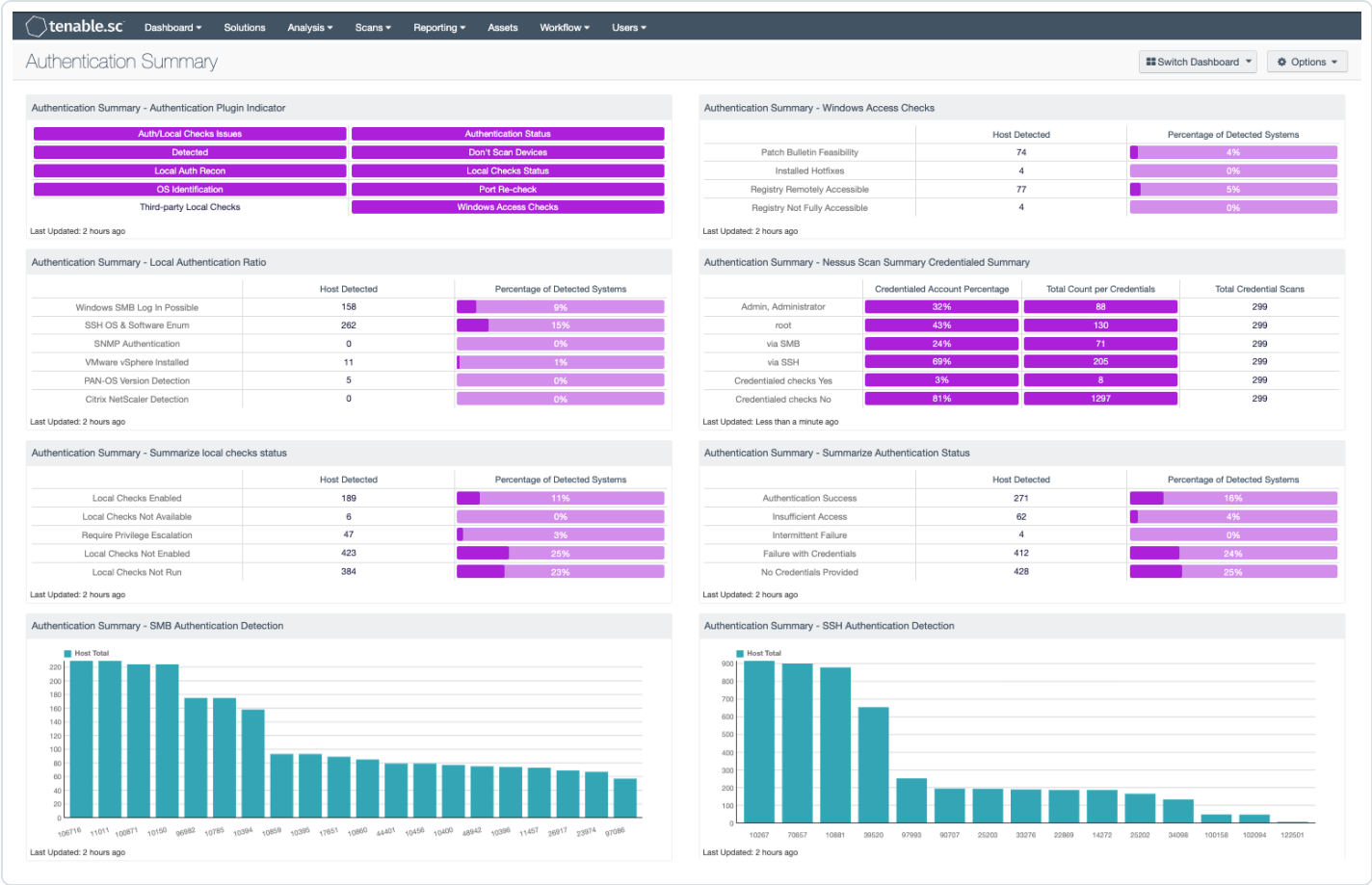
NIST CSF The ISA/IEC 62443 references sections within Policies and Procedures.

- ISA/IEC 62443 (SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12)

Authenticated (credentialed) and unauthenticated (non-credentialed) scans offer different approaches to vulnerability assessments. They primarily differ in the level of access and permissions granted to the Tenable Nessus scanner. Agent or credentialed scans perform a wider variety of checks than non-credentialed scans, which can result in more accurate scan results. However, there are benefits to an unauthenticated scan as well. For example, unauthenticated scanning is fast, and can detect vulnerabilities that are visible from outside the network, such as open ports, services, and potential entry points for attackers. The choice between the two methods depends on the specific goals of the assessment. Often a combination of both will provide the most comprehensive view of a system's vulnerabilities.

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





Authentication is a process of connecting to a system by providing credentials to gain access. Systems are scanned using different network protocols (SSH, SMB, HTTPS, SNMP, etc.) to gain access to the target asset. For example, logging into a remote host via SSH using a username and password is a method of authentication. Each asset can allow authentication using several protocols. Assets with more than one available authentication protocol (for example, a Windows server running a SQL server) could report both authentication success and failure. Understanding this fact during analysis is key to determining if the system was successfully scanned or not. While in many cases the successful authentication of an asset may seem binary, there are many examples of successfully scanned systems with authentication failures. Tenable recommends system administrators review all of the failures and investigate the services which are enabled on the asset for a complete analysis.

Credentialed vulnerability scans are easier with Nessus Agents, because after the agents are installed, they don't need on-going host credentials. When Nessus Agents are installed (either manually or with a software management system), they are installed under the local SYSTEM account in Windows or root on Unix-based operating systems. The agents then inherit the

permissions of the account used for installation so they can perform credential scans, even if the credentials on the system have changed.

Tenable Nessus Agents are designed to have minimal impact on the system and the network, giving organisations the benefit of direct access to all hosts without disrupting your end users. Additionally Tenable Nessus Agents provide extended scan coverage and continuous security, eliminate the need for credential management, reduce network bandwidth, and minimise maintenance.

There are also cases where there is overlap in the intent of the check. For example, if you use OS fingerprinting without credentials in a network-based scan and query the system for the exact version of its OS in a credentialed scan, this overlap heightens the credential findings over the network, since the network version tends to be a best guess.

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

Additional information can be located in the Vulnerability Assessment/Scanning section of the Vulnerability Management Cyber Study.

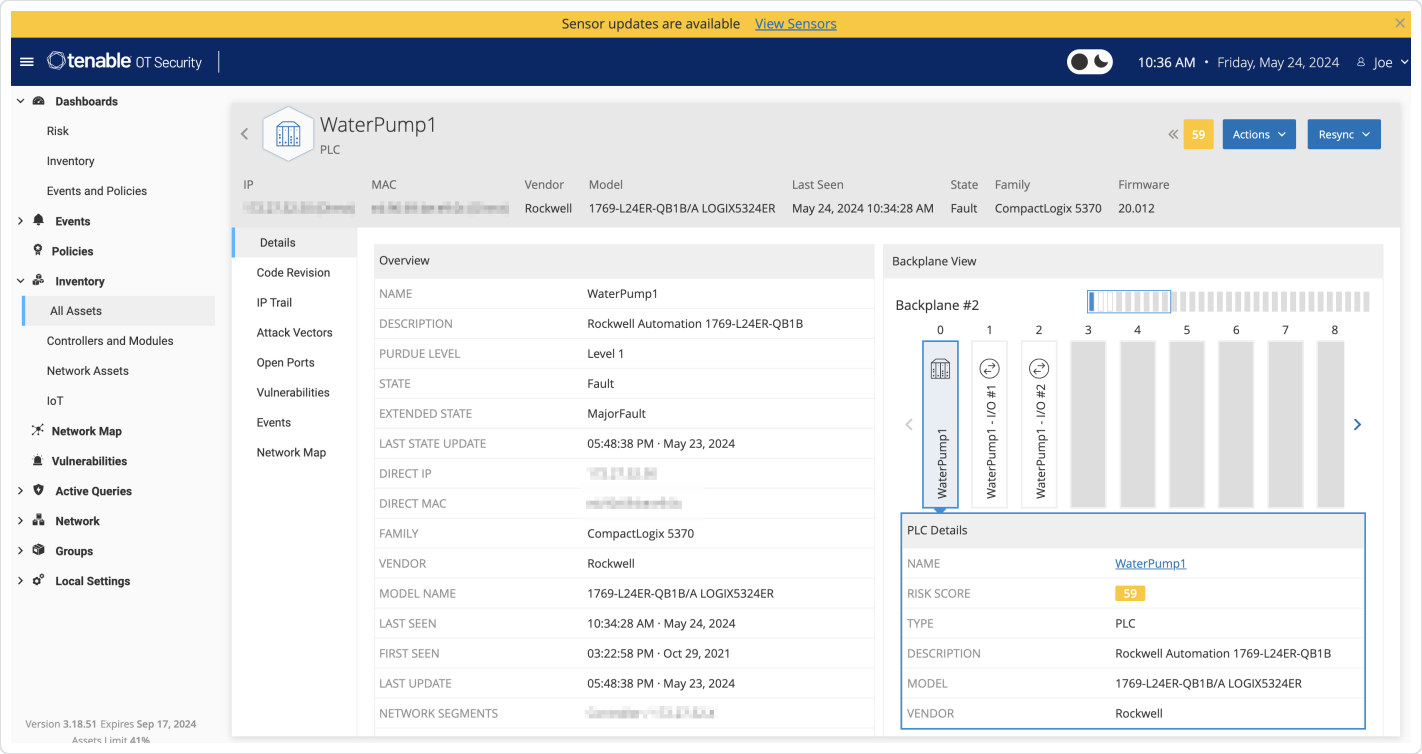
Industrial Control Systems

Article 21(2)(d): (d) Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers.

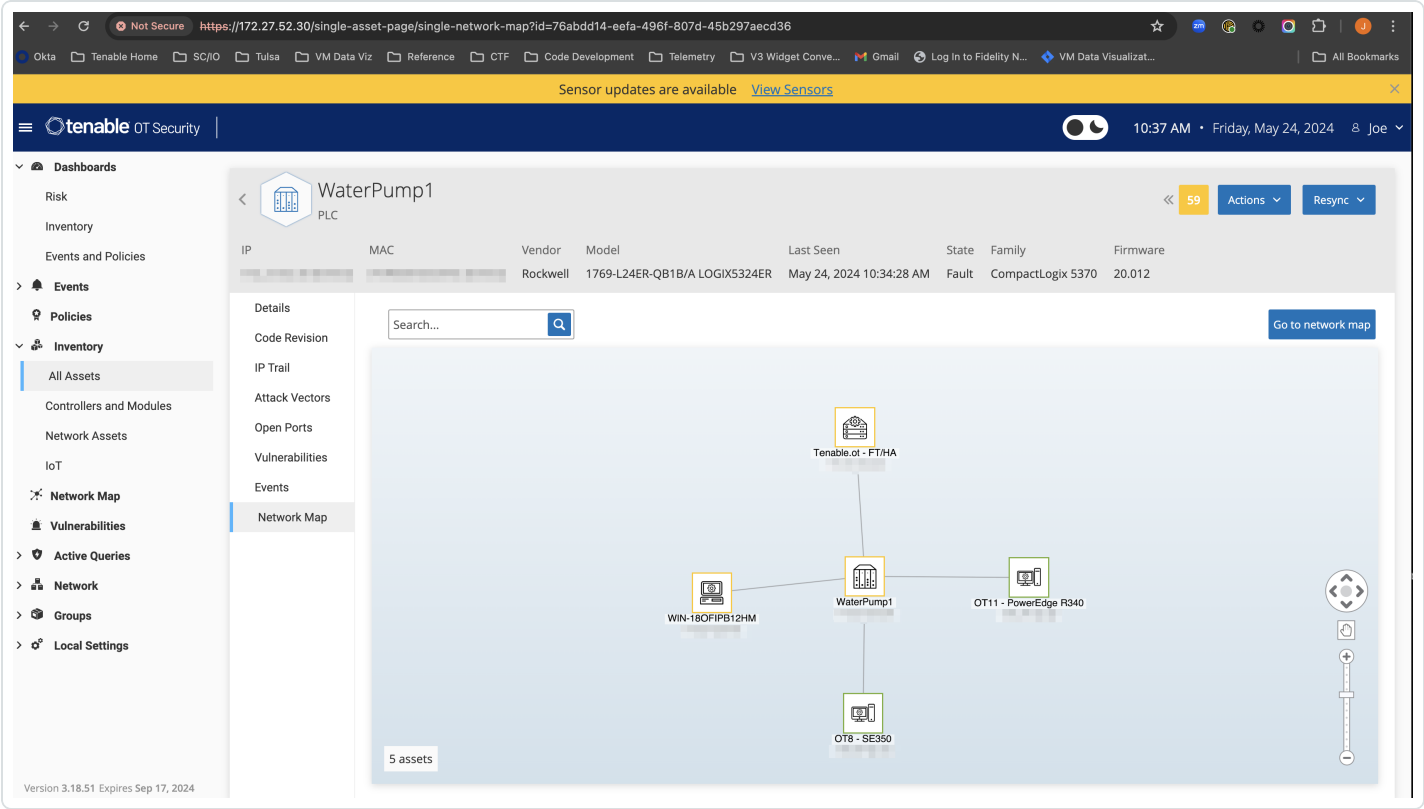
Tenable OT Security maps out assets as well as communication paths. A complete visibility of assets across the environment (IT and OT) is available. Tenable OT Security uses active sensors that can be deployed deep within network segments, to sniff packets and identify the devices communicating on the wire. Once there is an inventory of the assets on the network, Tenable OT Security sends active queries in a safe and secure manner to discover the remaining dormant devices. This discovery process is called hybrid discovery and Tenable is the first to use this methodology for effective asset inventory and mapping.

Information Technology (IT) primarily deals with data processing and communications. Operational Technology (OT) generally refers to the hardware and software that is used to monitor and control devices and processes within industry, manufacturing, energy, transportation, and utility environments. OT can also include industrial control systems (ICS), supervisory control and data acquisition (SCADA) systems, programmable logic controllers (PLC), and other devices used to monitor and control industrial processes.

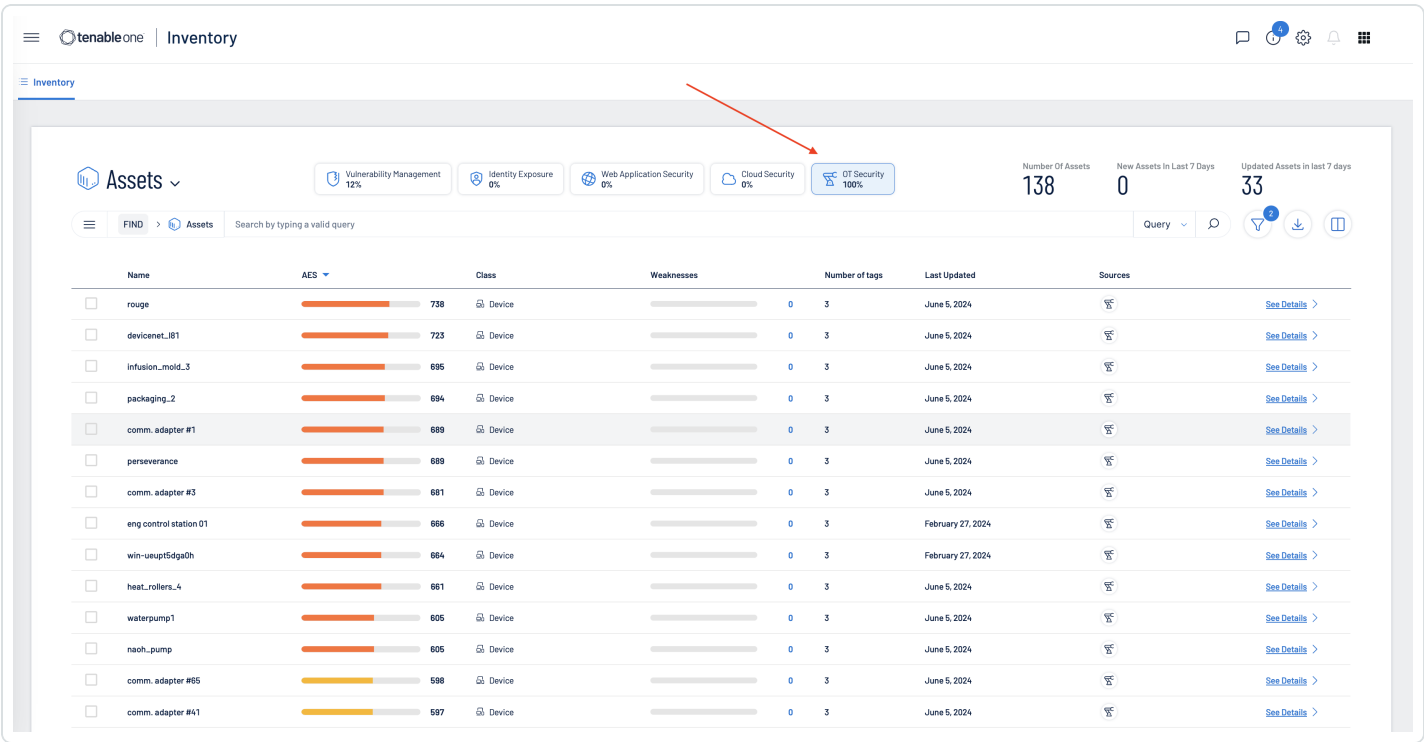
As technology advances and IT-OT systems converge, new challenges are created and these systems become more vulnerable to cyber threats. Safety and security become increasingly important. Security teams can now get visibility into device make and model, as well as firmware version and status.



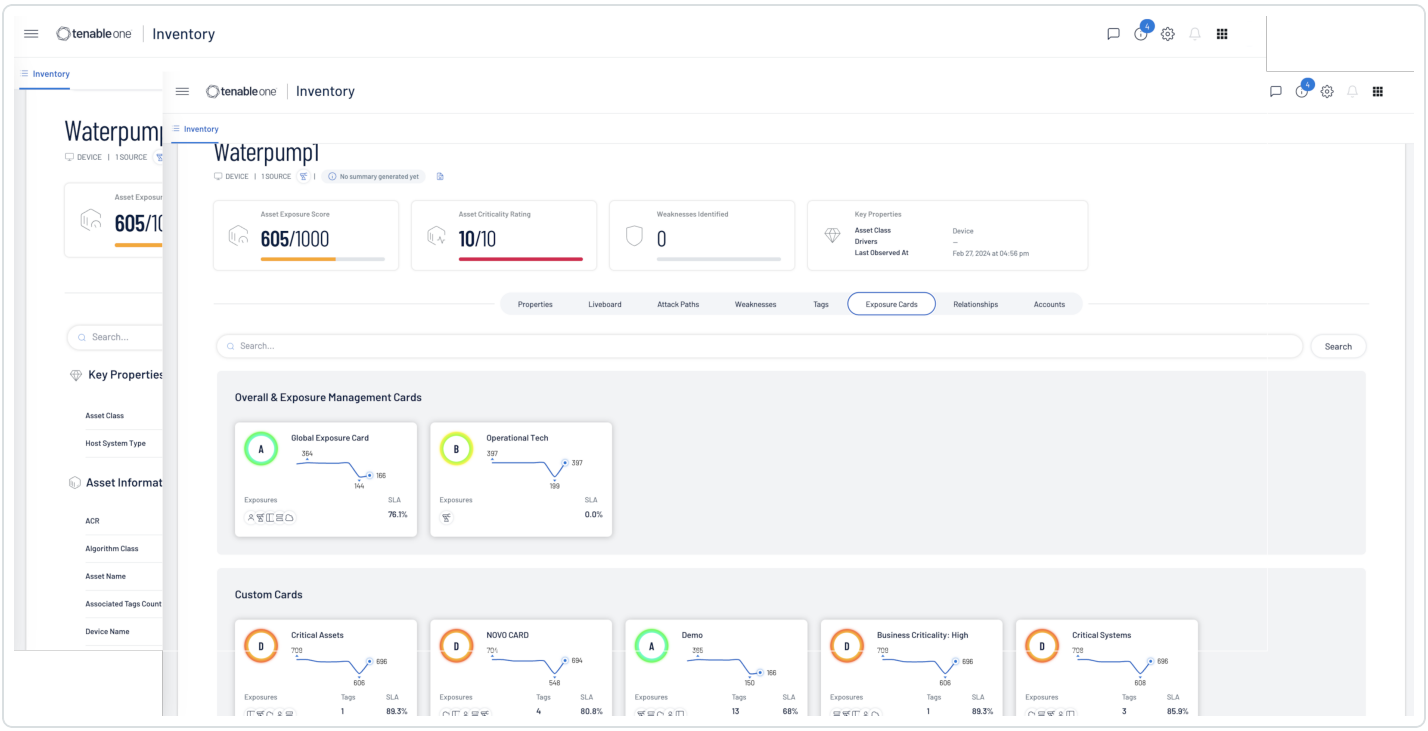
Connections can also be mapped to other devices on the network.



Utilising Tenable One, **OT Assets** can be displayed by selecting the **OT Security icon**.



Clicking on the See **Details** link to the right of the page presents additional information on the asset, such as properties, **Attack Paths, Weaknesses, Exposure Cards** and more.



The following Security Domains, Sub-Domains, and Measures are related to Industrial Control Systems, and can assist organisations already using other standards to comply with NIS 2.

For click here for more information on Tenable One.

NIS 2 Article 21(2)(d) references supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers.

Security domains define how information is classified, categorised, or administered. The following Security Domains, Sub-Domains, and Measures are related to NIS 2 Article 21(2)(d), and can assist organisations already using other standards and frameworks to comply with NIS 2.

SECURITY DOMAIN: Protection.

SECURITY SUB-DOMAIN: IT Security Maintenance.

SECURITY MEASURE: Industrial Control Systems.

In an effort to foster higher consistency and reliability across multiple frameworks and the NIS 2, Article 21(2)(d) can be associated with the ISO 27001, NIST CSF, and ISA/IEC 62443 utilising the

following cross-references for Industrial Control Systems. The following cross-references cover the processes and procedures related to supply chain security and other security-related aspects.

CROSS REFERENCES:

The ISO 27001 references sections within Context, Leadership, Support, Operation, Performance Evaluation, and Improvement, specifically the following sections:

- ISO 27001 (4, 5.2, 5.3, 7, 8, 9.1, A.6.1.1, A.8.1.1, A.8.2.3, A.9, A.11, A.12, A.14, A.15, A.17)

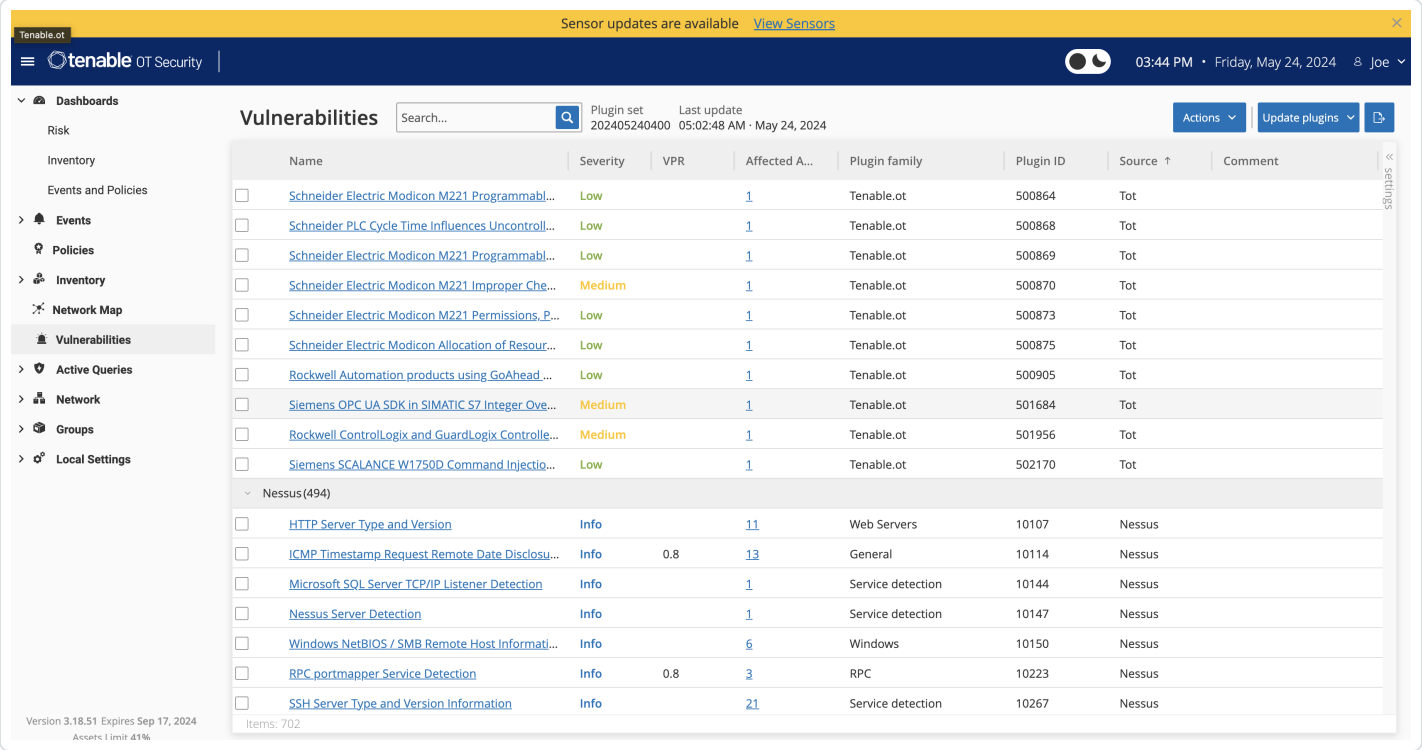
The NIST CSF references the following sections within Identify and Protect.

- NIST CSF (ID.BE -1, 2, 3, 4, ID.AM -1, 2, 4, 6, ID.GV -2, ID.SC -1, 2, 3, 4, 5, PR.AC -5, PR.PT -4)

The ISA/IEC 62443 references the following sections within nearly every system requirement.

- ISA/IEC 62443 (SR 1.10, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7, SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.1, SR 3.2, SR 3.3, SR 3.4, SR 3.5, SR 3.8, SR 3.9, SR 4.1, SR 4.2, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 5.4, SR.6.1, SR 6.2, SR 7.1, SR 7.2, SR 7.3, SR 7.4, SR 7.6, SR 7.8)

The **Vulnerabilities** screen within Tenable OT Security displays a list of all vulnerabilities detected by the Tenable Plugins that affect your network and assets. Vulnerabilities include those detected by Tenable OT Sensors, as well as Nessus. You can customise the display settings by adjusting which columns are displayed and where each column is positioned. For an explanation of the customization features, see Management Console User Interface Elements.



The Vulnerabilities page displays the following details:

Parameter	Description
Name	The name of the vulnerability. The name is a link to show the full vulnerability listing.
Severity	This score indicates the severity of the threat detected by this Plugin. Possible values: Info, Low, Medium, High, or Critical.
VPR	Vulnerability Priority Rating (VPR) is a dynamic indicator of the severity level, which is constantly updated based on the current exploitability of the vulnerability. Tenable generates this value as the output of Tenable Predictive Prioritization, which assesses the technical impact and threat posed by the vulnerability. VPR values range from 0.1-10.0, with a higher value representing a higher likelihood of exploitation.
Plugin ID	The unique identifier of the Plugin.
Affected Assets	The number of assets in your network affected by this vulnerability.

Plugin family	The family (group) with which this Plugin is associated.
Comment	You can add free text comments about this Plugin.

For more information on Tenable OT Security, consult the [Getting Started with Tenable OT Security found here](#).

IT Security Maintenance

Timely and effective remediation remains the Achilles' heel for too many organisations. Even if security teams identify a concise list of prioritised CVEs, they must work closely with their IT counterparts to address those issues, providing detailed information about how to remediate each vulnerability and why it's a priority. Without adequate teamwork, the security program is not nearly as effective. Remediation also involves indirect costs, whether that's IT Operations or Information Security team's time or the cost of taking down a business-critical system to install and test a patch. The teams are required to efficiently allocate resources where they can have the greatest impact for the least amount of effort.

Once the highest priority vulnerabilities are identified, the 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, and as organisations develop a comprehensive understanding of the environment. The terms remediate, mitigate, and accept, can be best defined as:

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 been done to actually fix the vulnerability

itself. Instead, organisations are accounting for other mitigating factors that neutralise some or all of the risk posed by the vulnerability. For example, organisations may have firewall rules in place that effectively block an exploit from accessing sensitive data. To account for this mitigating factor, organisations 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 organisations choose to accept risk, the Vulnerability Management platform may allow you to remove the risk score from reports or set the score to "0." However, organisations need to understand that while the vulnerability may no longer be immediately visible, the actual risk still remains in your environment.

NIS 2 Article 21(2)(e) references network and information systems security, including vulnerability handling and disclosure.

Security domains define how information is classified, categorised, or administered. The following Security Domains, Sub-Domains, and Measures are related to NIS 2 Article 21(2)(e), and can assist organisations already using other standards and frameworks to comply with NIS 2.

SECURITY DOMAIN: Protection.

SECURITY SUB-DOMAIN: IT Security Maintenance.

SECURITY MEASURE: IT security maintenance procedure.

In an effort to foster higher consistency and reliability across multiple frameworks and the NIS 2, Article 21(2)(e) can be associated with the ISO 27001, NIST CSF, and ISA/IEC 62443 utilising the following cross-references for IT security maintenance. The following cross-references cover the processes and procedures related to IT security maintenance procedures.

CROSS REFERENCES:

The ISO 27001 references sections within Support, Operations, Improvement, and Technological Controls, specifically the following sections:

- ISO 27001 (7.5.3, 8.1, 10.1, A.11.2.4, A.12.1.2, A.12.6.1, A.14.1.1, A 14.2, A.15.2.2)

The NIST CSF references the following sections within Protect.

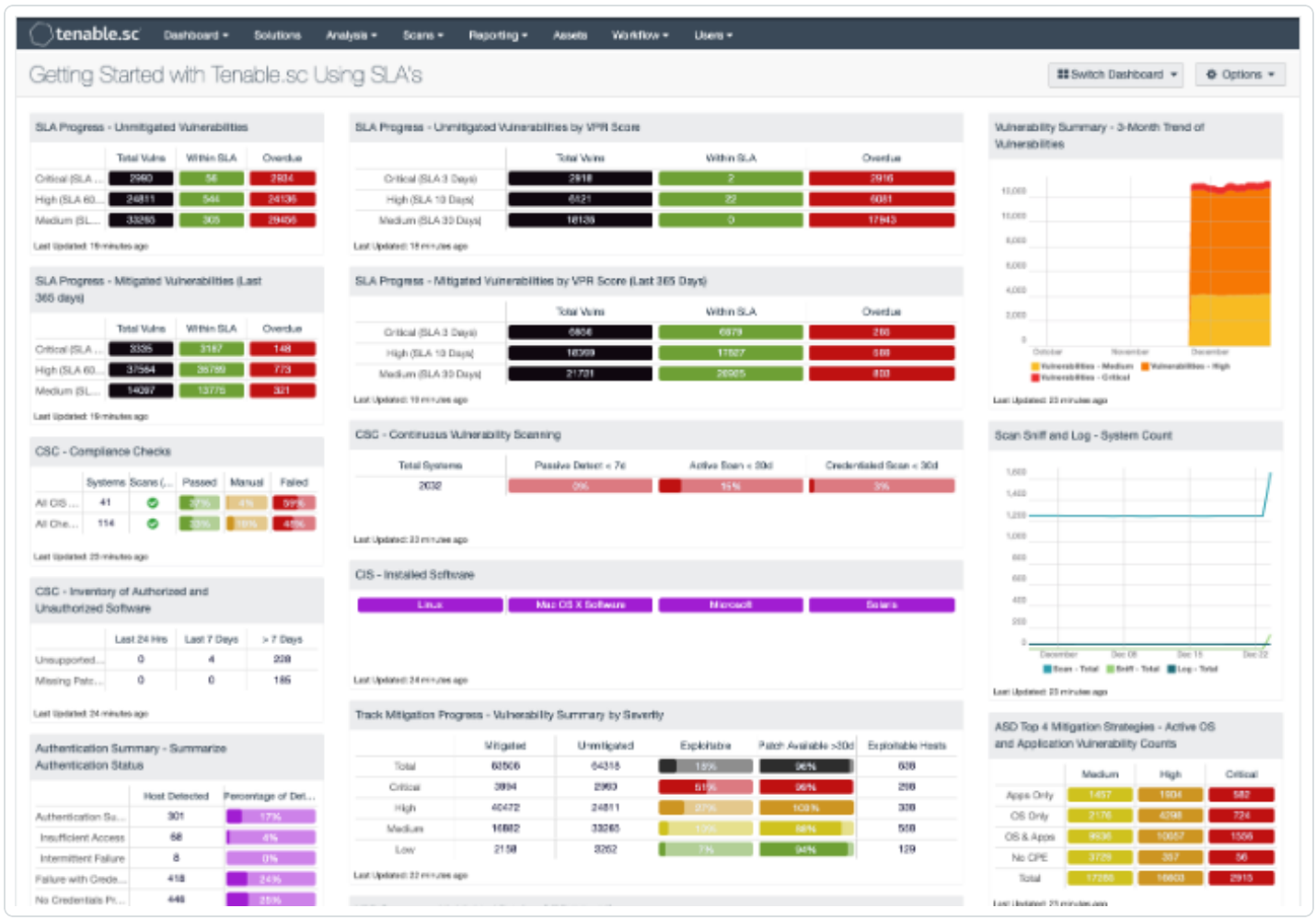
- NIST CSF (PR.MA -1, 2, PR.IP -1, 2, 3,4, 7, PR.DS -3, 4, ID.SC -4)

The ISA/IEC 62443 references the following sections within Audit Logs and Network and Security Configuration Settings.

- ISA/IEC 62443(SR 3.1, SR 3.3, SR 3.4, SR 3.8, SR 6.1, SR 7.6)

Service Level Agreements (SLA) are often utilised in the IT industry to outline or track expectations between a service provider and a customer. An SLA is a great; and often used, option to track other items within an organisation, such as patching and vulnerability remediation progress. Tracking SLA progress is a definitive method to demonstrate the success of an organisation's remediation efforts.

Service Level Agreements often change from one organisation to the next, however meeting SLAs is a common issue among organisations industry wide. Tenable.sc provides a vast array of data that provides vulnerability management SLA metrics, but where can organisations get started? This dashboard is commonly used by the sales team at Tenable to help coach organisations to meet SLAs. The components in this dashboard are grouped in 3-series, which provide a CISO and Risk Manager with a starting point for SLA analysis.



https://www.tenable.com/sc-dashboards/getting-started-with-tenable-sc-using-slas

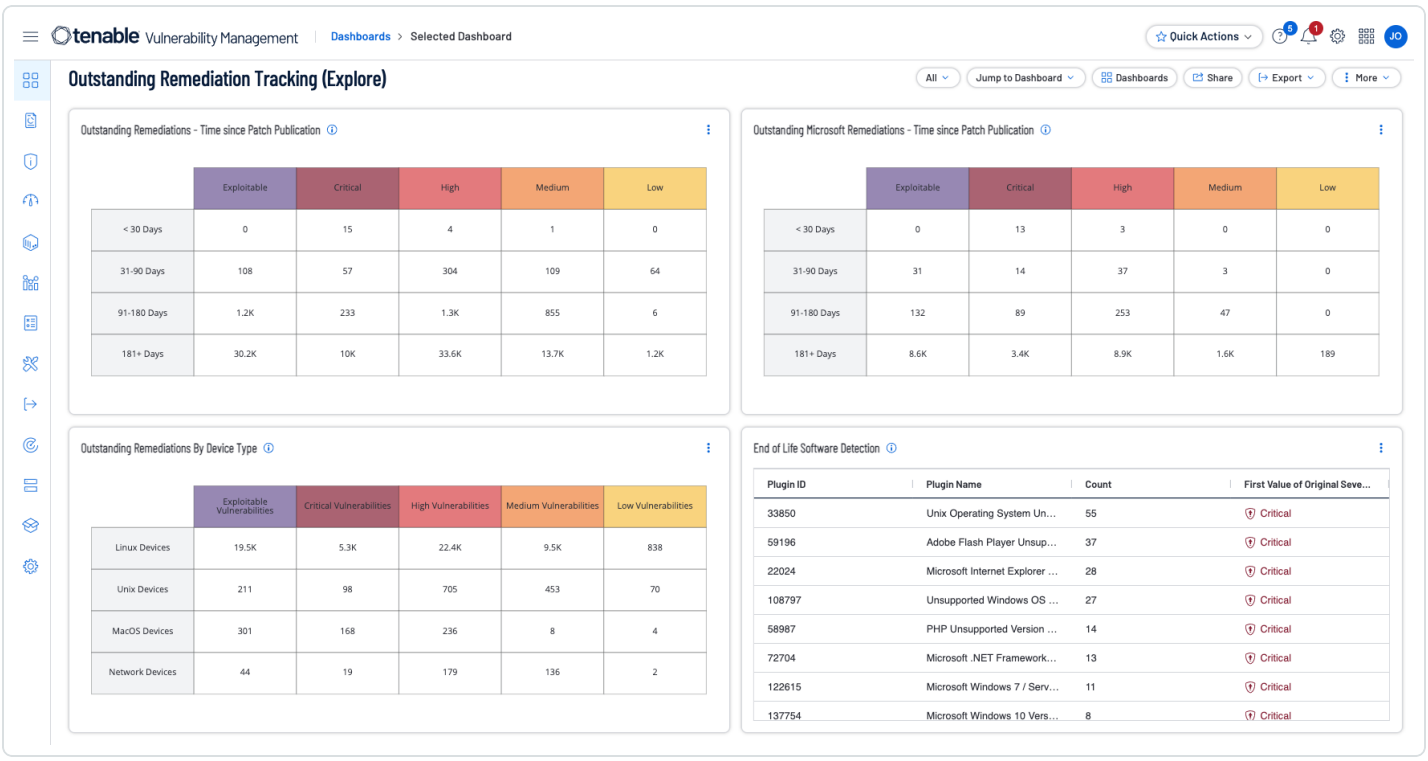
Within Tenable Vulnerability Management, the **Vulnerability SLA** widget enables organisations to track and report on their remediation efforts over time and severity.

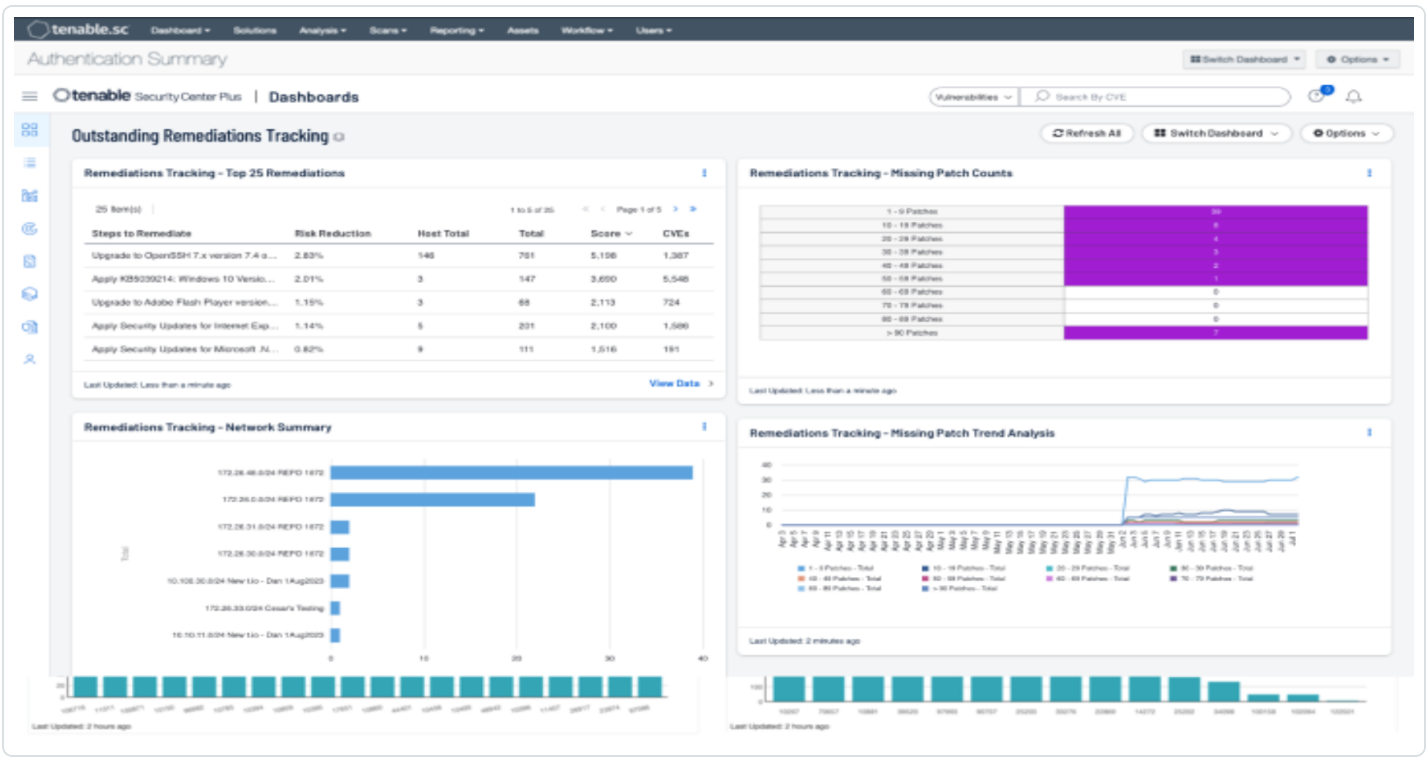
Vulnerabilities SLA

Severity / Date Range	>90	61 - 90	31 - 60	15 - 30	8 - 14	0 - 7
Critical	1.51K	156	17	5	0	18
High	3.87K	474	10	3	3	5
Medium	1.99K	271	21	5	2	0
Low	175	39	0	0	0	0

Vulnerabilities are displayed by severity and time to remediate from less than 7 days to over 90 days. Tenable recommends prioritising remediation of exposures that pose the greatest risk to the organisation. This widget enables organisations to identify the vulnerabilities that are not being remediated quickly, or outside of established timeframes. Organisations with an effective vulnerability management program have critical vulnerabilities displayed in the far right three columns, representing remediations occurring within 30 days or less. Vulnerabilities that pose less risk of exposure could have higher counts in the middle of the matrix in the 30-90 day time period. Numbers in the far left of the matrix depict vulnerabilities that are remediated after 90 days have passed.

Unpatched assets expose organisations to vulnerabilities that are actively being exploited. End of life assets may pose the greatest risk since they are unsupported and no longer receiving security updates or support from the vendor. Tenable provides the **Outstanding Remediation Tracking** dashboard for Tenable Vulnerability Management and Outstanding Remediations Tracking.



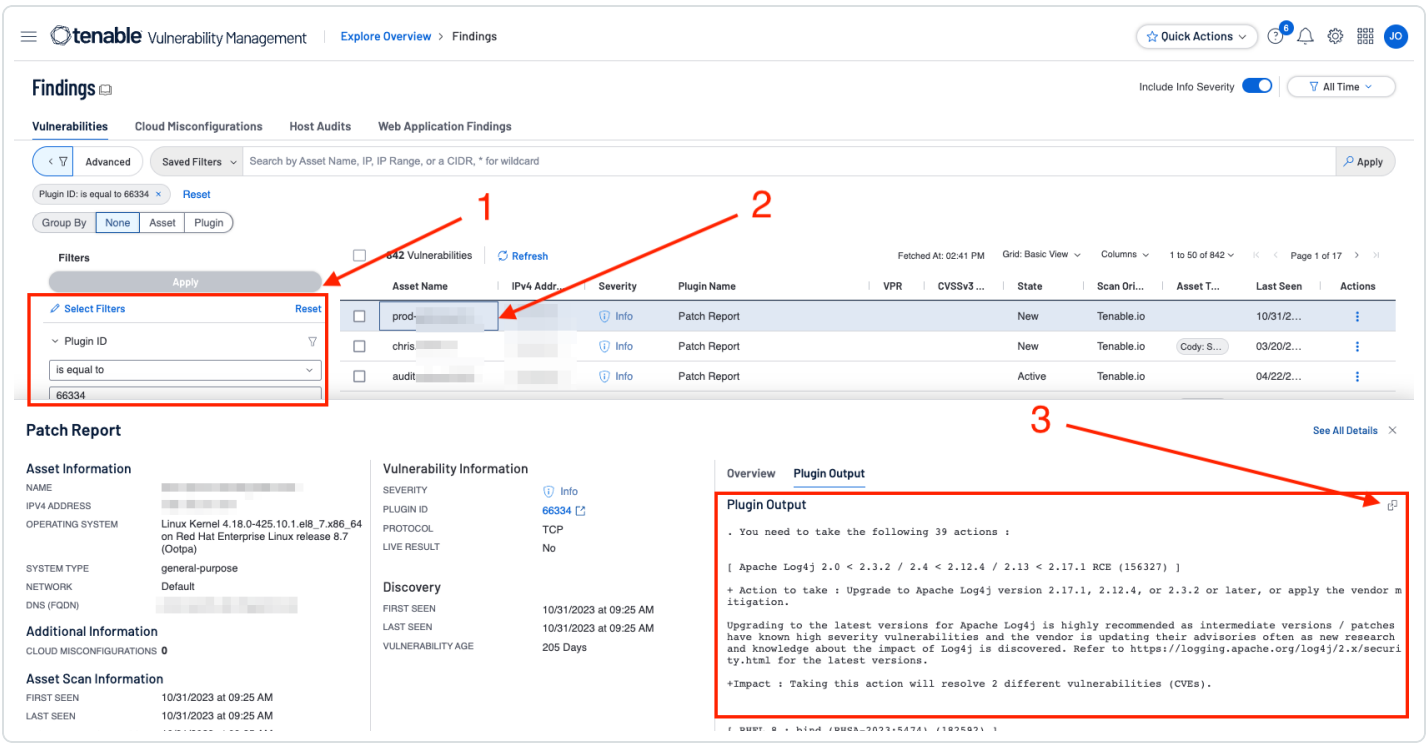


The Outstanding Remediations Tracking dashboard provides risk guidance using the “Remediation Summary” tool. This tool works by employing a concept called “top patch”. Tenable.sc uses proprietary technology to identify a chain of patches. The first patch in the chain is called the “top

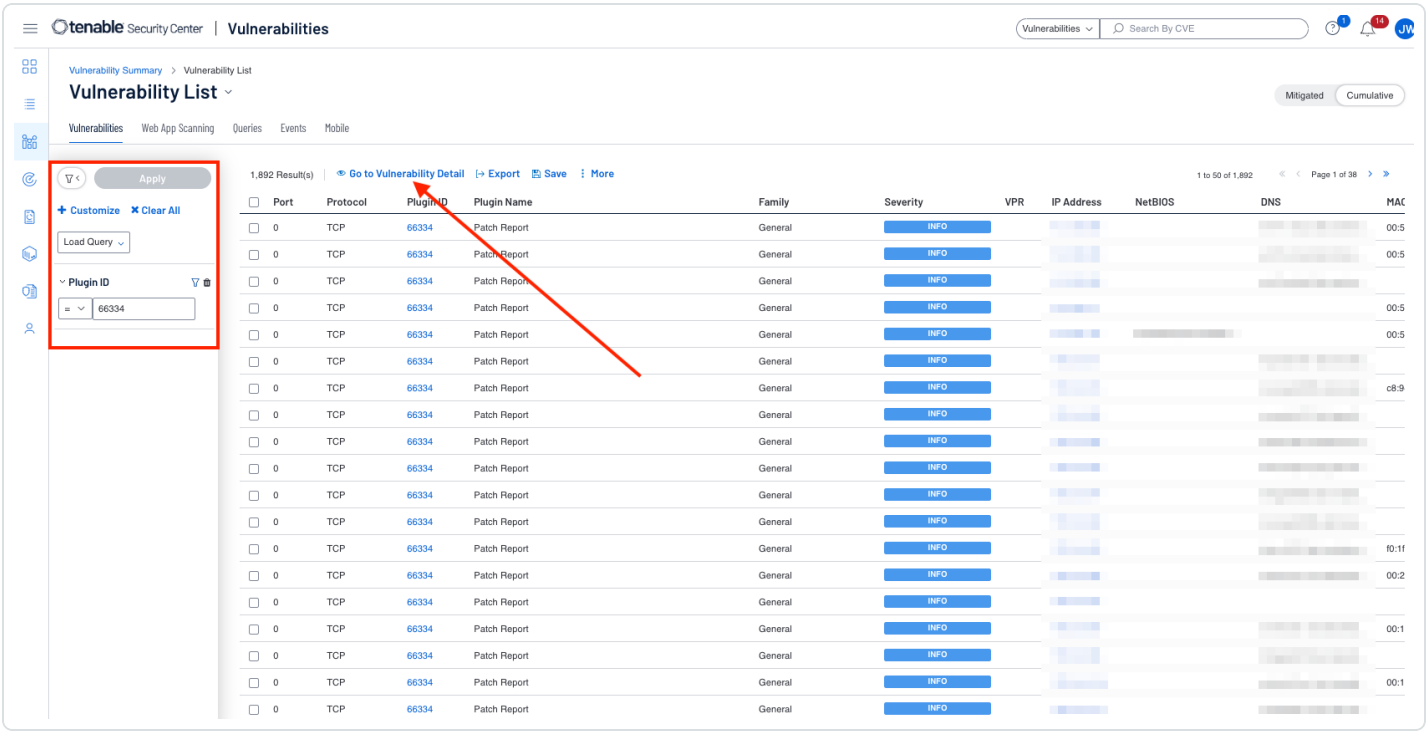
patch". If the "top patch" is applied, all subsequent vulnerabilities will also be remediated at the same time. Using both the Remediation Summary tool and "Patch Report" plugin, the organisation can better plan remediation efforts. Within Tenable Vulnerability Management several filters are used including those for unsupported products, patch publication date ranges.

The Nessus "Patch Report" plugin (66334) summarises all of the missing patches and general remediation actions required to remediate the discovered vulnerabilities on a given host. Instead of counting the number of vulnerabilities, the plugin lists applications that need to be upgraded. The approach is not only much easier for IT administrators to consume, but the count of applications provides a measure of how much "work" is required to secure a system.

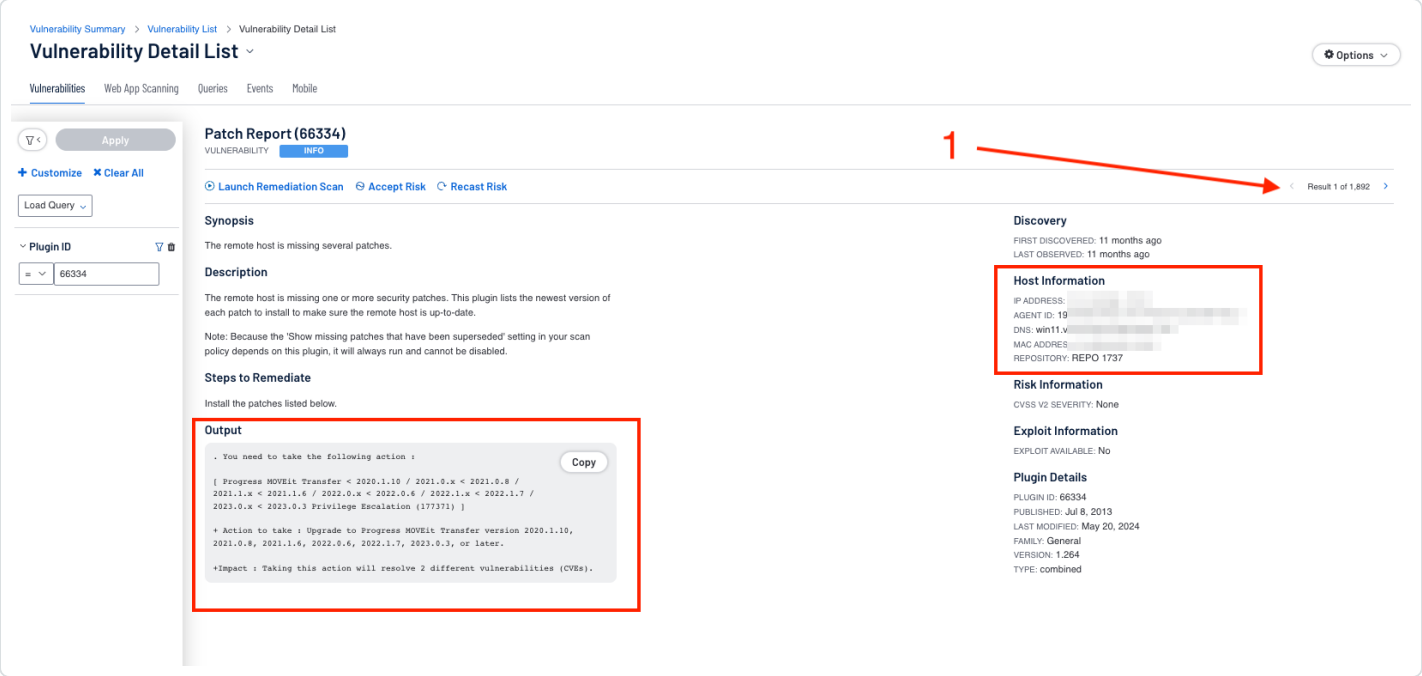
Within **Tenable Vulnerability Management**, analysts can create a filter for plugin 66334 within the filters component on the **Findings** page as shown following (1). Once results have appeared to select an asset (2) by clicking on the asset name opens the details window at the bottom of the page. Selecting Plugin Output reveals the detailed Actions to undertake, including the Impact those actions have. The information can easily be exported to the clipbord by clicking the copy (3) icon. An additional filter can be added to change the State filter to "Fixed" to review patches that have previously been resolved.



The steps are similar if using **Tenable Security Center**, however they vary slightly. From the **Analysis** tab, choose Vulnerabilities. Create a filter for plugin 66334. After the results are displayed choose to go to **Vulnerability Detail**.



The **Vulnerability Detail** is shown with the detailed Actions to undertake, including the Impact those actions have. The information can easily be exported to the clipboard by clicking the copy icon. To select the next detail click next (1). An additional filter can be added to change the state to "**Mitigated**" and "**Previously Mitigated**" to review patches that have previously been resolved.



Risk Assessment

Several sections within the NIS 2 may be best suited to fall into the Risk Assessment category. Those include:

- Article 21(2)(a): Risk Analysis and Information System Security: Cyber Risk-Based Approach
- Article 21(2)(c): Business Continuity: Business Continuity Process and Technology

Periodic risk assessment is the primary tool for engineers and security analysts to manage risks by maintaining good cyber hygiene, reducing operational downtime and mitigating the potential impact of threats.

Risk = Probability x Impact

Probability refers to the likelihood that an event occurs. Impact refers to the consequences or severity if the risk event actually does occur. This formula is foundational in assessing and prioritising risks within an organisation. Assessing the probability involves evaluating factors such as historical data and expert judgement, along with potential causes that could lead to the occurrence of a risk event. The result of the assessment is often a qualitative rating, such as Low,

Medium, or High. Impact can only be determined by understanding the potential consequences of an event on various organisational aspects, such as finances, operations, reputation, safety, and legal compliance. Impact is quantified in terms of monetary value, or time.

Based on impact, two options are available, risk acceptance and risk mitigation. If the organisational risk is low, perhaps the risk can be accepted. Tenable products allow risk acceptance as an option. Accept risk rules can be created that allow for the acceptance of vulnerabilities without actually changing the severity level of the plugin. Vulnerabilities that have been accepted are still identified by a scan, but hidden in the results of the scan. For risks that require remediation, a risk assessment process should be followed.

A risk assessment is a systematic process of identifying and evaluating identified risks that may impact organisations operations or assets. There are five main steps to performing a risk assessment: Identification of the hazards, Assessing the risks, Controlling the risks, Recording the findings, and Reviewing the controls. Once the vulnerabilities have been identified, the organisation needs to assess the identified risks, and prioritise the remediation efforts. Vulnerabilities should be assessed on their potential impact, and strategies should be developed to mitigate or manage these risks effectively.

Risk assessments are critical for helping organisations make informed decisions, prioritising resources, and proactively managing risks, while minimising potential negative impacts. While the vulnerability management section deals specifically with identification aspects, this section provides guidance to organisations on how to assess and prioritise risks which have been identified within the environment.

Prioritising Risk with ACR, AES, and VPR

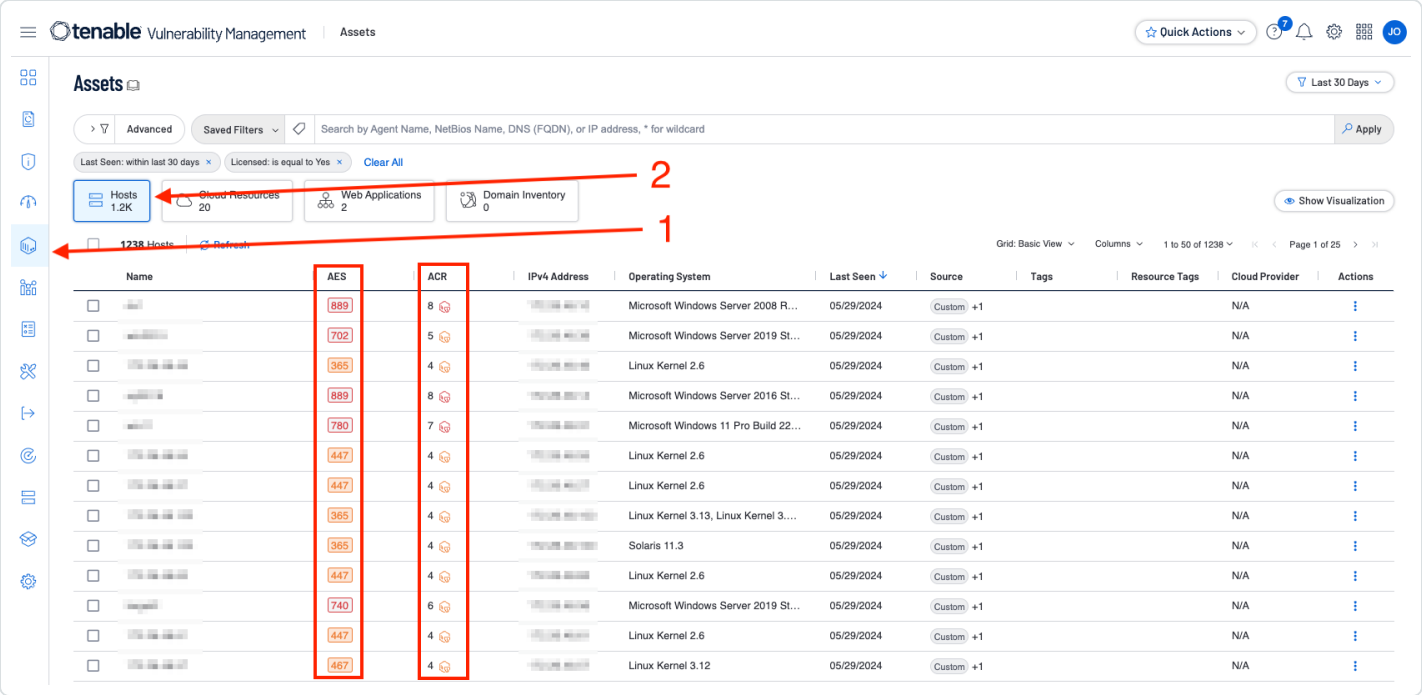
When dealing directly with assets, Tenable assists organisations prioritise risk by assigning an Asset Criticality Rating (ACR), and Asset Exposure Score (AES). When dealing with vulnerabilities a Vulnerability Priority Rating (VPR) is assigned. The ACR establishes the priority of each asset based on 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 organisation's most critical and carry the greater business impact if compromised.

Critical	High	Medium	Low
9-10	7-8	4-6	1-3

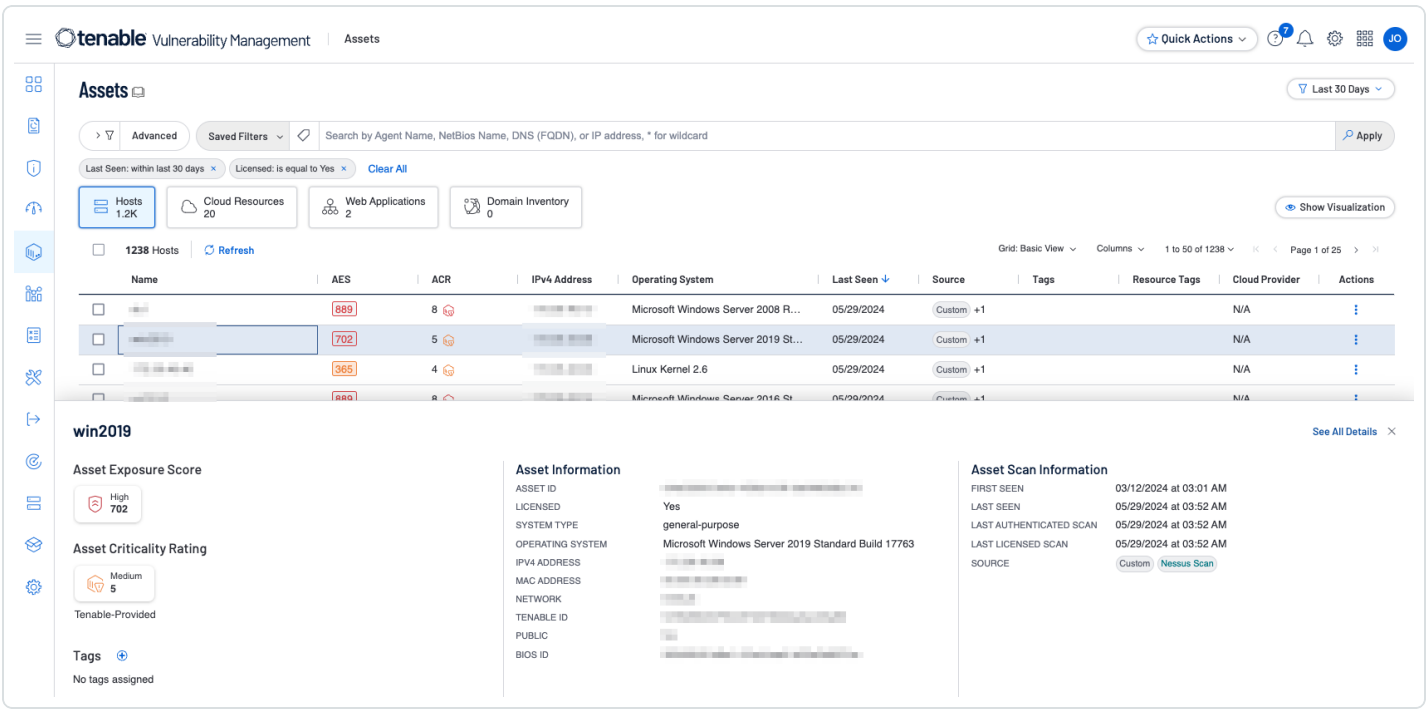
Asset Exposure Score (AES) is also calculated for licenced assets. Asset Inventory calculates a dynamic AES for each asset on your network to represent the asset's relative exposure as an integer between 0 and 1000. The AES is a calculated integer using both ACR and the asset level VPR. A higher AES indicates higher exposure, as the following chart converts the AES number to a severity rating.

High	Medium	Low
650-1000	350-649	0-349

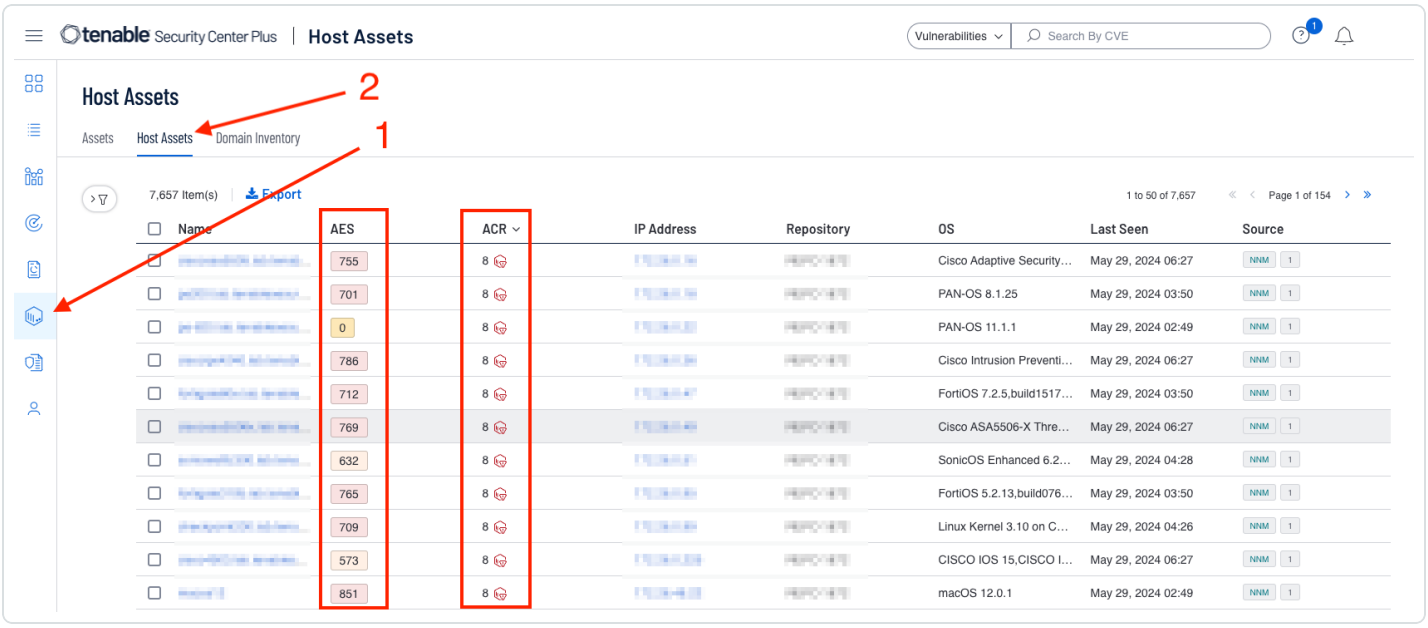
To view the ACR or AES information for any asset within Tenable Vulnerability Management, Navigate to the **Assets** page.



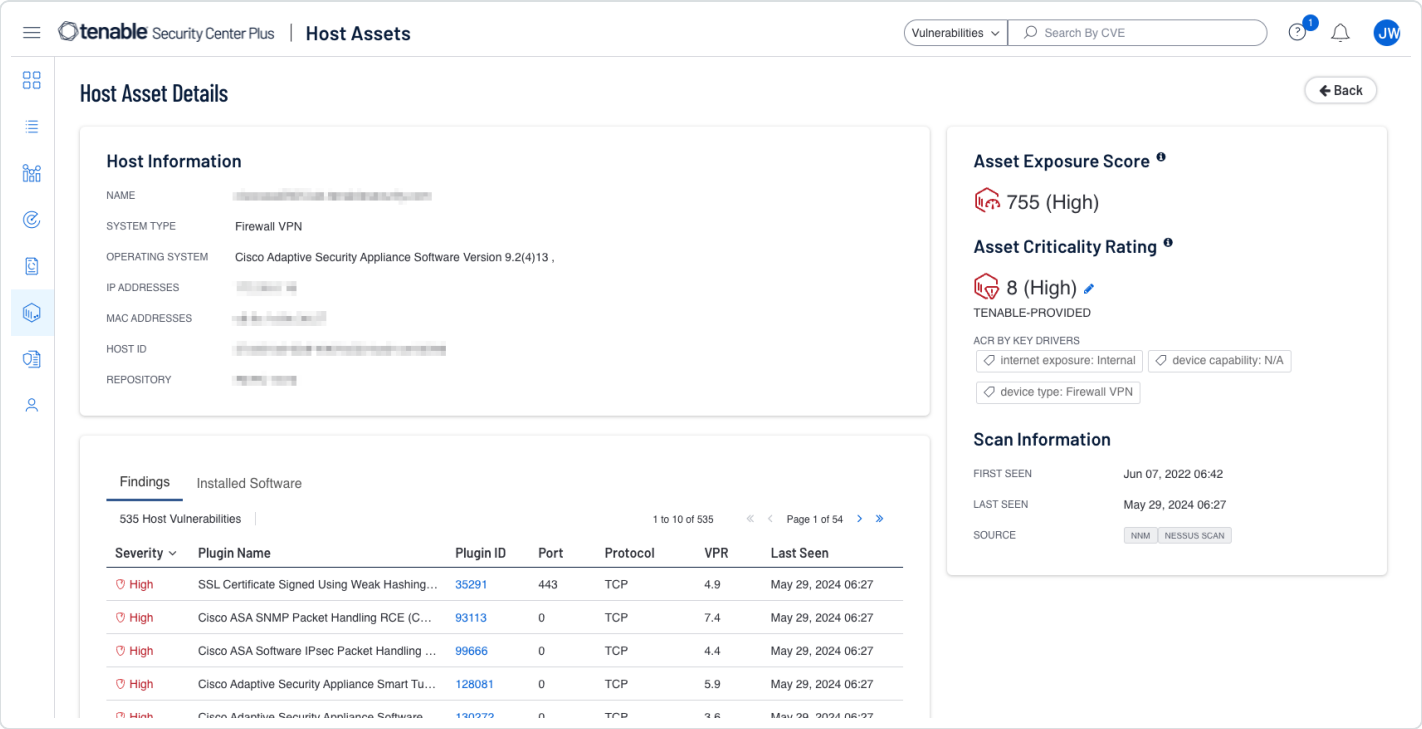
Select an **asset** to view the asset details.



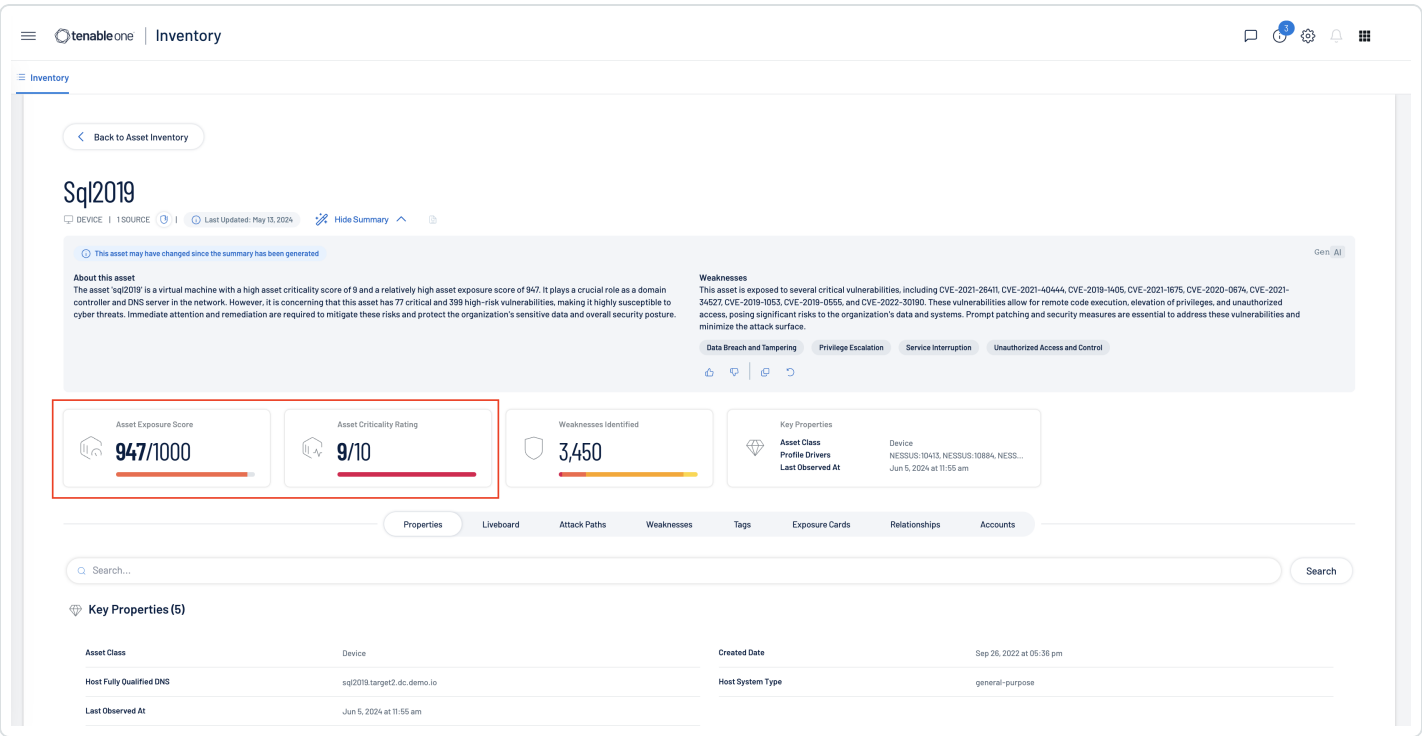
To view the ACR or AES information for assets within Tenable Security Center the process is similar. Navigate to the **Assets** page, then select Host Assets. A list of assets will be displayed along with their associated ACR and AES scores.



Select an asset to view the asset details.



Within Tenable One, AES and ACR can be best viewed from the See **Details** link on the **Assets** page.



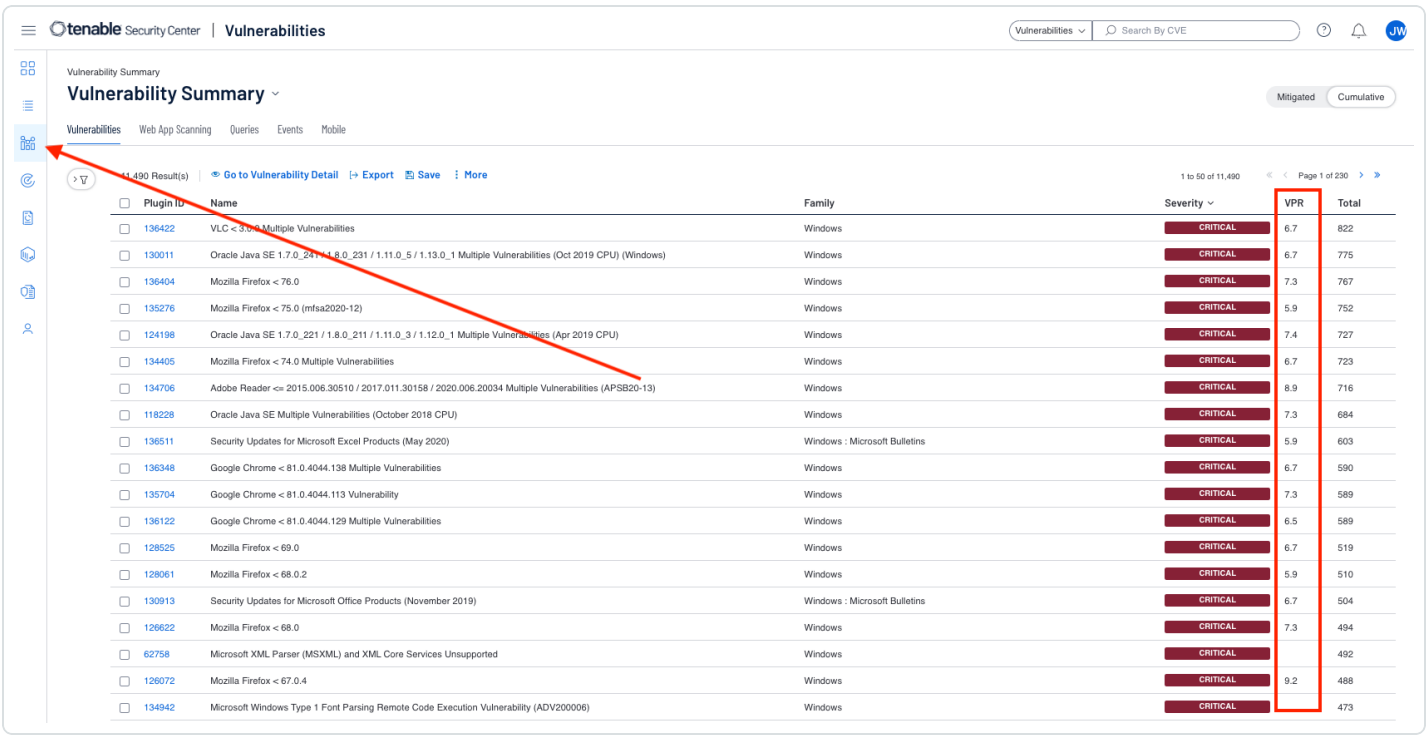
AES and ACR scores are attributed to assets. A Vulnerability Priority Rating (VPR) is associated with the vulnerabilities themselves. If the organisation is familiar with the Common Vulnerability Scoring

System (CVSS), the VPR score is similar to the CVSSv3 impact subscore. VPR is a unique vulnerability severity rating in that the rating can change over time. Tenable updates a vulnerability's VPR score daily to reflect the current threat landscape. VPR ranges are values from 0.1-10, with the highest value representing a higher likelihood of exploitation. VPR severity ratings cannot be edited or customised. VPR scores are derived from seven key drivers:

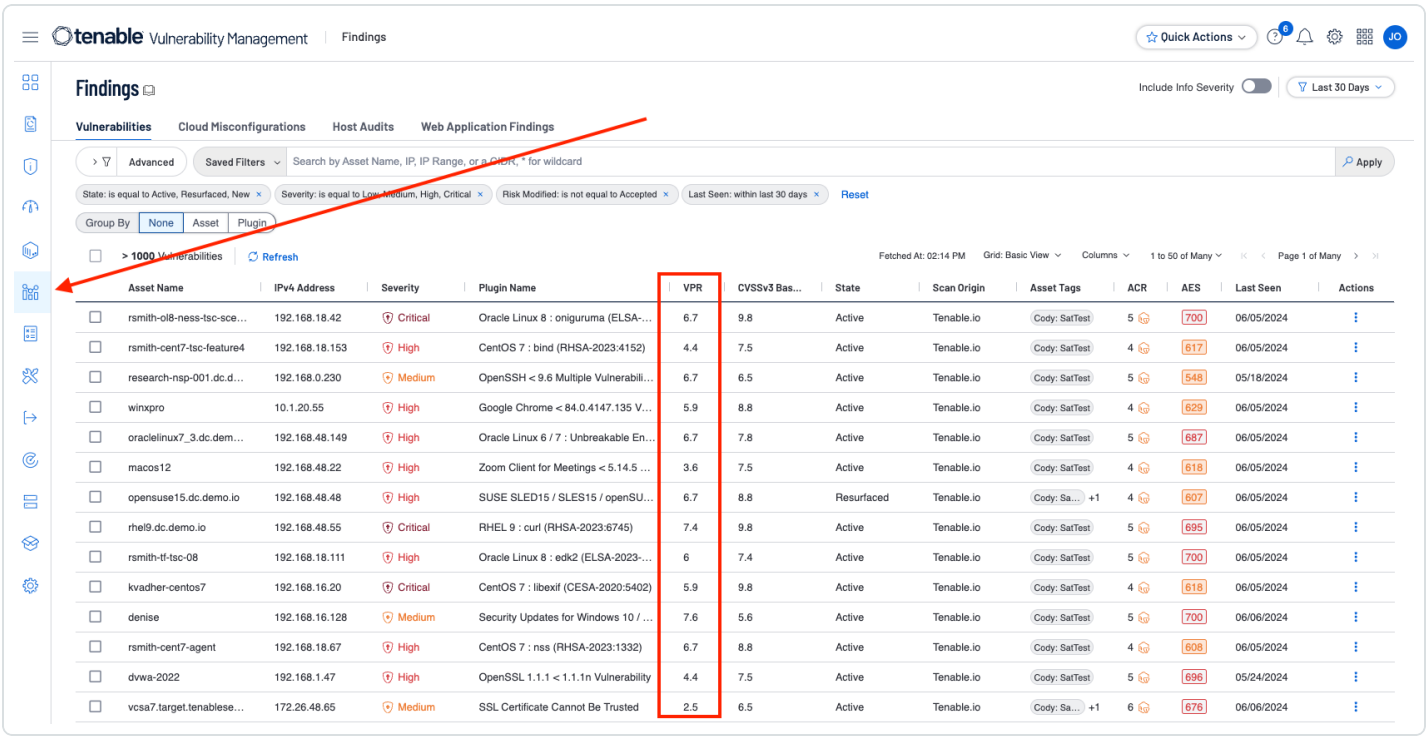
- Age of Vulnerability: - The number of days since the National Vulnerability Database (NVD) published the vulnerability.
- CVSSv3 Impact Score - The NVD-provided CVSSv3 impact score for the vulnerability. If the NVD did not provide a score, Tenable Vulnerability Management displays a Tenable-predicted score.
- Exploit Code Maturity - The relative maturity of a possible exploit for the vulnerability based on the existence, sophistication, and prevalence of exploit intelligence from internal and external sources (for example, Reversinglabs, Exploited, Metasploit, etc.). The possible values (High, Functional, PoC, or Unproven) parallel the CVSS Exploit Code Maturity categories.
- Product Coverage - The relative number of unique products affected by the vulnerability: Low, Medium, High, or Very High.
- Threat Sources - A list of all sources (for example, social media channels, the dark web, etc.) where threat events related to this vulnerability occurred. If the system did not observe a related threat event in the past 28 days, the system displays No recorded events.
- Threat Intensity - The relative intensity based on the number and frequency of recently observed threat events related to this vulnerability: Very Low, Low, Medium, High, or Very High.
- Threat Recency - The number of days (0-180) since a threat event occurred for the vulnerability.

VPR enhances traditional vulnerability ratings such as CVSS and Severity. The threat component reflects both recent and potential future threat activity against a vulnerability. Some examples of threat sources that influence VPR are public proof-of-concept (PoC) research, reports of exploitation on social media, emergence of exploit code in exploit kits and frameworks, references to exploitation on the dark web and hacker forums, and detection of malware hashes in the wild. Such threat intelligence is key in prioritising those vulnerabilities that pose the most risk to an organisation.

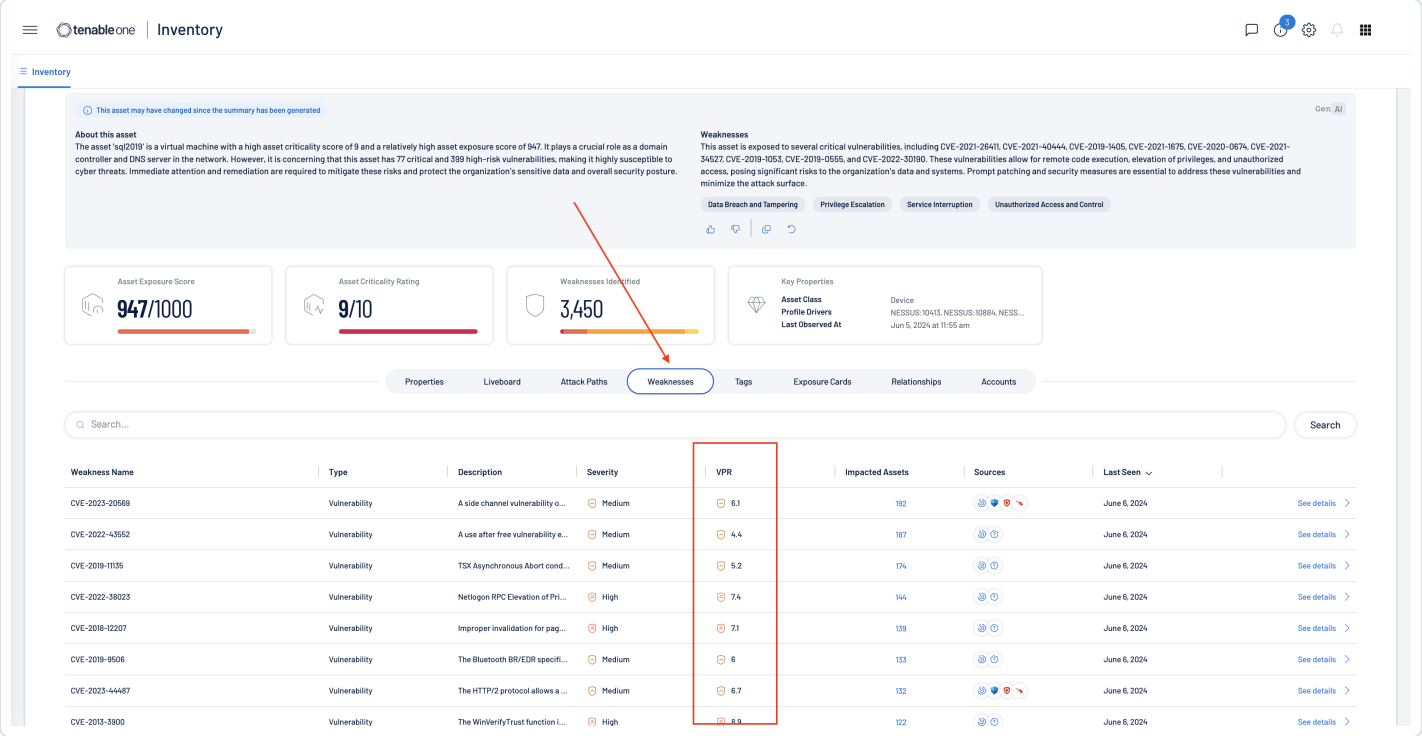
From within Tenable Security Center, VPR scores can be viewed from the **Analysis** tab.



From within Tenable Vulnerability Management, VPR scores can be viewed from the **findings** tab.



Tenable One VPR scores can be best viewed from the See Details link on the **Assets** page, and then by selecting Weakness.



Now that we have discussed AES, ACR, and VPR, along with their benefits, we can further enhance risk management with the Cyber Exposure Score (CES) The building blocks for the CES in the Tenable One Exposure Management Platform are similar to those used for years in Tenable products (for example, Tenable Vulnerability Management, Tenable Lumin). These mechanisms have to date only been used for vulnerability management data. Tenable One expands these concepts into new realms of the attack surface: Web Applications (Tenable Web App Scanning), Cloud Resources (Tenable Cloud Security), Tenable OT Security, and Identity (Tenable Identity Exposure).

The following concepts are foundational to the scoring utilised in Tenable One:

Vulnerability Priority Rating (VPR): The severity and exploitability of a given vulnerability. A vulnerability's VPR is expressed as a number from 0.1 to 10, with higher values corresponding to a higher likelihood of the vulnerability leading to a compromise and a higher impact on the asset. This score is found in Tenable Vulnerability Management.

Asset Criticality Rating (ACR): Rates the criticality of an asset to the organisation. An asset's ACR is expressed as an integer from 1 to 10, with higher values corresponding to the asset being more critical to the business. This score is utilised in Tenable Lumin.

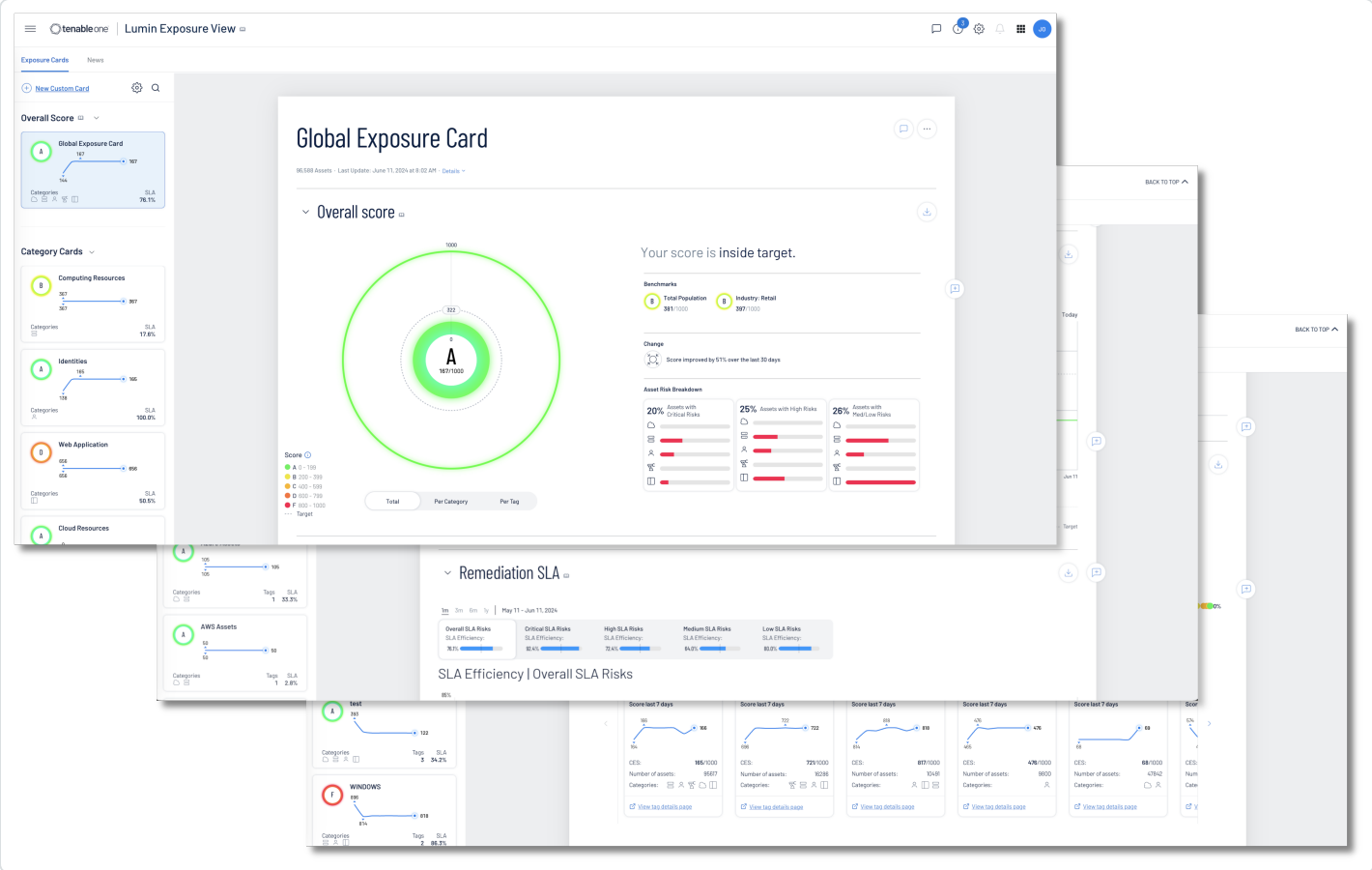
Asset Exposure Score (AES): A combination of the VPR and ACR of a given asset.

Prioritising Risk with Lumin Exposure View and Attack Path Analysis

Tenable Lumin Exposure View provides at-a-glance insight into all weaknesses and exposures. It combines data sources from all Tenable solutions, including IT assets, identity systems, cloud resources, web applications, and your OT infrastructure.

One of the hardest tasks to accomplish is proper risk prioritisation and communication of risks and vulnerabilities. Lumin Exposure View provides the exposure cards, which allows easy identification of problem areas so resources can be applied properly where needed. An exposure card represents incoming data from configured tags and data sources. This data is aggregated and normalised to provide a visual representation of your CES and other metrics. Note: Exposure cards can be customised or Tenable provided cards can be used.

The CES is presented under the letter grade, in the form of a number such as 167/1000. The CES score is a value from 0-1000, with higher values indicating higher exposure and higher risk.



Follow this link for more information on Lumin Exposure View.

Tenable Attack Path Analysis gives security teams the ability to take the attackers perspective with context across the organisation. Analysts can easily browse an organisation's environment to understand relationships and exposures. This allows a physical view into the same combination of exposures that attackers can see, which lead to unwanted lateral movement into critical assets. Additionally, organisations can remove the guesswork of where to start first, identify and prioritise attack paths based on unique context, and stay up to date with common adversary Tactics, Techniques, and Procedures (TTPs) from MITRE ATT&CK.

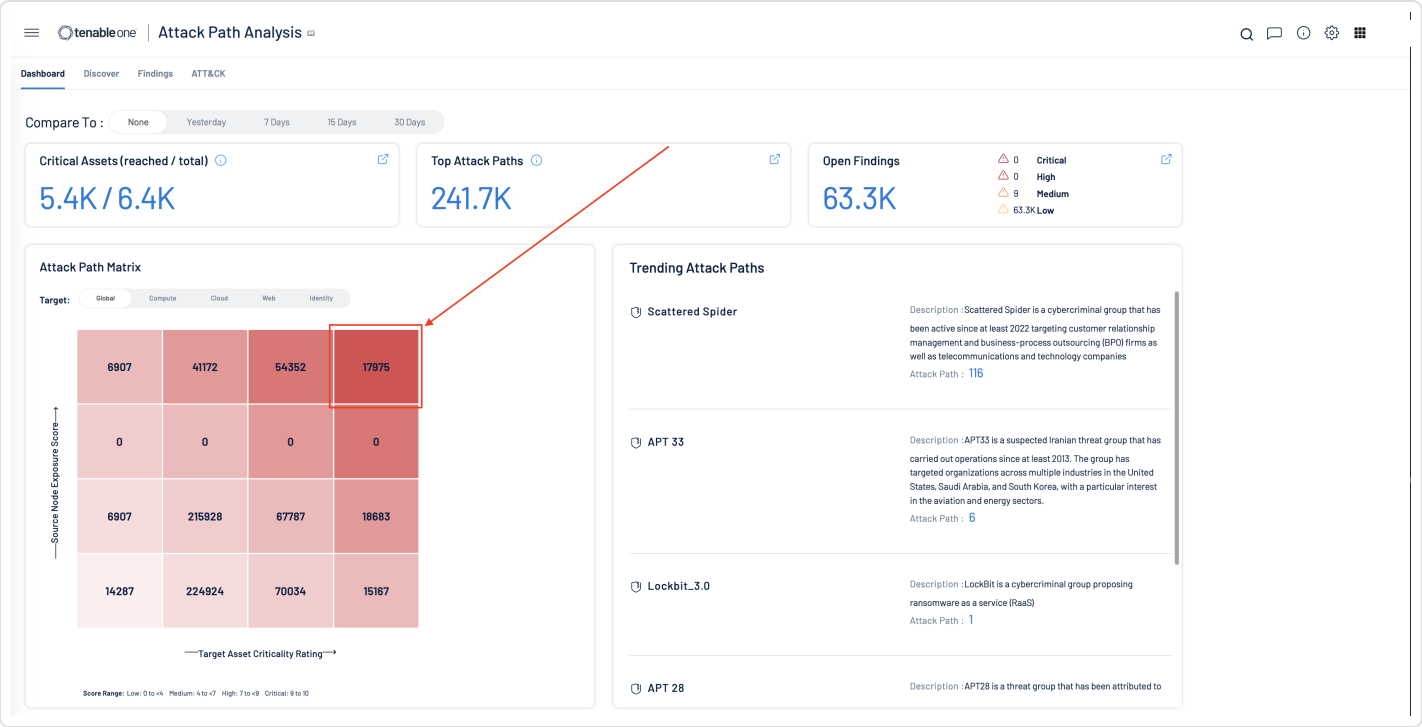
To achieve the best results a few criteria must be met:

- The percentage of authenticated Tenable Vulnerability Management scans and Web Application scans must be at least 40%.
- Tenable Identity Exposure must be configured
- A Tenable Cloud Security resource must have been performed.

For more information, see Get Started with Attack Path Analysis

Attack Path Analysis anticipates and prioritises the most critical attack paths within the environment by leveraging advanced threat intelligence and analytics. By leveraging the power of artificial intelligence, Attack Path Analysis delivers guidance based uniquely on the organisation's environment. By maintaining the relationship between assets, vulnerabilities, and potential attack paths, organisations can stay ahead of threats, and respond quickly to threats using step-by-step recommendations that are provided.

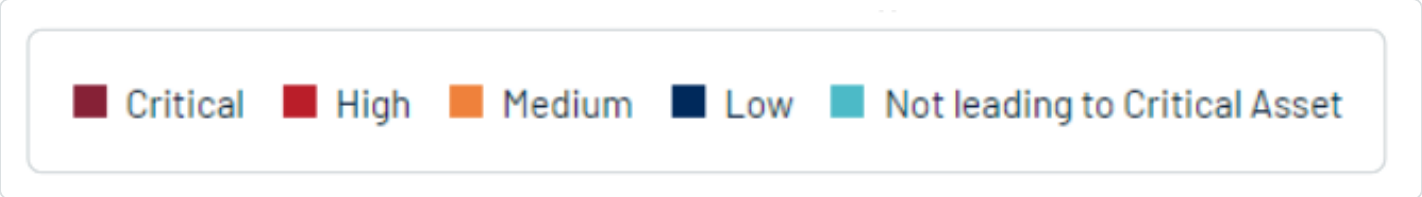
From the dashboard in **Attack Path Analysis**, selecting a cell (in this case the cell in the upper right reflects the most critical, combined highest exposure score and asset criticality rating), takes the user to the **Discover** page.



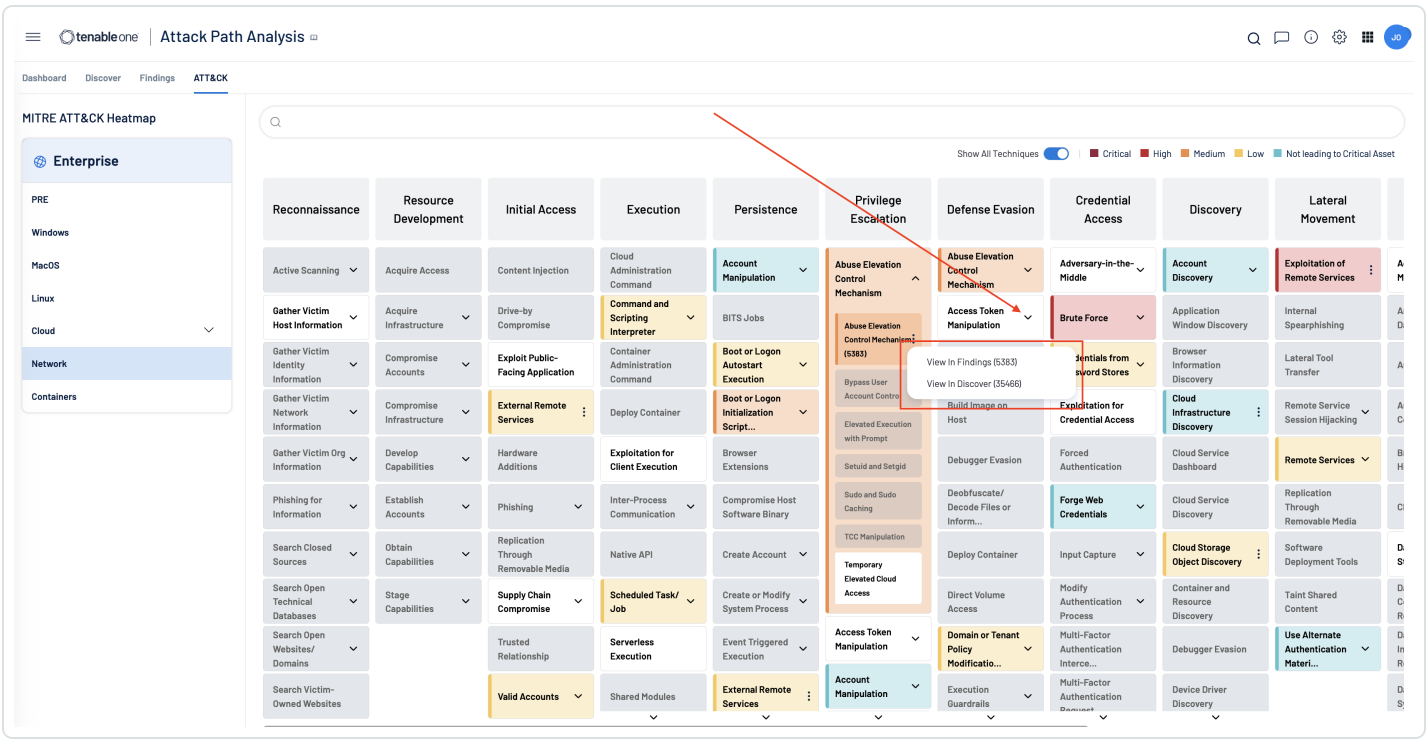
Selecting the ATT&CK page displays the MITRE Att&ck Heatmap. The heatmap provides a holistic view of the organisation's data based on the enterprise tactics and techniques from MITRE Att&ck. The data is presented in a table format which allows organisations to quickly prioritise and remediate critical vulnerabilities that are the most relevant to your organisation.

Table cells are colour-coded to indicate:

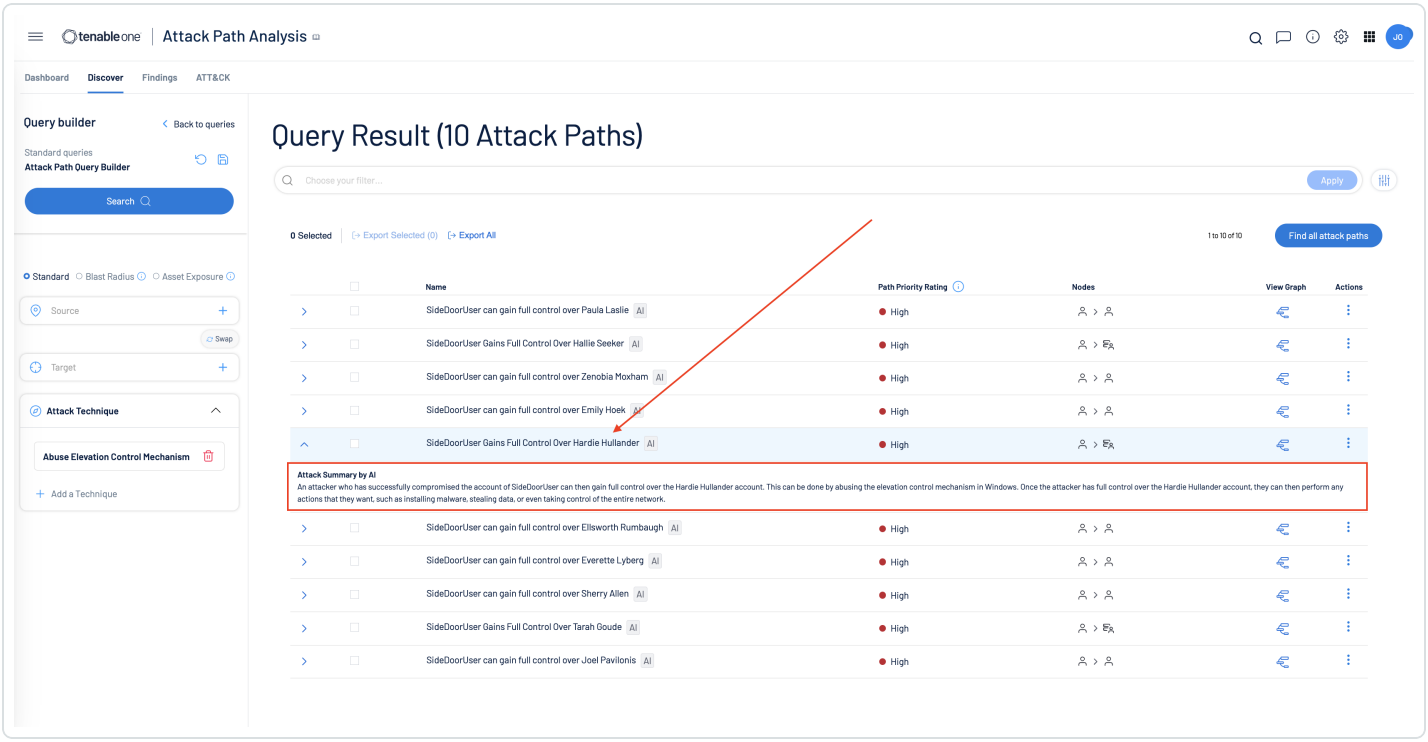
- Grey - Tenable does not currently support these techniques
- White - Tenable supports and detects these techniques, however they are not relevant to your organisation.
- All other colours are based on severity:



Clicking the item displays options which can lead you back to the **Findings or Discover** page to view possible attack paths for the selected technique or sub-technique.



On the **Discover** page, clicking on one of the displayed attack paths display an attack summary explaining the attack path.



For a complete workflow example using Tenable Lumin Exposure View and Attack Patch Analysis to prioritise risks, see this example workflow link.

For more information related to Attack Path Analysis, see this link.

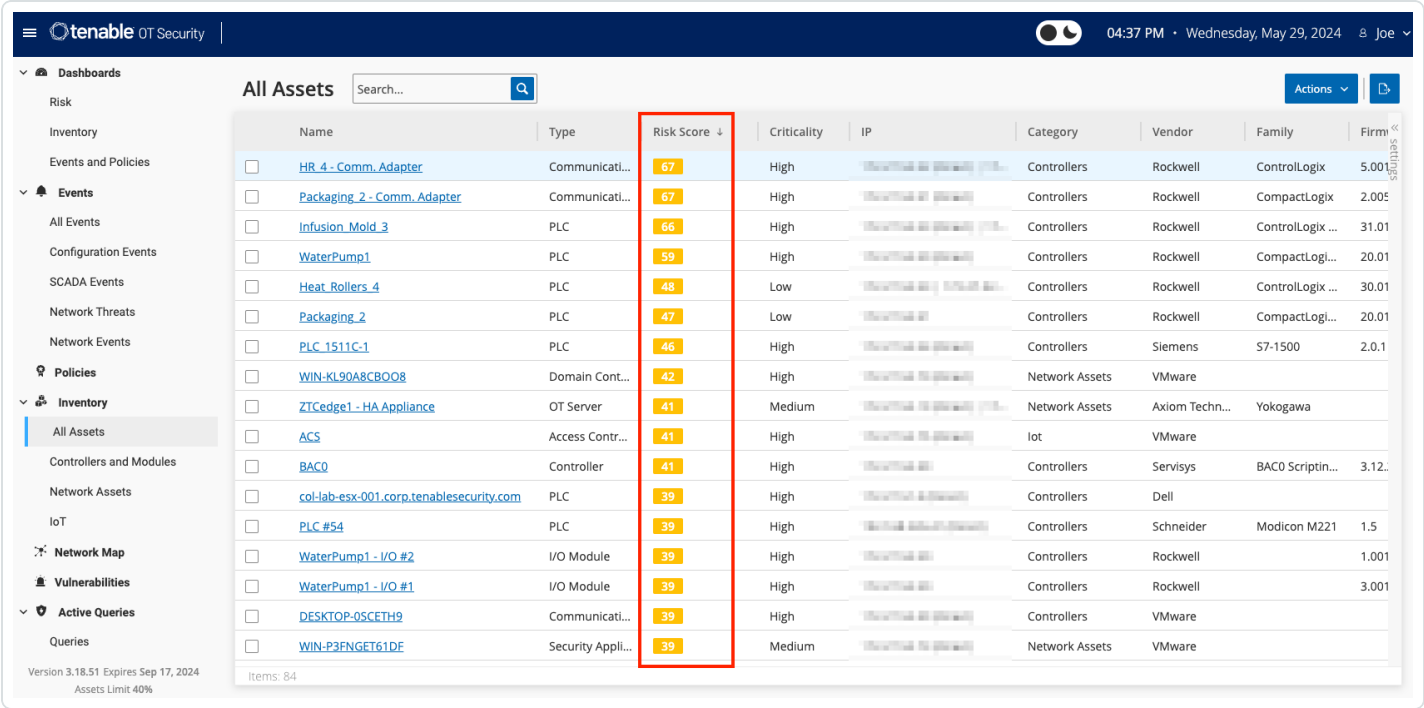
Tenable OT Security applies sophisticated algorithms to assess the degree of risk posed to each asset on the network. A Risk Score (from 0 to 100) is given for each Asset in the network. The Risk score is based on the following factors:

- Events — Events in the network that affected the device (weighted based on Event severity and how recently the Event occurred). Note: Events are weighted according to currency, so that more recent Events have a greater impact on the Risk score than older Events.
- Vulnerabilities — CVEs that affect assets in your network, as well as other threats identified in your network (for example, obsolete operating systems, usage of vulnerable protocols, vulnerable open ports, and so on.). In the OT Security, these are detected as plugin hits on your assets.
- Asset Criticality — A measure of the importance of the device to the proper functioning of the system.

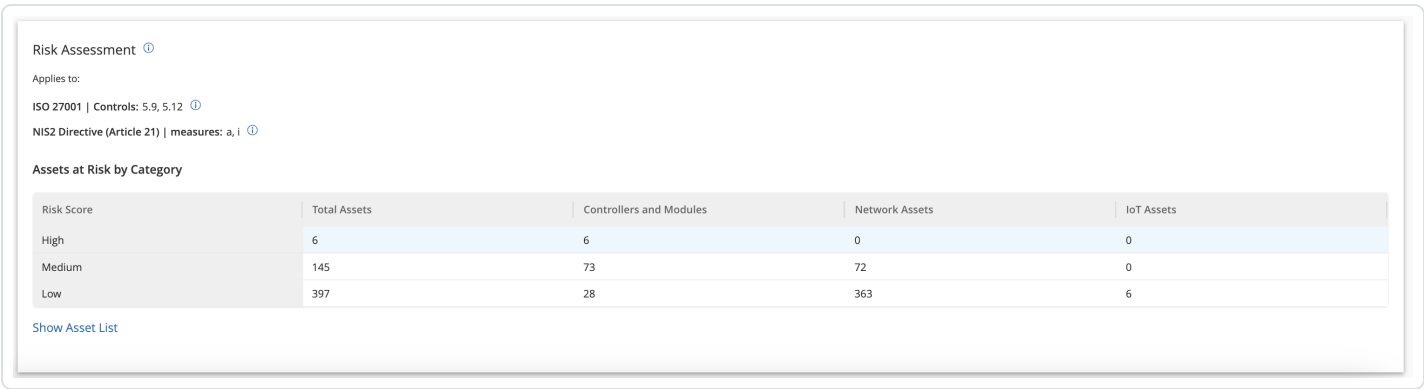
> **Note**: For PLCs that are connected to a backplane, the Risk score of other modules that share the backplane affect the PLC's Risk score.

The Risk Score can be viewed in several ways.

- All three dashboards (Risk, Inventory, Events, and Policies)
- All four inventory dashboards (All Assets, Controllers and Modules, Network Assets, IoT)



The Risk Assessment widget for Tenable OT, located on the compliance dashboard provides organisations with an updated and dynamic overview of at-risk assets by their criticality. Displaying assets by criticality assists organisations in prioritising and managing risks related to the OT/IoT environment. Key items displayed are assets with High, Medium, Low vulnerabilities and assets at high risk.



The External Exposure Risk widget also for Tenable OT, located on the compliance dashboard identifies external connections to the Industrial Control Systems (ICS) networks. This widget assists organisations meet compliance within supply chain security. As more vendors (both ICS equipment and machine builders) are using hybrid models. These hybrid models may reside in or out of cloud environments. This widget assists organisations identify, evaluate, and mitigate OT network, and IoT assets from unexpected external communication.

External Exposure Risk

Applies to:

ISO 27001 | Controls: 5.15

NIS2 Directive (Article 21) | measures: a, i

Assets with potential external exposure risk

Risk Type	Purdue Level 0-1 Assets	Purdue Level 2-3 Assets
External Connection	0	0

The following cross-reference information is provided to derive a more comprehensive and effective approach to managing information security requirements. NIS 2 Article 21(2)(a) references security in Risk Analysis and Information System Security.

Security domains define how information is classified, categorised, or administered. The following Security Domains, Sub-Domains, and Measures are related to NIS 2 Article 21(2)(a), and can assist organisations already using other standards and frameworks to comply with NIS 2.

SECURITY DOMAIN: Defence

SECURITY SUB-DOMAIN: Detection

SECURITY MEASURE: Detection

In an effort to foster higher consistency and reliability across multiple frameworks and the NIS 2, Article 21(2)(a) can be associated with the ISO 27001, NIST CSF, and ISA/IEC 62443 utilising the following cross-references for risk analysis. The following cross-references cover the processes and procedures related to Risk Analysis, Defense, and Detection.

CROSS REFERENCES:

The ISO 27001 references sections within Performance Evaluation, specifically the following sections:

- ISO 27001(9.1, A.12.2, A.12.4, A.12.6.1, A.15.2.1)

The NIST CSF references the following sections within Detect, and Protect.

- NIST CSF (PR.DS -6, 8, DE.AE -1,5, DE.CM -1, 2, 3, 4, 5, 6 7, DE.DP – 1, 2, 3, PR.PT -1)

The ISA/IEC 62443 references the following sections within Policies and Procedures, Systems, Zone Boundary Protection, Application Partitioning, Audit Logs, and Continuous Monitoring.

- ISA/IEC 62443 (SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.1, SR 3.3, SR 3.4, SR 3.8, SR 3.9, SR 5.1, SR 5.2, SR 5.4, SR 6.1, SR 6.2)

Additionally, the following cross-references are also related to Security Risk Analysis and should be considered as a reference within governance.

SECURITY DOMAIN: Governance and Ecosystem

SECURITY SUB-DOMAIN: Information System Security Governance & Risk Management

SECURITY MEASURE: Information system security risk analysis

In an effort to foster higher consistency and reliability across multiple frameworks and the NIS 2, Article REPLACE can be associated with the ISO 27001, NIST CSF, and ISA/IEC 62443 utilising the following cross-references for vulnerability handling and disclosure. The following cross-references cover the processes and procedures related to Risk Analysis and Governance and Ecosystem.

CROSS REFERENCES:

The ISO 27001 references sections within Planning, Operation, Performance Evaluation, and Improvement, specifically the following sections:

- ISO 27001 (6, 8, 9.3,10, A.8.1.1, A.12.6.1, A.18.2.1)

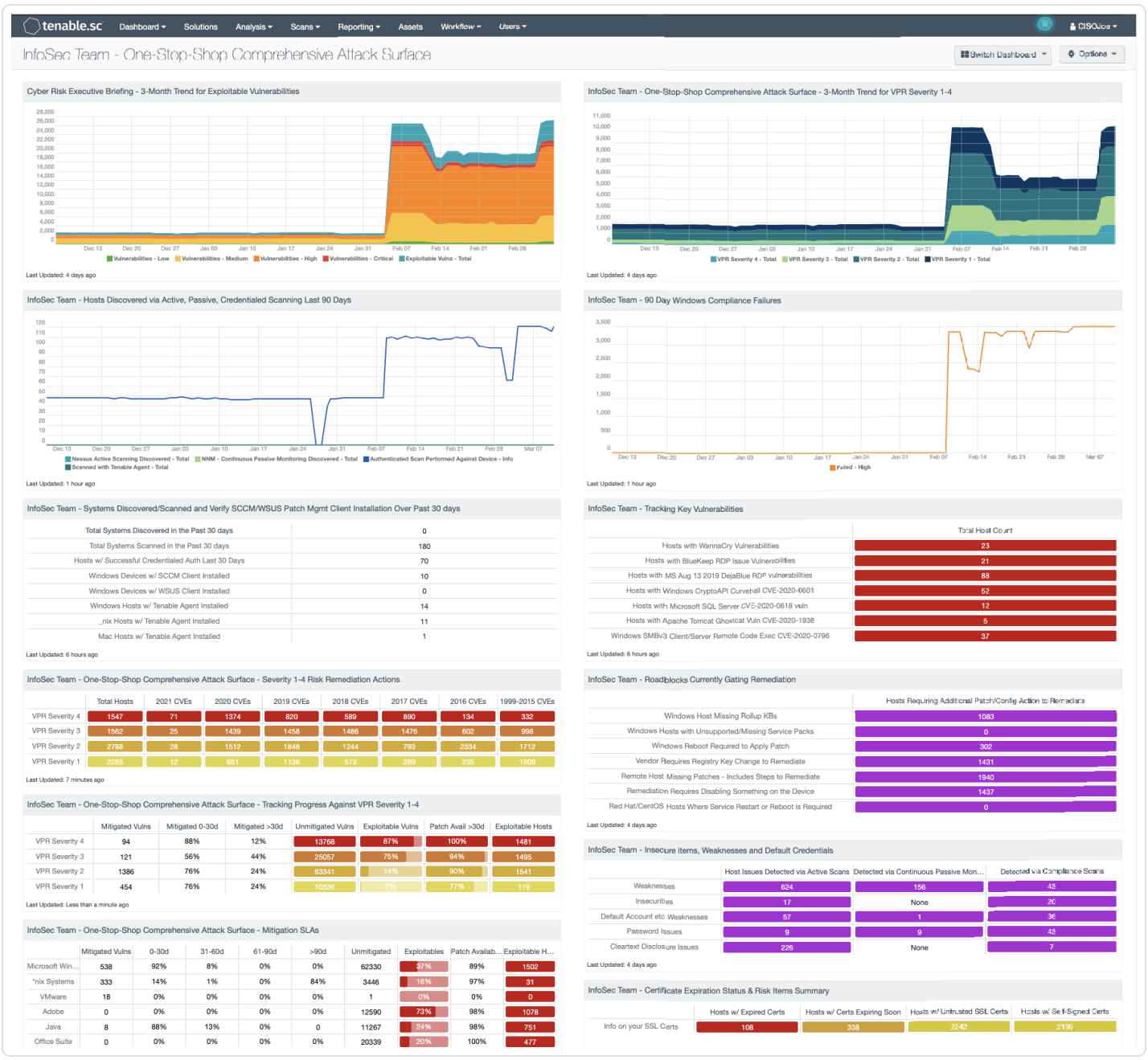
The NIST CSF references the following sections within Identify, Respond, Detect, Recover, and Protect.

- NIST CSF (ID.GV -4, ID.RA-1, 3, 4, 5, 6, ID.RM-1, 2, 3, RS.IM -1, 2, ID.SC -1, 2, PR.IP 12, RC.IM -1, 2, ID.AM -1, 2, 4, 5, DE.CM -8, RS.MI -3, RS.AN -5)

The ISA/IEC 62443 references the following sections within the Control Systems Component Inventory.

- ISA/IEC 62443 (SR 7.8)

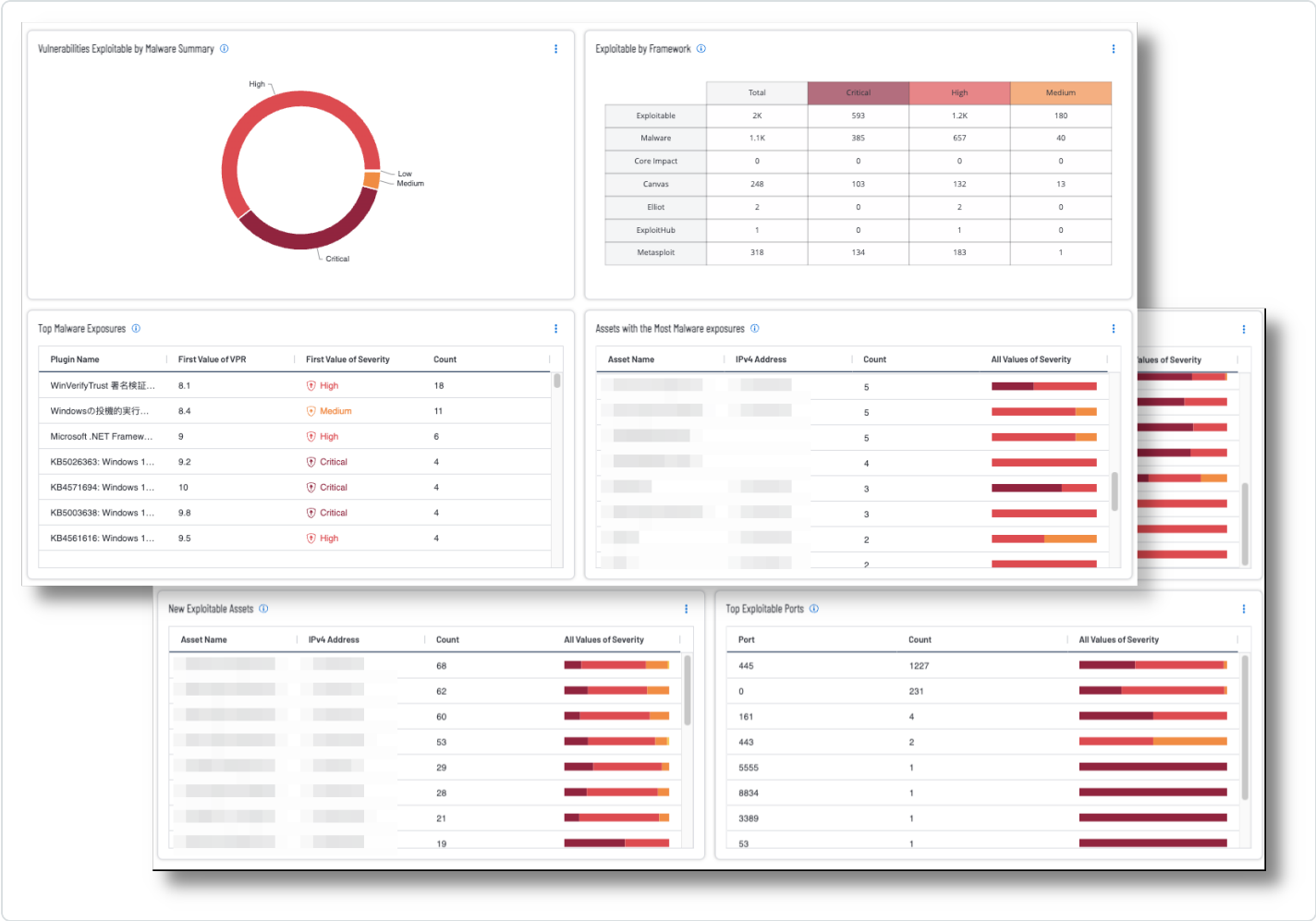
Organisations often have teams that focus on the detailed information relevant to the teams' assets; or operational focus areas, such as Windows, Linux, databases, or network infrastructure. The [InfoSec Team – One-Stop Shop Comprehensive Attack Surface dashboard](), shown in the following image, contains components that do not require specific asset list filters to be applied before use. The following dashboards provide a unique risk perspective to organisations across their entire environment, enabling quick and easy vulnerability prioritisation.



The Cyber Security Framework (CSF) category ID.RA (Risk Assessment) provides guidance to organisations on cyber risk and helps to define recommended actions for the security operations team. The ID.RA-1 category states requirements for the National Institute of Standards and Technology (NIST) 800-53 control CA-8 Penetration Testing. The control states 'Penetration testing is a specialised type of assessment conducted on information systems or individual system components to identify vulnerabilities that could be exploited by adversaries.' Some security teams leverage exploitation frameworks such as Core Impact, Canvas, or others to help with this control. Tenable Vulnerability Management identifies which vulnerabilities are exploitable by different

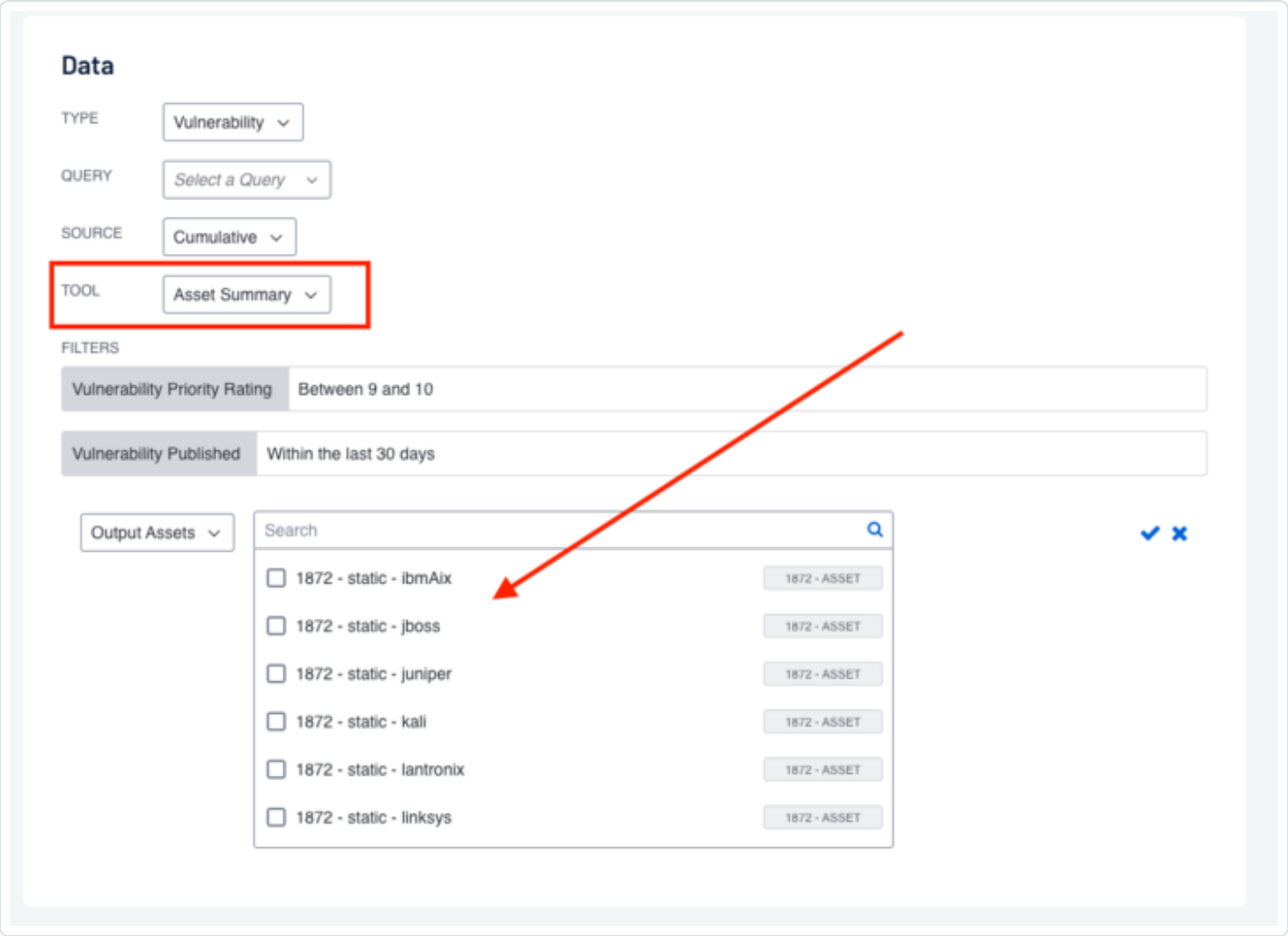
frameworks. Exploit frameworks do not always have the same exploits, and, while there may be some overlap, a correlated view of exploits in the environment from multiple frameworks helps organisations understand which exploit frameworks pose the greatest threat.

For Tenable Vulnerability Management, **the Pen Testing Team: One-Stop-Shop** dashboard provides security operations teams a centralised view of common vulnerabilities and exploit frameworks present in the organisation's environment.

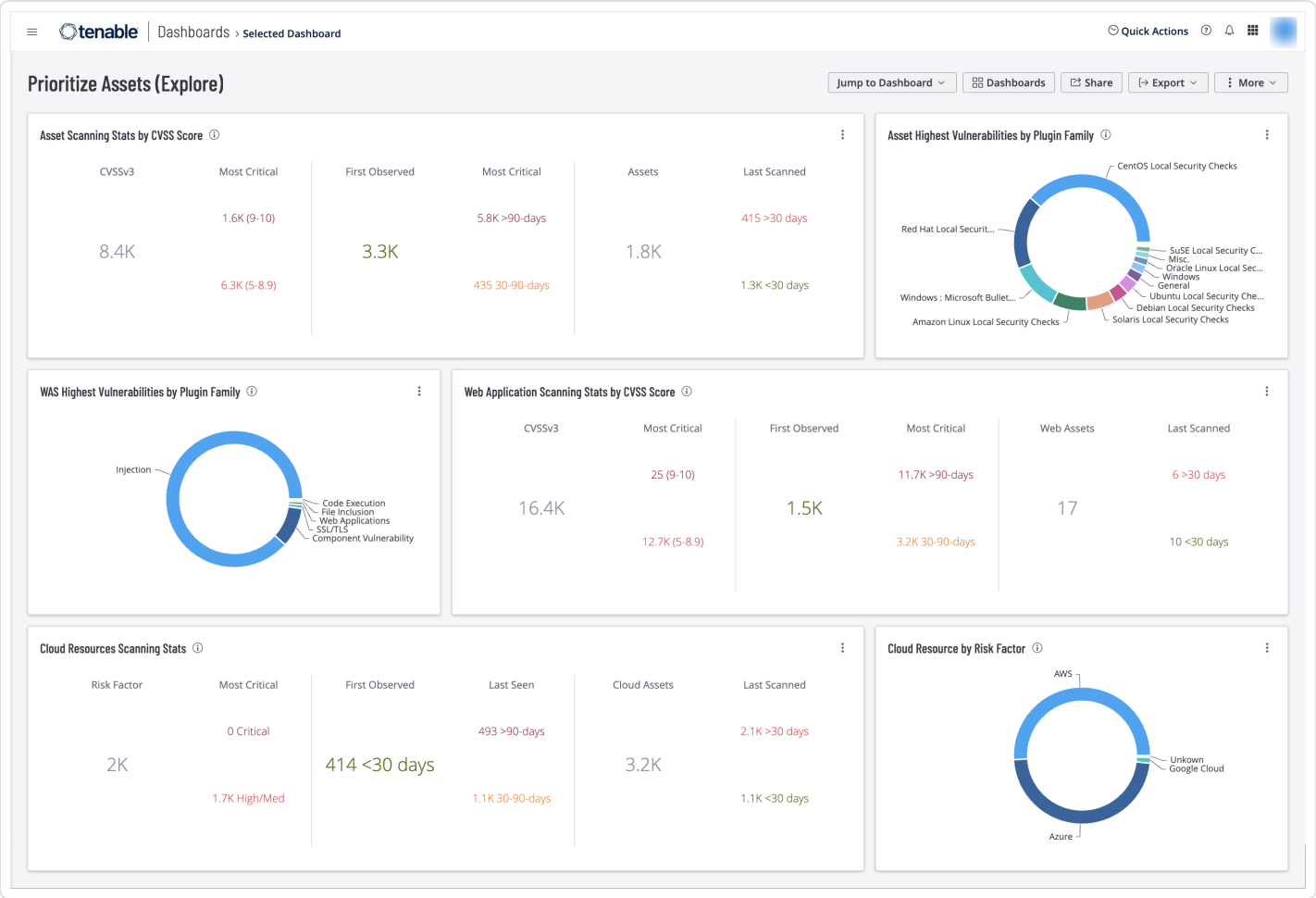


However, organisations with teams that focus on a specific group of assets benefit from using custom asset lists. Information security teams can visualise findings against assets that are "owned by" or "assigned to" specific teams within the organisation using this method. Additionally, an Output Assets filter can be set to provide greater insight into where additional resources need to be allocated to mitigate vulnerabilities.

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.



The **Prioritise Assets** dashboard for Tenable Vulnerability Management helps prioritise remediation efforts by presenting lists of assets to prioritise in various categories. The widgets on this dashboard leverage vulnerability information from Tenable Web Application Security (WAS), Tenable.cs, and Tenable.io Vulnerability Management (Nessus, NNM).



The data presented closes the gap in awareness for security teams and enables system administrators to prioritise patch cycles and coverage in mitigation strategies. Security teams can add target groups to the dashboard template, allowing different asset managers to prioritise remediation efforts on the risk to their specific areas of concern. System administrators can take the same dashboards as actionable items to help set the priority of corrective actions and mitigation strategies.

The Worst of the Worst dashboards for Tenable Security Center and Tenable Vulnerability Management enables customers building or strengthening a vulnerability management program to better visualise the modern attack surface. The information presented focuses on the vulnerabilities that organisations should prioritise and mitigate first, by leveraging the Vulnerability Priority Rating (VPR). The VPR score is an output of Predictive Prioritization, which allows organisations to focus on what matters first by combining research insights, threat intelligence, and vulnerability rating to reduce noise. Effective vulnerability remediation becomes easier as vulnerabilities that cause the most significant impact float to the top. VPR ratings can change over

time, as threat intelligence information changes. Again, allowing teams to focus on what is important right now.

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

Worst of the Worst - FIX THESE FIRST

Switch Dashboard Options

Worst of the Worst - Reduce Greatest Risk First

	Vuln Count
All Vulnerability Instances	150465
Exploitable Vulnerabilities	39700
Remotely Exploitable, Low Complexity, No Authentication Required Vulns	16550
And Tenable VPR Score is 9-10 - FIX THESE FIRST	3525

Last Updated: 43 minutes ago

Worst of the Worst - Top 10 Prioritized Actions

Solution	Risk Reduction
Apply the appropriate patch according to the January 2021 Oracle Critical Patch Update advisory.	31.69%
Upgrade to Mozilla Firefox version 86.0 or later.	20.06%
Upgrade to Adobe Flash Player version 32.0.0.445 or later.	9.44%
Upgrade to Adobe Reader version 2017.011.30188 / 2020.001.30018 / 2020.013.20074 or later.	8.09%
Apply KB4601349: Windows 8.1 and Windows Server 2012 R2 February 2021 Security Update	4.77%
Upgrade to Adobe Acrobat version 2017.011.30188 / 2020.001.30018 / 2020.013.20074 or later.	4.18%

Last Updated: 44 minutes ago

Worst of the Worst - Top 10 Must Remediate Vulnerabilities

Name	Severity	VPR	Total
Oracle Solaris Critical Patch Update : oct2020_SRU11_4_24_75_2	Critical	10.0	2
Oracle Solaris Critical Patch Update : oct2020_SRU11_3_36_23_0	Critical	10.0	2
Solaris 10 (sparc) : 153074-01	Critical	10.0	3
Windows DNS Server RCE (CVE-2020-1350)	Critical	10.0	6
Microsoft DNS Server Remote Code Execution (SIGRed)	Critical	10.0	4

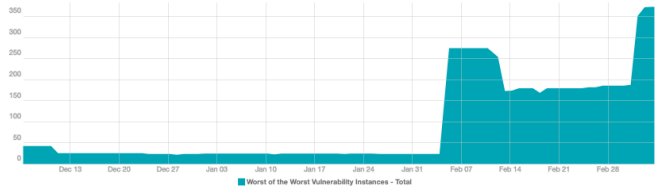
Last Updated: 44 minutes ago

Worst of the Worst - 10 Most Vulnerable Assets

IP Address	DNS	OS CPE	Score	Vulnerabilities
[redacted]	[redacted]	cpe:/o:microsoft:windows_8_1::gold	1400	35
[redacted]	[redacted]	cpe:/o:microsoft:windows_8_1::gold	1400	35
[redacted]	[redacted]	cpe:/o:microsoft:windows_server_2012	1160	29
[redacted]	[redacted]	cpe:/o:microsoft:windows_8::gold	1040	26
[redacted]	[redacted]	cpe:/o:microsoft:windows_8::gold	1040	26
[redacted]	[redacted]	cpe:/o:microsoft:windows_10	880	22

Last Updated: 44 minutes ago

Worst of the Worst - 90 Day Vulnerability Trend



Last Updated: 5 days ago

Worst of the Worst - OS/Application/No CPE Vulnerabilities

	VPR > 9	VPR < 9
Apps Only	2763	6255
OS Only	432	165
OS & Apps	229	136
No CPE	0	35

Last Updated: 5 days ago

Worst of the Worst - New Vulnerabilities Published Last 30 Days

Name	Severity	VPR	Total
VMware vCenter Server RCE (direct check)	Critical	9.8	5
VMware vCenter Server 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2021-0002)	Critical	9.8	5

Last Updated: 44 minutes ago

Worst of the Worst - By Asset

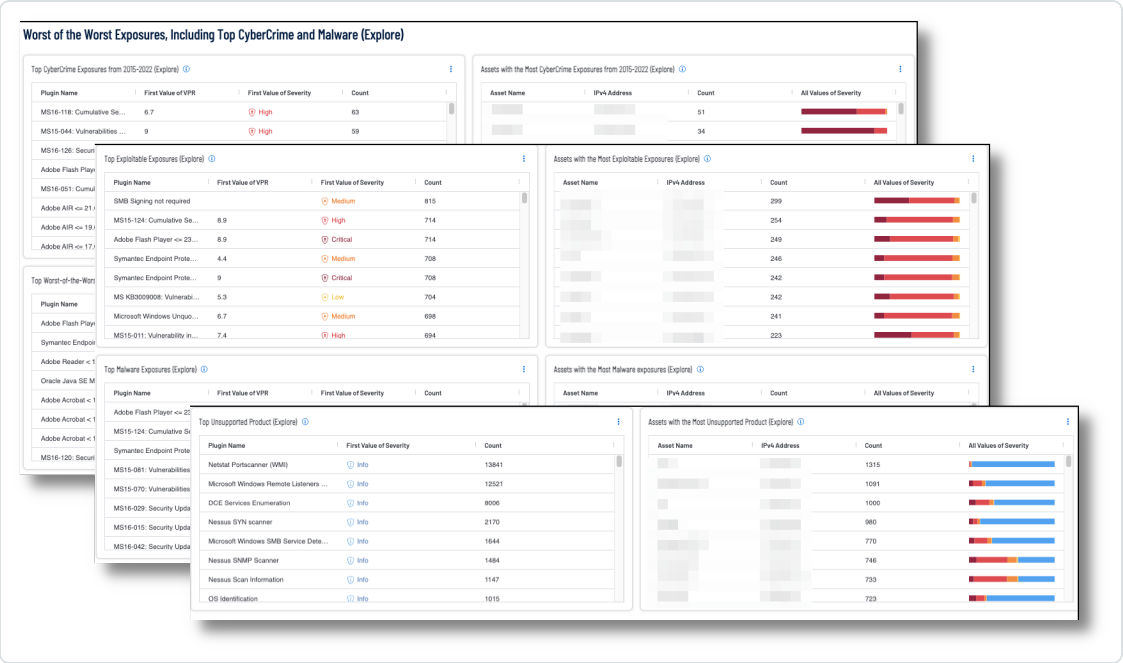
Asset	Total	Vulnerabilities	
Exploited by Malware	3444	2802	639
Systems with Software inventory	3438	2792	643
Windows Hosts	3408	2772	635
Systems that have been Scanned	3359	2744	612
Systems with authentication plugins present (Pass or Fail)	3291	2679	609

Last Updated: 44 minutes ago

Worst of the Worst - Certificate Concerns by Asset

Asset	Total	Vulnerabilities	
Systems that have been Scanned	745	77	668
SSL or TLS Servers	745	77	668
Systems with authentication plugins present (Pass or Fail)	719	70	649
Systems with authentication plugins present (Pass or Fail)	719	70	649
[redacted]	727	67	660

Last Updated: 44 minutes ago



Continuous Monitoring

Continuous monitoring is the real-time, or near real-time process of monitoring and analysing systems for vulnerabilities. The process is an ongoing assessment of the organisation's infrastructure, networks, and systems to detect and respond to threats. By continuously collecting and analysing information, organisations can identify issues early, mitigate risks, and improve the overall effectiveness of the cyber security program. Continuous monitoring helps to quickly identify vulnerabilities and potential breaches, helping organisations maintain a proactive approach to risk management.

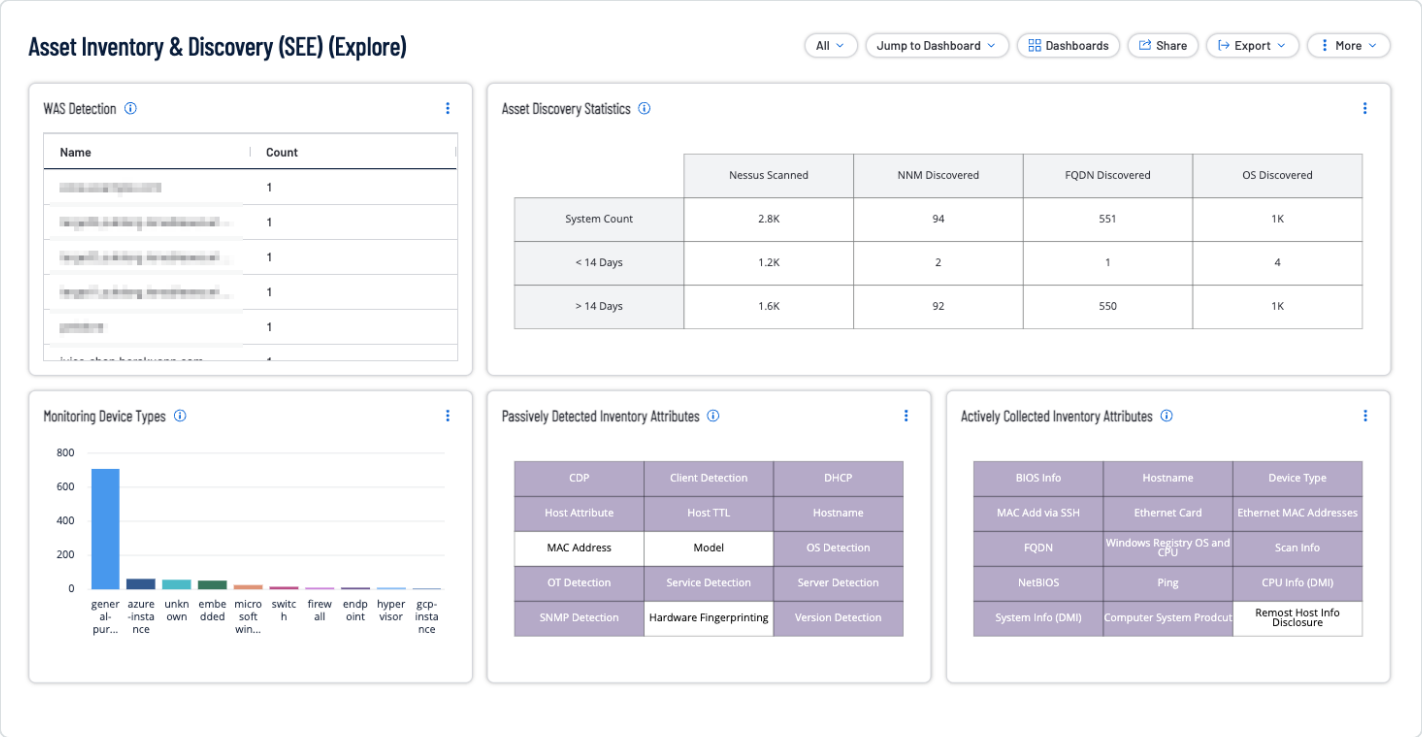
The following sections within the NIS 2 may be best suited to fall into the Continuous Monitoring category:

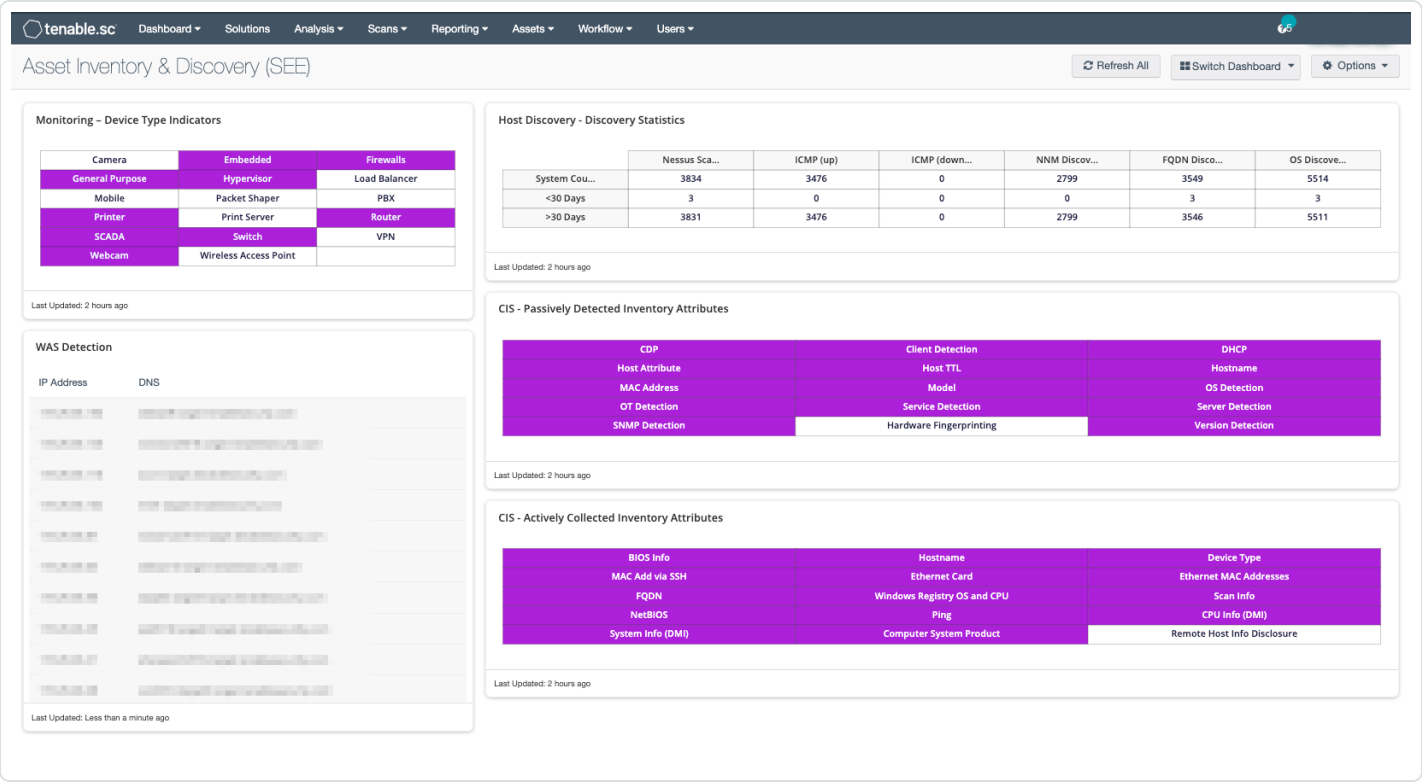
- Article 21(2)(c): Business Continuity: Business Continuity Process and Technology
- Article 21(2)(i): Access Control Policies and Asset Management: Asset Discovery and Access Control

A successful continuous monitoring program includes automated tools and techniques to monitor the organisation's infrastructure for vulnerabilities. These include using a vulnerability scanner to

scan networks, systems, and applications for known vulnerabilities, misconfigurations, or weak points that can be exploited.

Organisations must know the existence and location of critical assets to ensure that assets are monitored and protected based on each asset's business risk rating. Identifying assets facilitates vulnerability scanning and remediation by ensuring that scans are configured to probe for common weaknesses in the platform or application. Discovering all assets enables organisations to establish an inventory, which can be used to assess and mitigate associated risks to the organisation. **The Asset Inventory** and **Discovery** dashboards for Tenable Vulnerability Management and Tenable Security Center assist organisations with the continuous monitoring and identification of assets with the organisation.





The next steps include a vulnerability assessment, risk prioritisation, remediation, and patch management. The continuous monitoring program feeds data into these processes. Each of these steps has their own sections within this guide which focus on providing strategies which enable organisations to be successful in starting or maintaining their vulnerability management program. Continuous asset discovery is also an important aspect of continuous monitoring. For more information on Asset Discovery and Classification reference the Asset Inventory and Discovery Cyber Exposure Study.

In order to monitor for, and to identify vulnerabilities, meet guidelines/SLAs for timely remediation, compliance requirements, manage organisational assets, and proactively manage risks – continuous monitoring is an essential component of any comprehensive security strategy. For this section, the focus is on the first step, ensuring that the organisation's assets are being assessed on a regular basis. This can best be achieved by first ensuring that the scanning program is healthy.

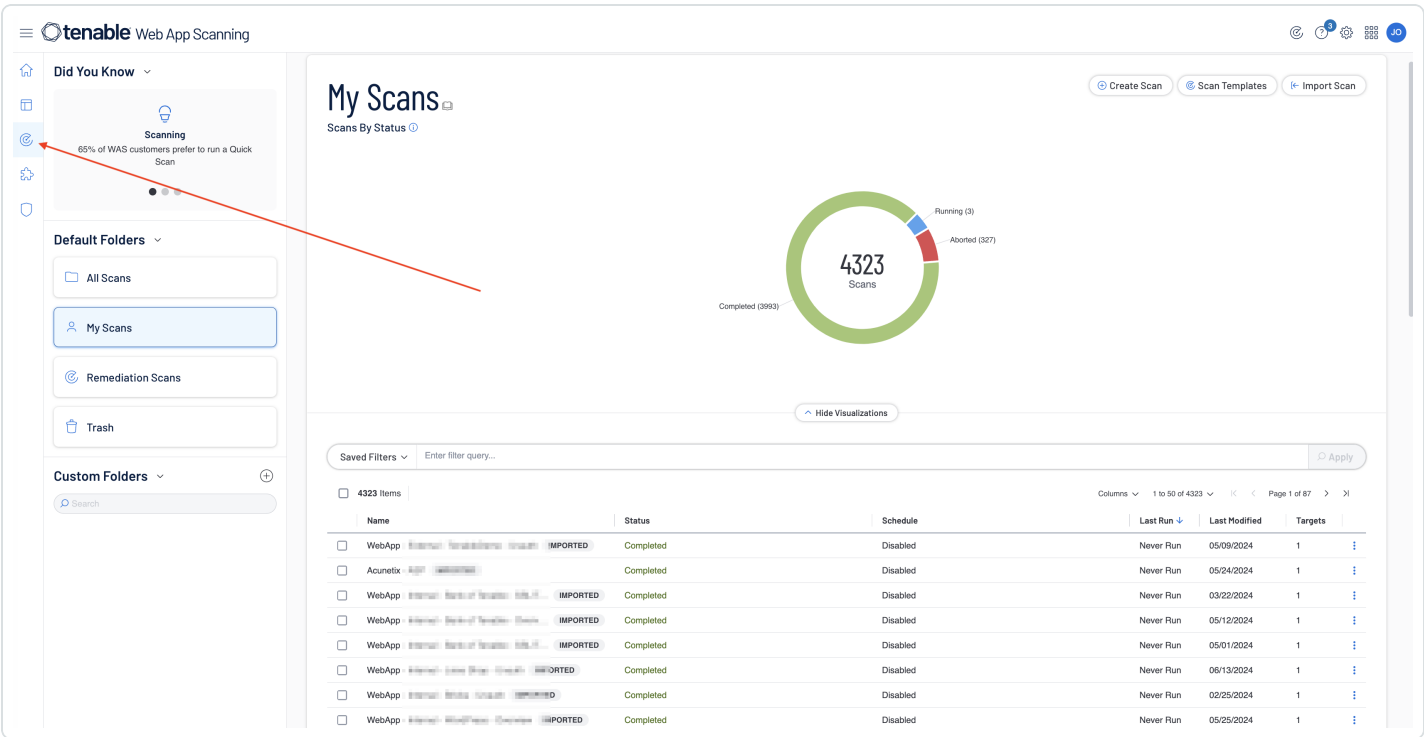
Ensure that the proper scan credentials are being used for the broadest vulnerability analysis. For more information on Authenticated vs. Unauthenticated Scanning see the Vulnerability Management section of this guide, and the Vulnerability Assessment/Scanning section of the Vulnerability Management Cyber Study.

There are a number of useful plugins used to authenticate to the remote host which assist in determining the health of the vulnerability scanning program. These plugins gather the information necessary for local checks, and enable local checks. These plugins can be used to troubleshoot authentication problems. Their output and audit trails provide details of any problems that were encountered. These plugins and their descriptions are listed under Local Authentication in the following guide: [Vulnerability Assessment/Scanning section of the Vulnerability Management Cyber Study](#).

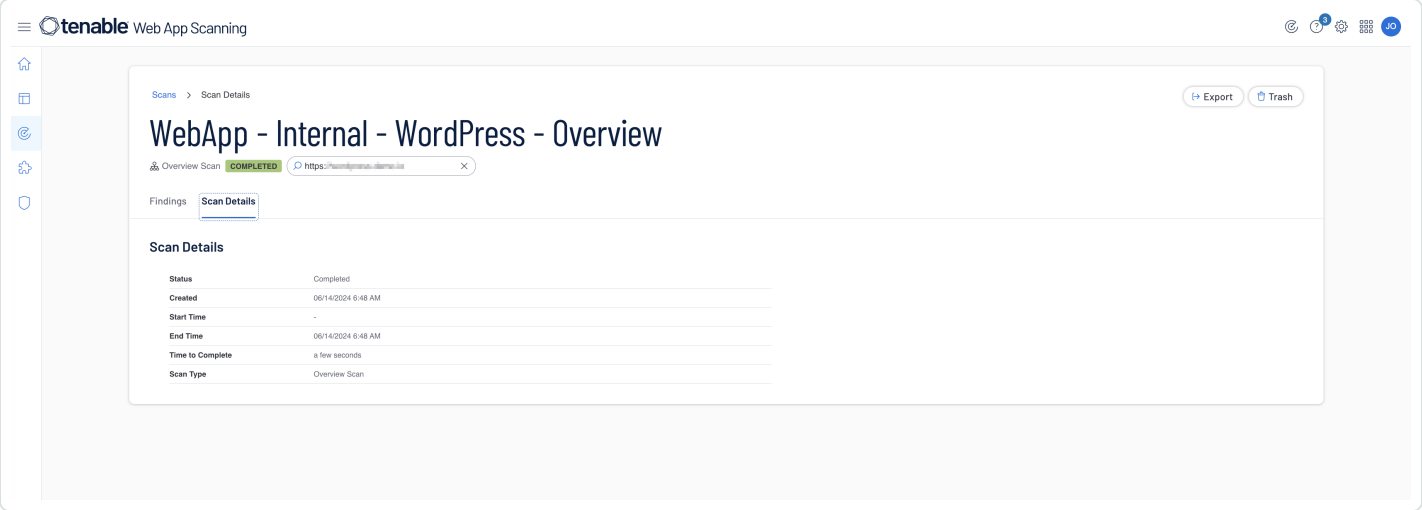
Web Applications

Web Applications require additional treatment. Tenable Web App Scanning provides easy-to-use, comprehensive, and automated vulnerability scanning for modern web applications. There are significant differences between scanning for vulnerabilities in web applications and scanning for traditional vulnerabilities with Tenable Nessus, Tenable Nessus Agents, or Tenable Nessus Network Monitor. As a result, Tenable Web App Scanning requires a different approach to vulnerability assessment and management.

When reviewing scan program health details from within Tenable Web App Scanning, click on the **Scans** icon that is available on any page. The **My Scans** page will load and information on the status of the Web Application Scanning program will be displayed. To view additional details click on any scan and then select **Scan Details**.



The **Scan Details** displays information on the status of the scan (Completed, Aborted), the start and end time, duration of the scan, and the scan type.



For more information on Web App Scanning, see the following information: [Getting Started with Web Application Scanning](#).

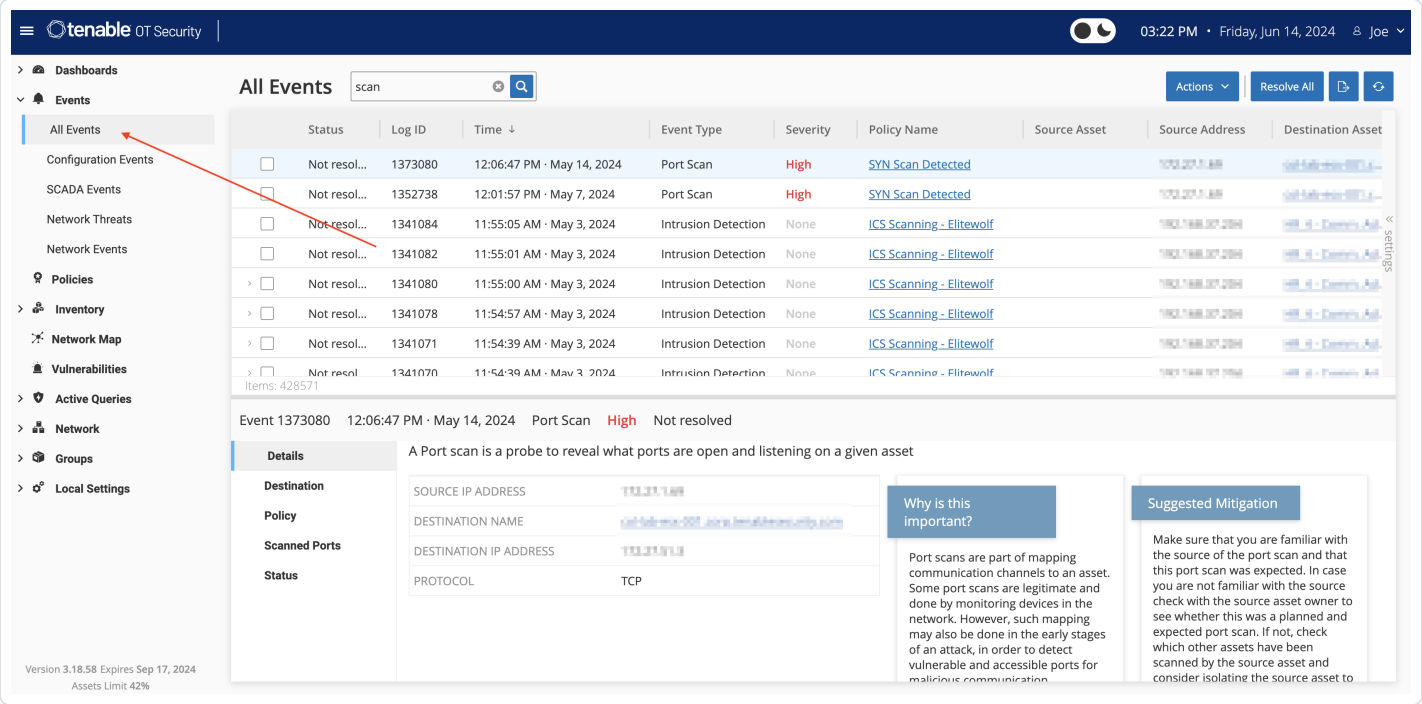
Industrial Control Systems

When OT devices are an integral part of the organisation, Tenable.ot continuously monitors all ICS activities, including activities taking place over proprietary PLC protocols. Tenable.ot identifies real-time anomalies, suspicious and unauthorised activities, and reports on these cyber security events. Tenable.ot uses a network threat detection engine that routinely searches for malicious activity in the network. The engine generates alerts based on the identification of these threats in the network.

This is accomplished by automatically establishing a baseline of each controller configuration and continuously monitoring for configuration changes. All changes are reported, and security staff members are alerted if any unauthorised change is made through the network or physically by connecting directly to the OT device. Besides providing useful information, this capability documents that all configuration changes to controllers were noted and accounted for.

Tenable.ot regularly (at user-defined intervals) scans each controller and takes a snapshot of the device's configuration file. These snapshots are then compared with the previous day's file, changes are noted, and alerts with information on those changes are created. This allows organisations to catch suspicious changes and investigate or reverse them. Conventional anomaly detection solutions can't do this. New baselinings can be invoked at any time by the administrator.

Additionally, Tenable.ot monitors the network traffic and creates a baseline of the expected network communications. Any violation to this baseline triggers an alert. Tenable.ot monitors the used network ports/protocols and any deviation from the expected network protocols (baseline) triggers an alert which can be viewed under the **Events** page, and then selecting a filtering option or All Events.

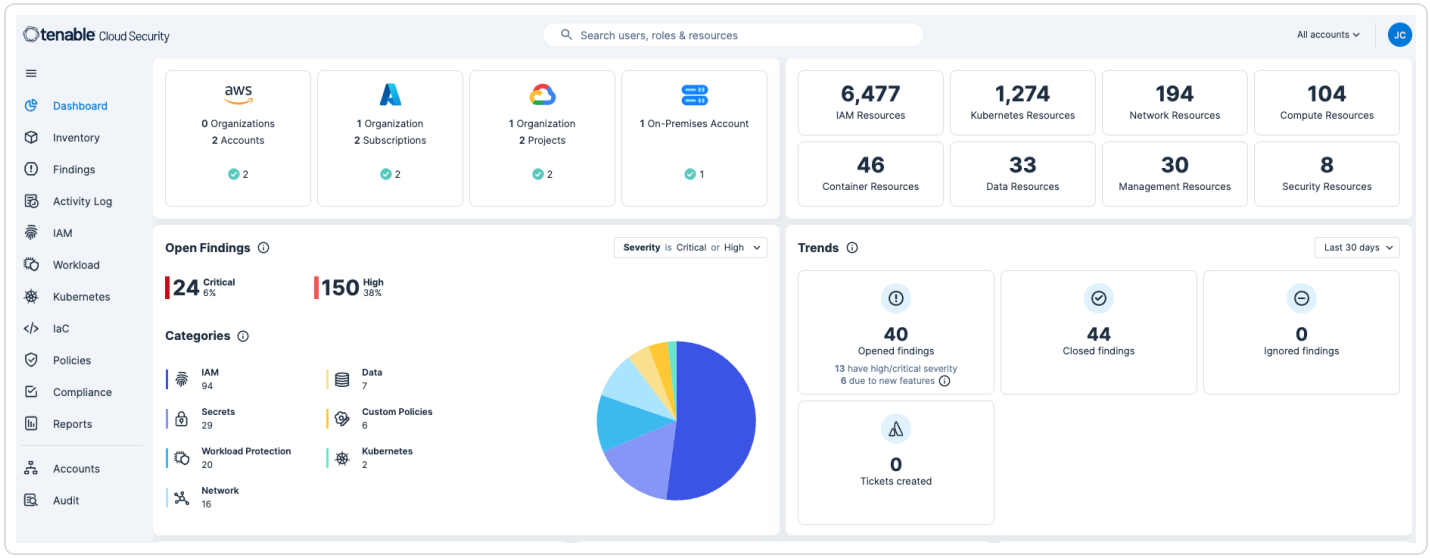


Cloud Infrastructure

The dynamic, distributed nature of cloud environments often creates alerts that lack context at a volume that can overwhelm security teams. Manually sifting through log data and attempting to correlate the data can quickly flood teams with false positives instead of actionable insights. To make matters worse, when suspicious or unusual activity such as misconfigurations or access-related risks are found, teams may quickly realise they lack the depth and context needed to get to the bottom of it.

Tenable Cloud Security automates threat detection and remediation to eliminate noise enabling your team to focus on what matters most. In-depth investigation, monitoring, and reporting on suspicious or unusual activity across AWS, Azure, and GCP is simplified by creating a behavioural baseline for each identity. By continuously assessing and prioritising risk across human and service identities, network configuration, data, and compute resources Tenable Cloud Security proactively reduces the attack surface and blast radius in case of a breach.

The organisation's entire multi-cloud environment is continuously analysed, evaluating risk factors including effective exposure, misconfigurations, excessive and risky privileges, leaked secrets and vulnerabilities. Unusual data access, privilege escalation and other identity-related threats, as well as changes in login settings, unusual reconnaissance, and unauthorised use or theft of access keys, can all be detected. Tenable analyses cloud provider logs to reveal the identity behind each activity and affected accounts, resources, and services.



For more information on Tenable Cloud Security, [reference the following documentation](#).

The following cross-reference information is provided to derive a more comprehensive and effective approach to managing information security requirements. NIS 2 Article 21(2)(c) references security in resilience and Business continuity management. NIS 2 Article 21(2)(i) references Asset Discovery, both processes fall within continuity management.

Security domains define how information is classified, categorised, or administered. The following Security Domains, Sub-Domains, and Measures are related to NIS 2 Article 21(2)(c) and (i), and can assist organisations already using other standards and frameworks to comply with NIS 2.

SECURITY DOMAIN: Resilience

SECURITY SUB-DOMAIN: Continuity of operations

SECURITY MEASURE: Business continuity management

In an effort to foster higher consistency and reliability across multiple frameworks and the NIS 2, Article 21(2)(c) and (i) can be associated with the ISO 27001, NIST CSF, and ISA/IEC 62443 utilising

the following cross-references for continuity of operations. The following cross-references cover the processes and procedures related to Resilience and Business continuity management.

CROSS REFERENCES:

The ISO 27001 references sections within Performance Evaluation, and Improvement, specifically the following sections:

- ISO 27001 (9.3, 10.2, A.5.1.2, A.11.2.4, A.17.1, A.17.2)
- The NIST CSF references the following sections within Identify, Protect, Respond, Recover, and Protect.
- NIST CSF (ID.RM-1, 2, 3, PR.IP -4, 7, 9, 10, RS.IM- 2, RC.IM -1, 2, RC.RP -1, RC.CO -1,2,3, PR.PT -5, PR.DS -4, ID.BE -5, ID.SC -5)

The ISA/IEC 62443 references the following sections within Auditable Events, Security Functionality Verification, Boundary Protection, Audit Logs, and Resource Availability.

- ISA/IEC 62443 (SR 2.8, SR 3.3, SR 5.2, SR.6.1, SR 7.1, SR 7.2, SR 7.3, SR 7.4)

Incident Detection and Response

Incident detection and response are the process and activities involved in the identification, analysing, and reacting to potential security incidents within an organisation's IT infrastructure. Incident detection refers specifically to the continuous monitoring of an organisation's infrastructure to detect any signs of malicious activity. For more information related to continuous monitoring or vulnerability management, see the relevant sections of this guide.

The following sections within the NIS 2 may be best suited to fall into the Incident Detection and Response category:

- Article 21(2)(b): Incident Handling: Incident Management and Reporting

Incident response encompasses several key aspects:

- **Analysis** - The investigation and assessment of the scope of the incident to understand what happened and how.
- **Containment** - Taking immediate action to prevent additional assets within the organisation from being affected.
- **Eradication** - The removal of the threat or vulnerability, which may involve patching systems and/or updating configurations.
- **Recovery** - The restoring of data to a known good state or re-installing software.
- **Post-Incident Analysis** - The reviewing of the process to identify lessons learned, and improve future security measures.

Effective incident detection and response are crucial for reducing the impact of security incidents on an organisation's operations, reputation, and integrity. Good incident detection response plans include a variety of technologies, a solid vulnerability management program, and well-defined policies and procedures.

Tenable OT Security provides the following capabilities for incident detection:

System Abnormalities for Attack Detection: Tenable OT defines examples of abnormalities in system behaviour that provide practical ways of detecting malicious activity that is otherwise hard to identify. Both a statistical anomaly detection system and a rules-based whitelist/blacklist system to identify system behaviours indicative of compromise where the initial compromising event may not have been detected are used.

Proactive Attack Discovery: Tenable OT uses an informed understanding of more sophisticated attack methods and normal system behaviour to monitor proactively for malicious activity. This includes sophisticated detection not just of attack events, but also the consequences of such events, such as command and control traffic, malware transmission, etc. The event data can be used in frameworks such as MITRE ATT&CK and other TTP frameworks.

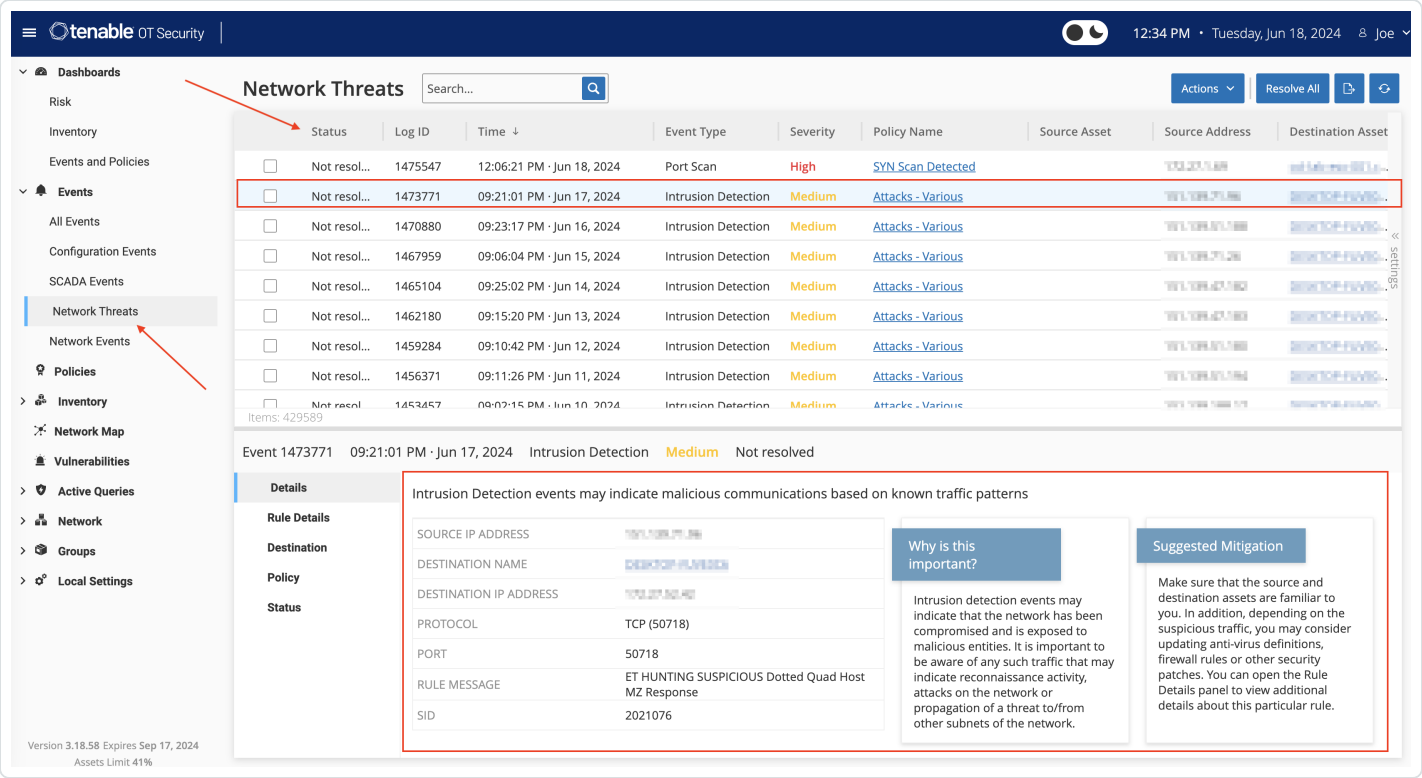
Tenable OT tracks and alerts across the following 16 event categories:

- **Code/Configuration/Firmware Transfer** - Uploading and downloading code, configurations, and firmware for various PLCs and controllers.
- **Delete** - Deleting code, configurations, and firmware from devices.
- **Device Operation** - Starting, stopping, restarting, and potentially going online/offline for devices. This might include cold/warm start events.
- **Modifying of Device Configuration**s - Modifying device configurations, including code edits, renames, sequence resets, and enabling/disabling unsolicited responses.
- **Device Status** - Monitoring and reporting on devices' health, configuration, and operational state. This includes status changes like module state changes.
- **HA and Redundancy** - Switching or resetting redundancy.
- **Suspicious Network Activity (Operational/Security)** - Events requiring attention due to potential security concerns or operational anomalies.
- **Version Change** - Version change.
- **Abnormal Network Activity** - Abnormal behaviour in the network.
- **Access Control** - Authentication-related activities, including successful/failed login attempts and file authentication.
- **Device Error** - Events indicating unexpected device behaviour, such as DNP3 errors and Telnet failures.
- **PLC Programming** - Changes the logic of the PLC.
- **Communication Establishment** - Typically, these events occur during system startup or when a new connection is initiated.

- **Communication Management** - Management of data exchange formats (datasets and tables) within established communication protocols.
- **Diagnostics and Maintenance** - Events used for various diagnostic and maintenance purposes, such as troubleshooting control logic, testing PLC functionality, simulating process conditions, and preparing a PLC for operation or taking the PLC out of service.
- **PLC Operation** - Ensuring proper functionality before integrating the PLC into the control process.

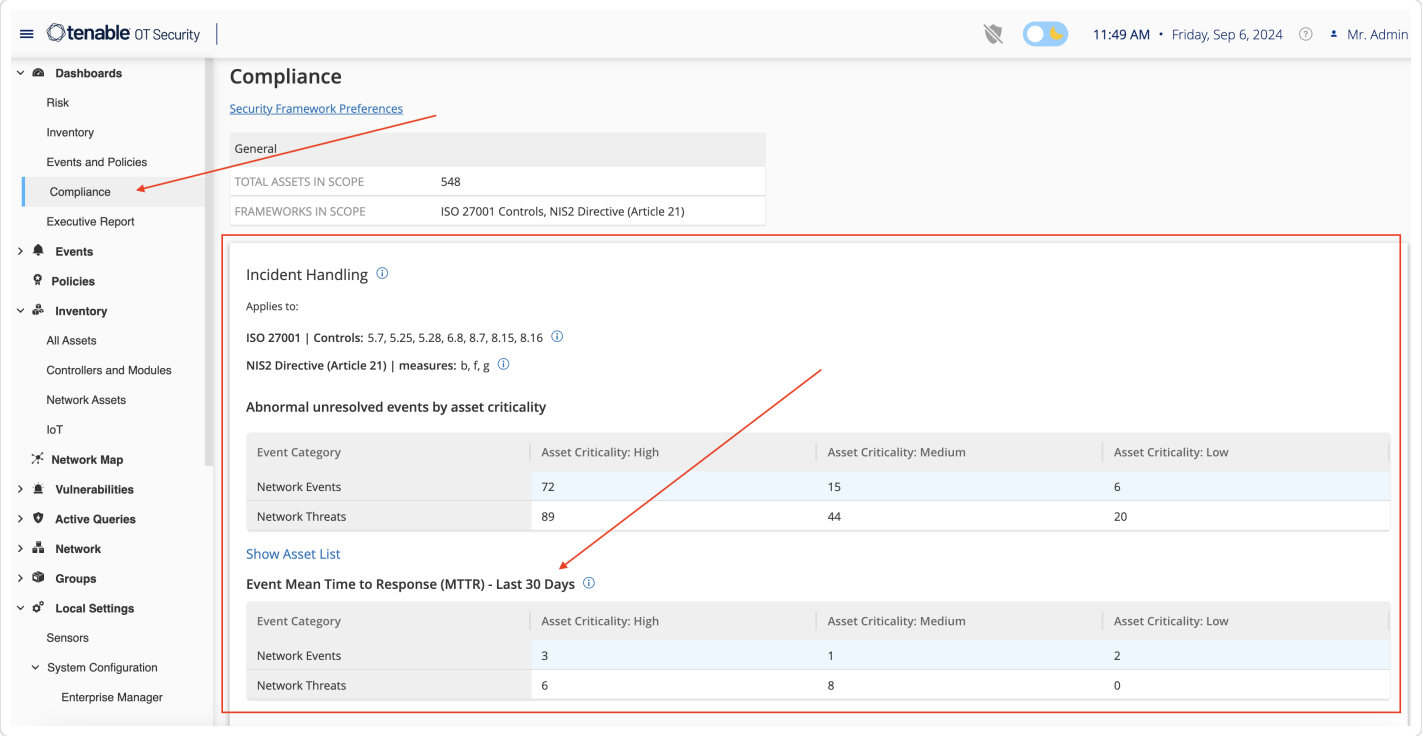
Specific events which are of particular importance to this section are: New Asset/Module discovery or removal, inactive/stopped assets, event start/resolution times, and vulnerability identification/resolution times.

In this example, from the **Events** page select **Network Threats**. On this page, we can set the status to all **Unresolved events**. Here we can identify a series of Intrusion Detection events. Selecting the first of these events we can view the details box. The details provide information on the type of event, why this event is important, and suggested mitigation techniques.

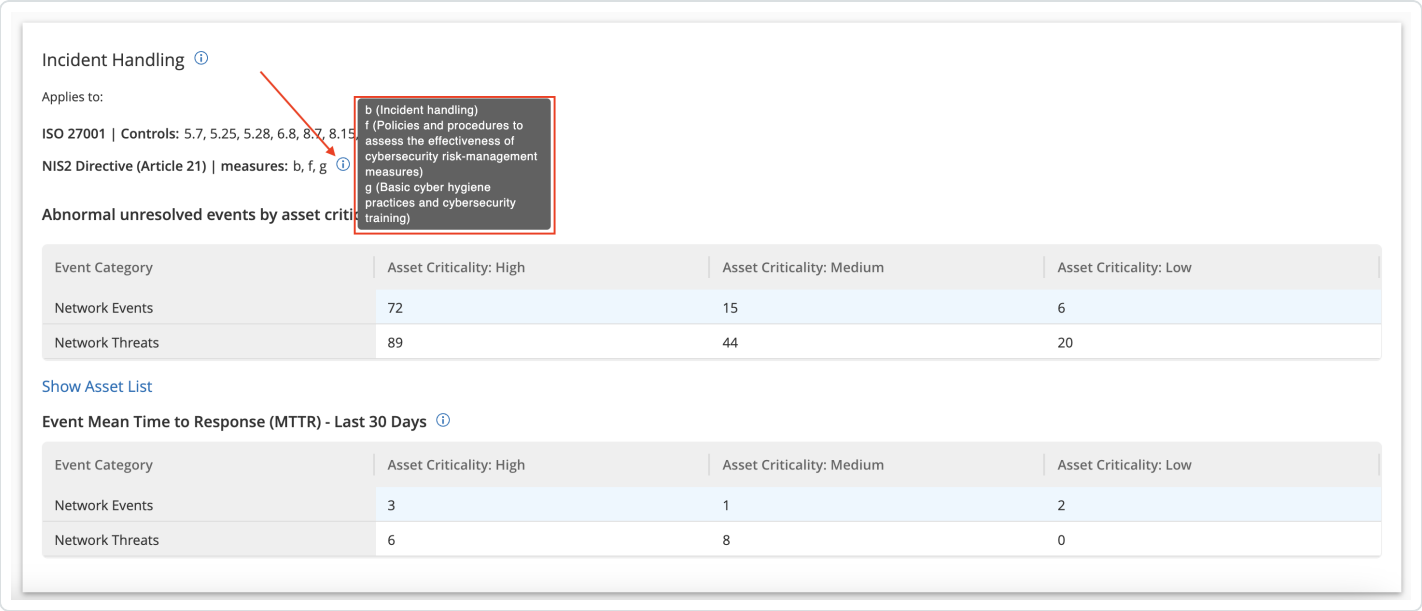


The incident handling widget for Tenable OT within the compliance dashboard, is a crucial tool that provides an immediate overview of the assets at risk by their criticality. The dashboard allows analysts to drill down into high risk areas and investigate security events.

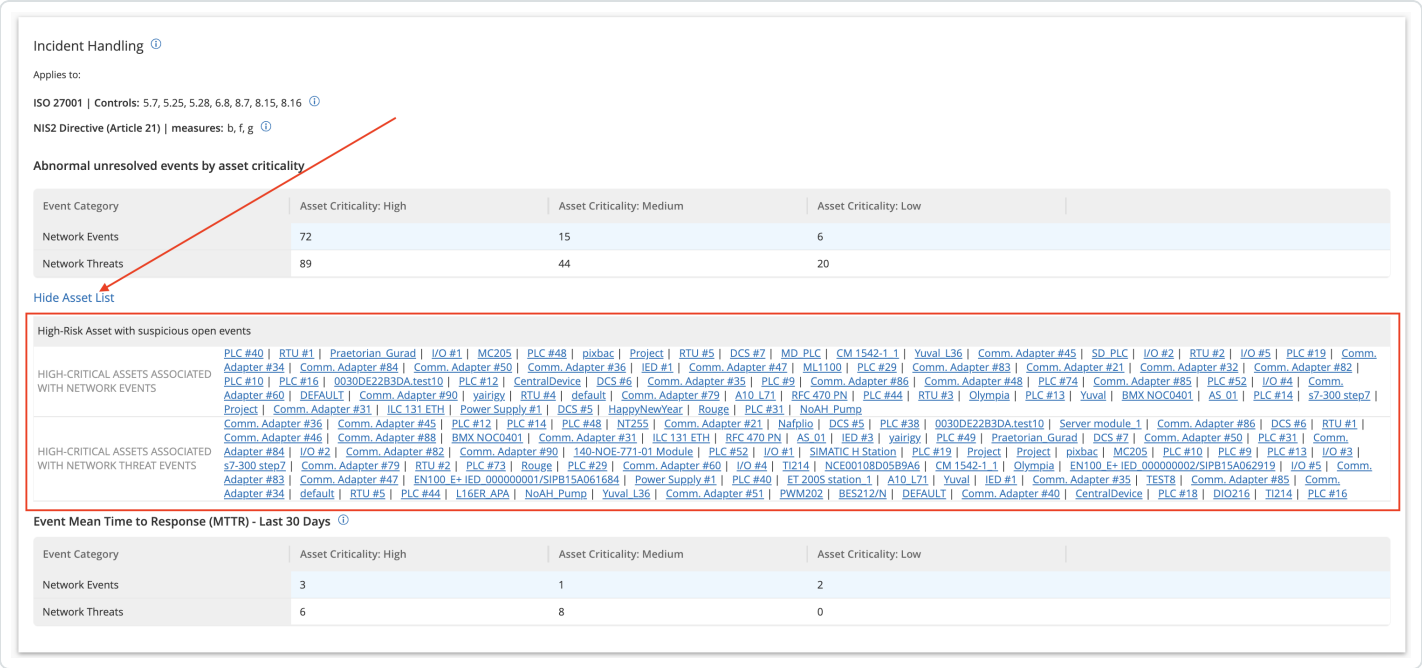
Event Mean Time To Respond (MTTR) is a critical key performance indicator (KPI). A shorter MTTR indicates a more efficient incident resolution process. Minimising downtime and disruptions is crucial for maintaining productivity and service availability.



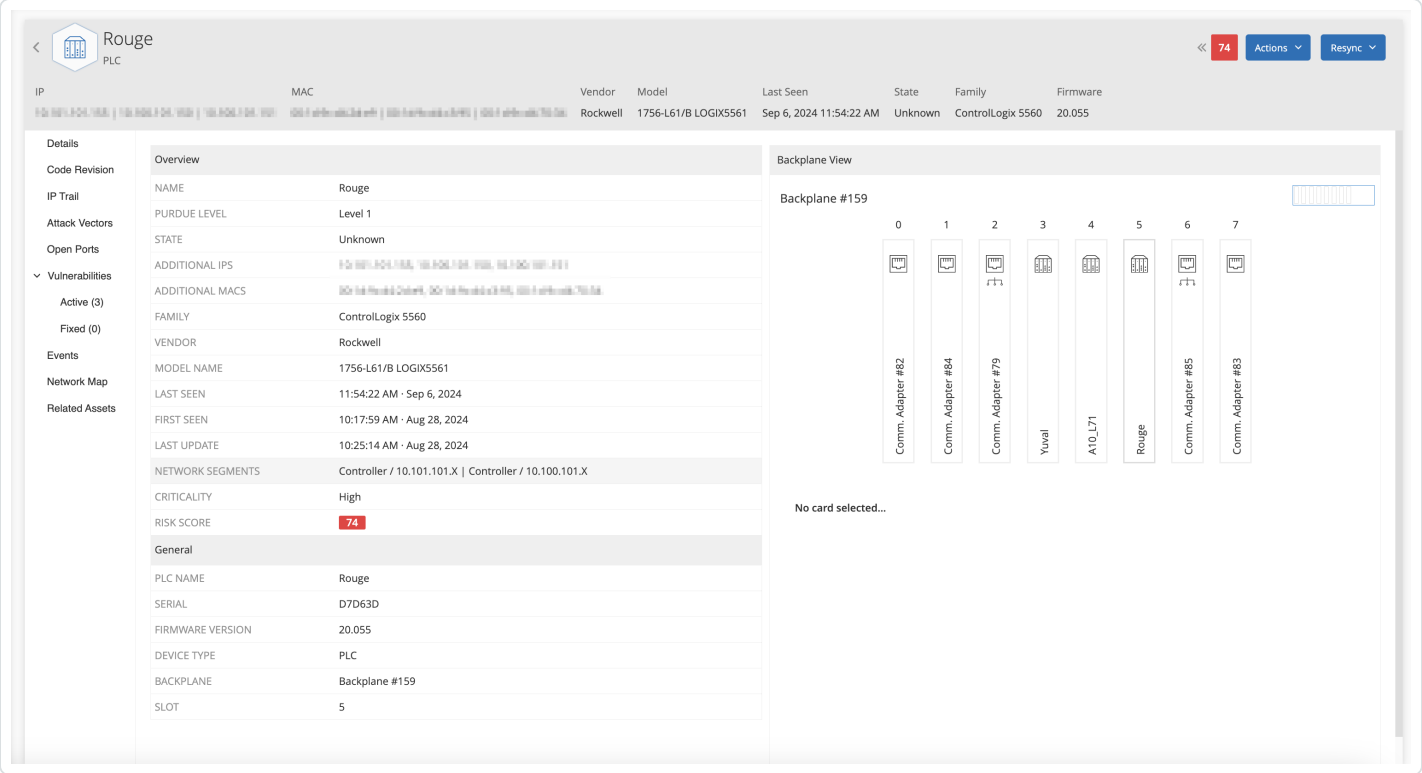
Each widget is mapped to the relevant area of the NIS 2 framework, assisting organisations to easily improve specific areas of focus. The information icon presents details on which framework measures are being addressed within each widget.



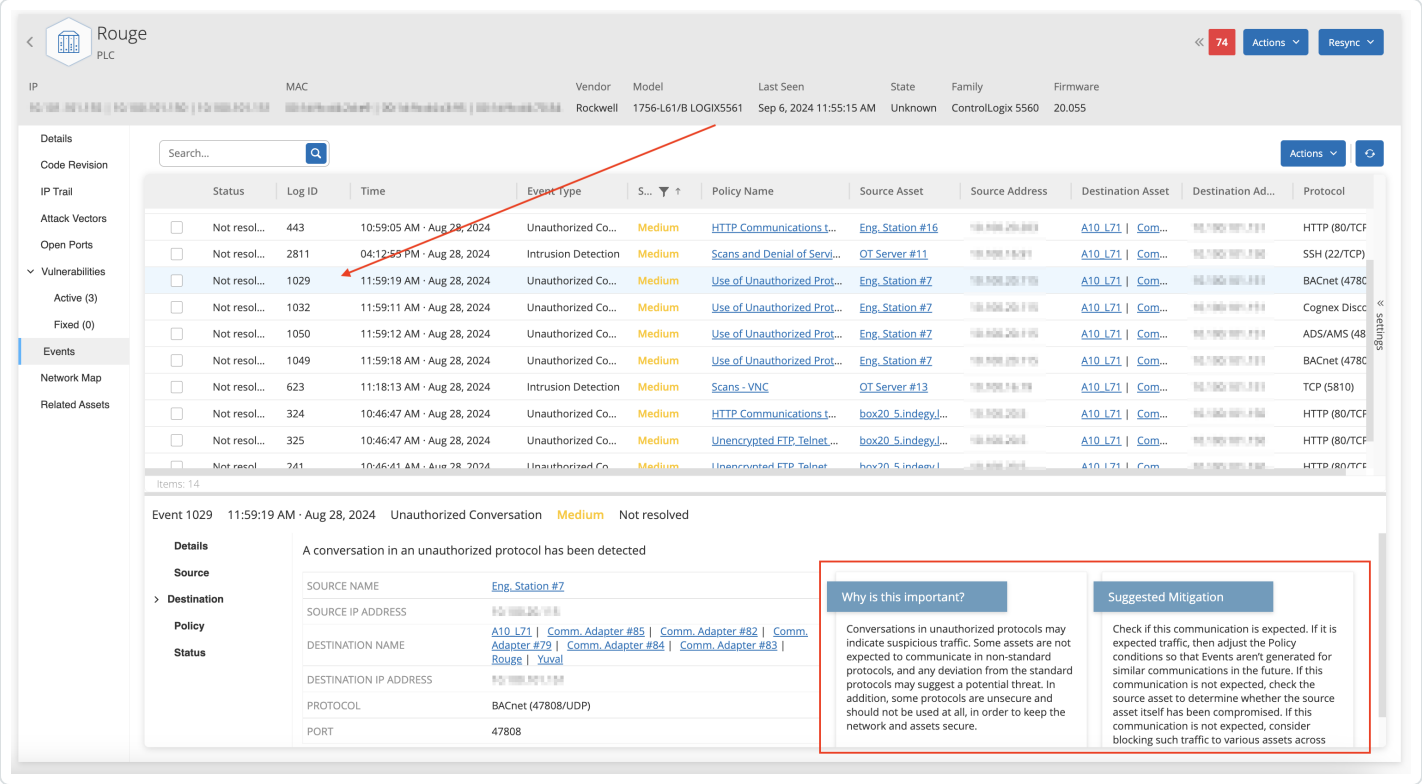
The Show/Hide Asset List link provides organisations with a deeper level of asset assessment by expanding out a list of assets vulnerable under this category. Selecting the link provides details which focus on the most critical action you have to take first, in this case Critical assets associated with Network and TD events.



Detailed asset information is available in the Single Asset View.



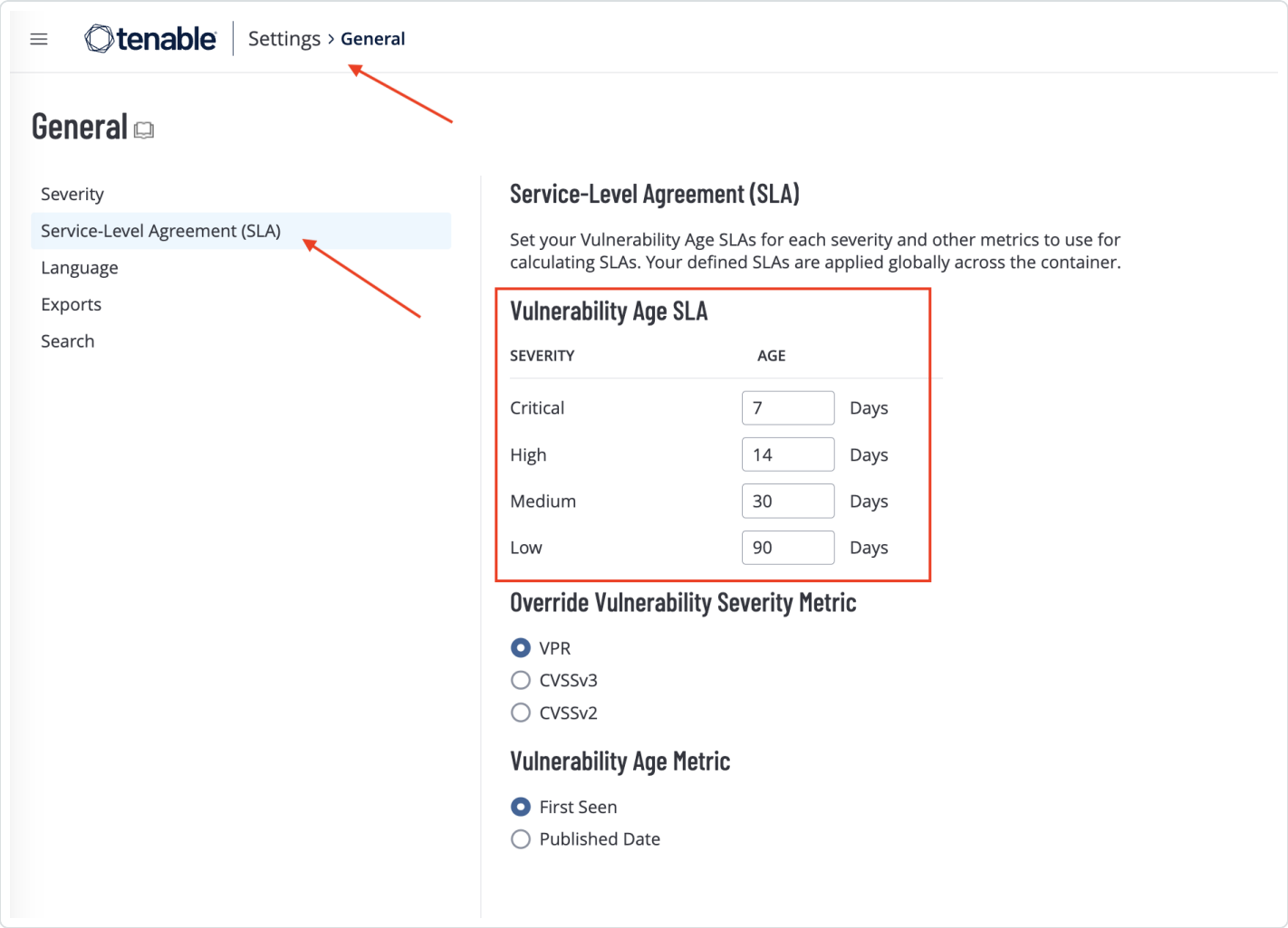
The Events section provides information on any associated events, which can be reviewed and investigated further. Included are details on the identified vulnerabilities, and suggested mitigation strategies. These details are available when an item is selected.



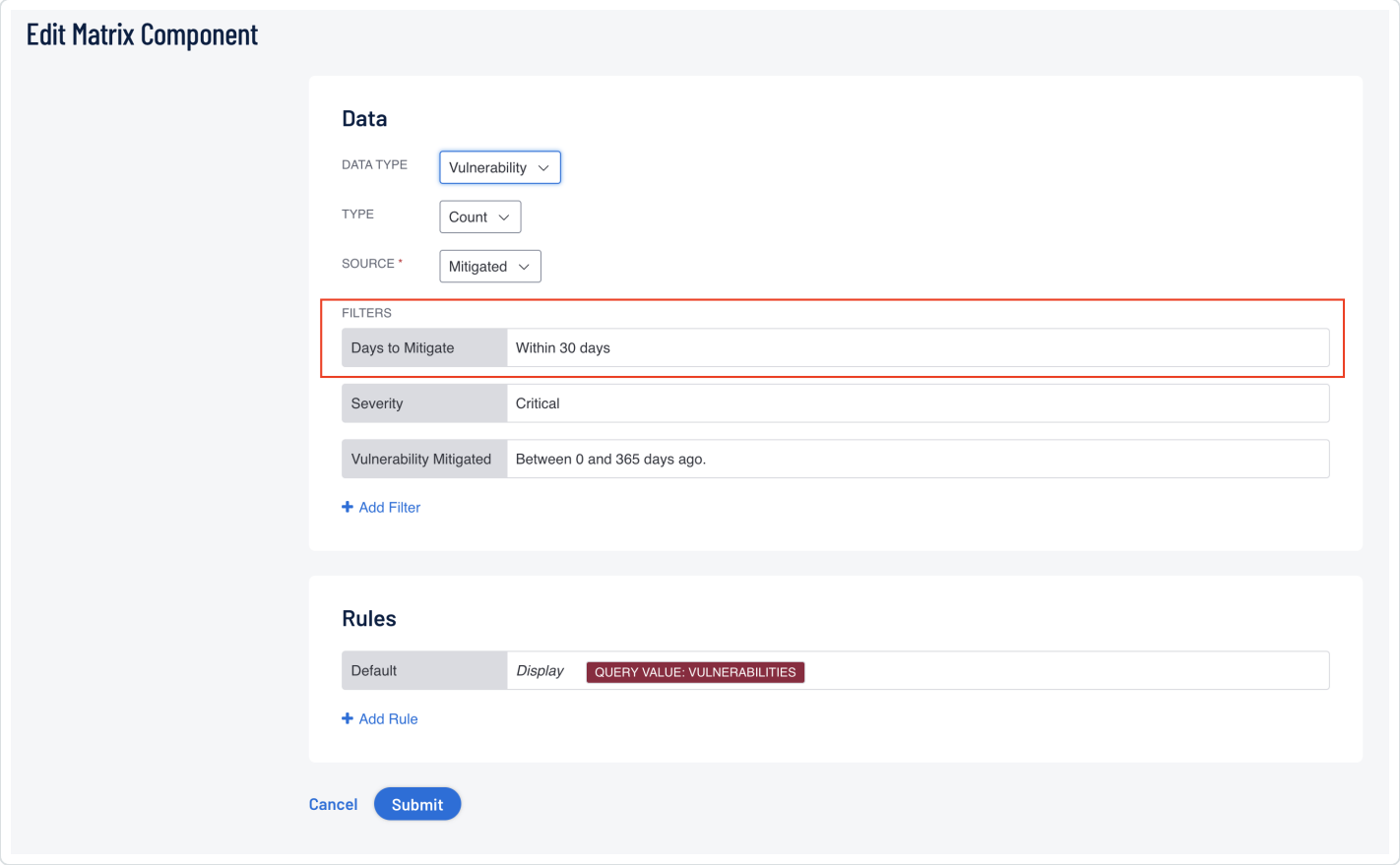
For more information on using Tenable OT Security reference the [Tenable OT Security Getting Started Guide](#).

Service Level Agreements (SLA) play an important role in the reporting process. If the organisation has an SLA established for remediation, those can be set into Tenable Vulnerability Management and Tenable Security Center to make reporting SLA progress a simple task. There is no set timetable to resolve vulnerabilities that fits every situation. SLAs can vary from organisation to organisation, and even vary between business units within the organisation. Tenable recommends aligning SLAs with technology or business objectives, starting with the most important assets.

To view or adjust the SLA reporting period within Tenable Vulnerability Management, navigate to **Settings > General**. From there, selecting **Service-Level Agreement (SLA)** will provide you with the page which allows you to define the proper SLA for your organisation.



To view or adjust the SLA reporting period within Tenable Security Center, the widget filter must be set. For this example, provided the SLA for critical vulnerability remediation is 30 days, adding and setting the **Days to Mitigate** filter to "Within 30 Days" sets the correct reporting timeframe for this widgets cell.



Tenable Lumin summarises key assessment maturity metrics to help improve assessment capabilities and security responsiveness. Tenable Lumin provides detailed analysis into asset scan distribution, frequency, and vulnerability age to strengthen program effectiveness and focus on process maturity. Interactive widgets allow analysts to drill into assessment maturity data to investigate the security posture of underlying assets. Tenable Lumin measures remediation responsiveness, remediation coverage, and provides the proper context for an organisation's process risk mitigation efforts.

The metrics provided by Remediation Maturity scores allow organisations to pinpoint the specific strengths and weaknesses of their remediation efforts. They can use this information to better understand their processes and modify them accordingly - either by changing those processes and/or making further investments.

Remediation maturity metrics include:

- Remediation Maturity Grade (A-F) for Org and Business Contexts
- Remediation Maturity Trending (Organizations vs Industry vs Population)
- Remediation Responsiveness Grade → Remediation Time Since -- Recovery and Remediation Time Since Vulnerability Publication

For more information on how Tenable Lumin can help see this guide. More information on Tracking and Reporting SLA progress can be found in this document.

The following cross-reference information is provided to derive a more comprehensive and effective approach to managing information security requirements. NIS 2 Article 21(2)(b) references Incident Handling and Reporting.

Security domains define how information is classified, categorised, or administered. The following Security Domains, Sub-Domains, and Measures are related to NIS 2 Article 21(2)(b), and can assist organisations already using other standards and frameworks to comply with NIS 2.

SECURITY DOMAIN: Defence.

SECURITY SUB-DOMAIN: Computer Security Incident Management.

SECURITY MEASURE: Information system security incident response.

In an effort to foster higher consistency and reliability across multiple frameworks and the NIS 2, Article 21(2)(b) can be associated with the ISO 27001, NIST CSF, and ISA/IEC 62443 utilising the following cross-references for incident handling. The following cross-references cover the processes and procedures related to information system security incident response.

CROSS REFERENCES:

The ISO 27001 references sections within Annex A, Information Security Controls Reference, specifically the following sections:

- ISO 27001(A.16.1.1, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7)

The NIST CSF references the following sections within Identify, and Protect.

- NIST CSF (ID.AM -5, ID.RM-2, 3, PR.IP -7,8, PR.DS -4, ID.BE -5)

The ISA/IEC 62443 references the following sections within System Integrity and Data Confidentiality.

- ISA/IEC 62443 (SR 3.4, SR 4.1)

Compliance and Reporting

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. The NIS 2 Directive (Network and Information Systems Directive 2022/2555) is a legislative framework established by the EU to enhance the cybersecurity and resilience of network and information systems across critical sectors. The NIS 2 builds upon the initial NIS Directive, expanding its scope and requirements for organisations.

The following sections within the NIS 2 may be best suited to fall into the Compliance and Reporting category:

- Article 21(2)(f): Policies and Procedures for Testing Cybersecurity Risk Management Measures: Policy Definition and Testing

Reporting is the process of documenting and communicating information related to compliance activities. This process involves the submission of accurate, timely, and comprehensive reports to relevant stakeholders. Together compliance and reporting help organisations maintain trust, manage risks, and uphold legal responsibilities.

The NIS 2 Directive imposes specific compliance requirements on in-scope essential and important entities. These requirements are designed to enhance cybersecurity and ensure the resilience of digital and physical assets involved in delivering essential or important services in the European Union. The key compliance requirements include:

Cybersecurity Risk Management Measures: In-scope entities are required to implement ten key measures to manage and mitigate cyber risks effectively. These measures encompass various aspects of cybersecurity risk management, including:

1. Policies on risk analysis and information system security.
2. Incident handling, covering prevention, detection, and response to incidents.
3. Crisis management and business continuity, including backup and recovery management.
4. Supply chain security, addressing relationships with suppliers and service providers.
5. Security in network and information systems acquisition, development, and maintenance, with a focus on vulnerability handling and disclosures.

6. Policies and procedures to assess the effectiveness of cybersecurity risk management.
7. Basic cyber hygiene practices and cybersecurity training.
8. Policies and procedures regarding the use of cryptography and, where appropriate, encryption.
9. Human resources security, access control policies, and asset management.
10. The use of multi-factor authentication or continuous authentication solutions, secured voice, video, and text communications, and secured emergency communication systems.

The penalties for noncompliance with the NIS 2 Directive can be substantial and vary depending on the classification of the entity falling within its scope. The directive prescribes specific penalties for essential and important entities as follows:

- **For Essential Entities**: Noncompliance with the NIS 2 Directive by essential entities can result in fines of up to €10,000,000 or at least 2% of the total annual worldwide turnover of the company to which the entity belongs, whichever amount is higher.
- **For Important Entities**: Important entities that fail to comply with the NIS 2 Directive may face fines of up to €7,000,000 or at least 1.4% of the total annual worldwide turnover of the company to which the entity belongs, whichever amount is higher.

These penalties are designed to encourage organisations to take cybersecurity and incident reporting seriously, as well as to ensure the security and resilience of essential and important services within the European Union. Noncompliance can have significant financial repercussions for organisations. This makes adhering to NIS 2 compliance requirements and deadlines crucial.

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.

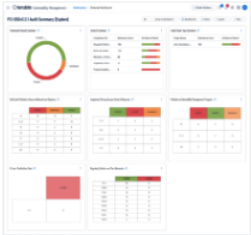
Search

Title

Dashboard Category

Compliance & Configuration Assessment

Apply



PCI-DSSv3.2.1 Audit Summary (Explore)

by Cesar Navas

April 23, 2024

Tenable.sc Dashboards

Keyword Search

Title Search

Dashboard Category

Compliance & Configuration Assessment

Apply

OWASP Categories

by Cody Dumont

August 22, 2023

CIS Audit Summary

by Cody Dumont

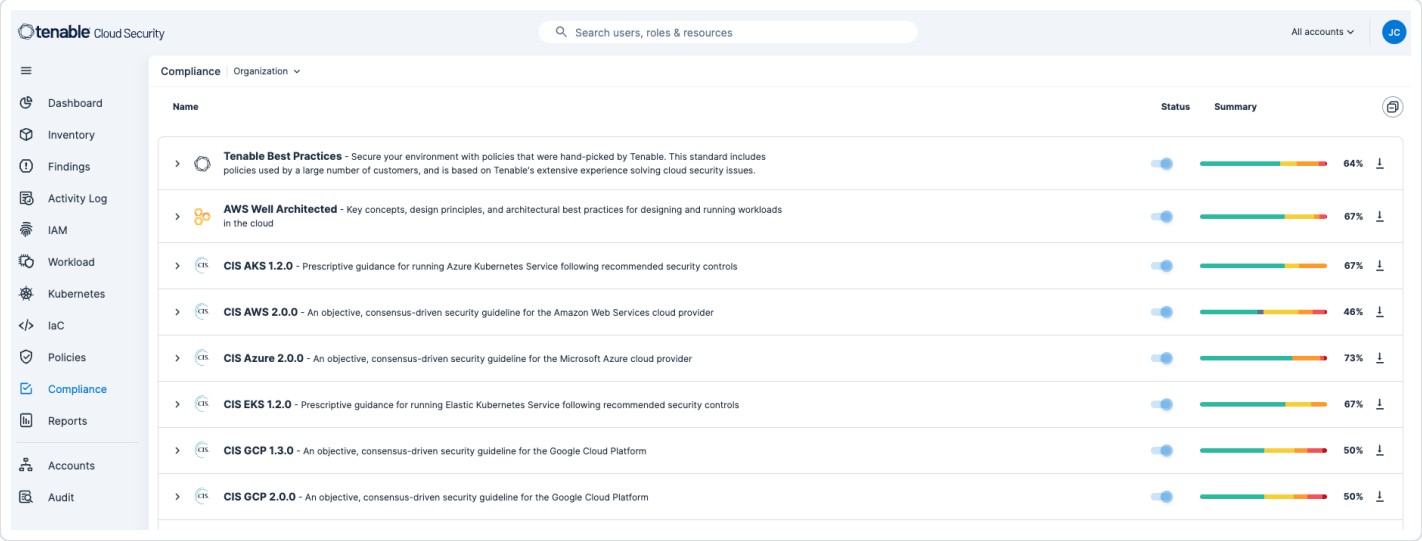
July 25, 2023

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

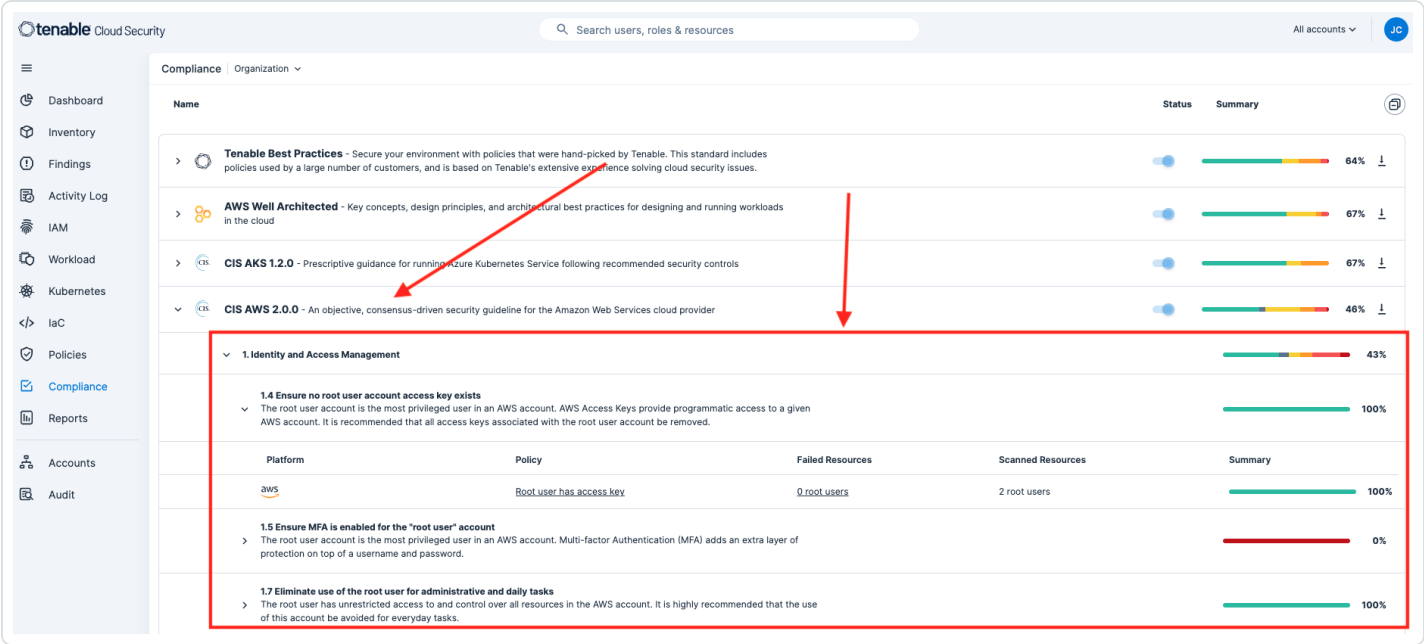
Cloud services are an integral part of business operations, offering scalability, flexibility, and accessibility. Cloud environments store vast amounts of sensitive data, including personal information, financial records, intellectual property, and proprietary business data. Ensuring robust security 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.



The following cross-reference information is provided to derive a more comprehensive and effective approach to managing information security requirements. NIS 2 Article 21(2)(f) references risk management measures.

Security domains define how information is classified, categorised, or administered. The following Security Domains, Sub-Domains, and Measures are related to NIS 2 Article 21(2)(f), and can assist organisations already using other standards and frameworks to comply with NIS 2.

SECURITY DOMAIN: Defence.

SECURITY SUB-DOMAIN: Computer Security Incident Management.

SECURITY MEASURE: Information system security incident response.

In an effort to foster higher consistency and reliability across multiple frameworks and the NIS 2, Article 21(2)(f) can be associated with the ISO 27001, NIST CSF, and ISA/IEC 62443 utilising the following cross-references for vulnerability handling and disclosure. The following cross-references cover the processes and procedures related to risk management.

CROSS REFERENCES:

The ISO 27001 references sections within Annex A, Information Security Controls Reference, specifically the following sections:

- ISO 27001(A.16.1.1, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7)

The NIST CSF references the following sections within Identify, and Protect.

- NIST CSF (ID.AM -5, ID.RM-2, 3, PR.IP -7,8, PR.DS -4, ID.BE -5)

The ISA/IEC 62443 references the following sections within System Integrity and Data Confidentiality.

- ISA/IEC 62443 (SR 3.4, SR 4.1)

Security Hygiene Practices

Information security hygiene refers to a set of practices and behaviours that organisations adopt to maintain their data security integrity. Several sections within the NIS 2 may be best suited to fall into the Risk Assessment category. Those include:

- Article 21(2)(g): Basic Cyber Hygiene Practices and Cybersecurity Training: Cyber Hygiene.
- Article 21(2)(h): Policies and Procedures regarding the use of cryptography, and appropriate encryption.

The practice encompasses a series of proactive measures designed to protect systems, networks, and data from threats, vulnerabilities, and unauthorised access. Good security hygiene practices include:

1. **Password and Authentication**: Using strong, unique passwords, and implementing multi-factor authentication (MFA) where possible.
2. **Software Updates and Patching**: Regularly updating operating systems, software applications, and firmware to protect against known vulnerabilities.
3. **Backup and Recovery**: Maintaining secure backups of critical systems and data, to ensure resilience against data loss due to accidents, malware, or ransomware attacks.
4. **Network Security**: Security networks with firewalls, intrusion detection/prevention systems, and virtual private networks (VPN) to defend against unauthorised access.
5. **Awareness and Training**: Educating users about security best practices, phishing scams, and social engineering tactics to reduce the likelihood of security breaches.
6. **Device Management**: Managing endpoint devices with encryption policies and secure configurations.
7. **Access Control**: Limiting access to sensitive information and resources based on the principle of least privilege to minimise exposure.
8. **Incident Response Planning**: Establishing protocols and procedures to quickly detect, respond, and recover from security incidents.
9. **Compliance and Regulation**: Adherence to relevant industry regulations and standards (GDPR, HIPAA) to ensure legal and regulatory compliance of data handling.

Establishing and maintaining good security hygiene practices is essential to mitigate risks and safeguard organisational assets from increasingly sophisticated threats.

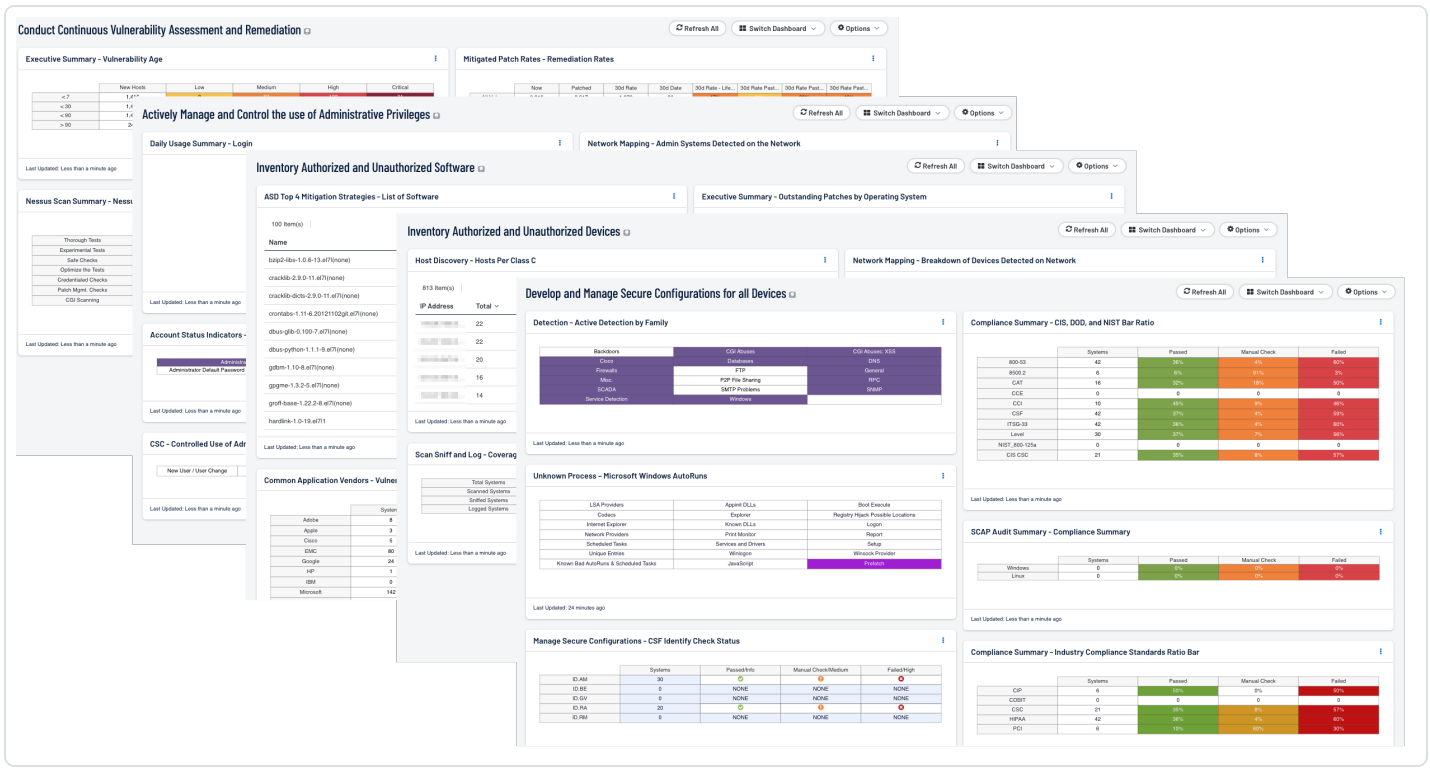
Basic cyber hygiene includes the need to cover basic scenarios, such as knowing what assets are in the environment and asserting what vulnerabilities may lurk within. Without knowing what vulnerabilities are present, analysts cannot ensure that the correct security controls are in place to mitigate or remove the vulnerability. Attackers may use such an opportunity to exploit the vulnerability to steal confidential information. When organisations lack this knowledge or are not aware of other threats such as lack of hardening systems to a common standard, large gaps of security can reside in critical points of infrastructure.

Unsupported products, operating systems and applications are a major cause of data breaches. The proliferation of unsupported and end-of-life (EOL) products is a common security problem experienced across all organisations. As applications and operating systems reach EOL, vendors stop offering support, causing security and stability to decrease over time. A comprehensive summary of unsupported products in the environment is provided.

Another major concern is visibility into the assets in the environment and how effectively vulnerabilities on those assets are managed. As vulnerabilities are identified, remediation must be prioritised and tracked in accordance with organisational goals and Service Level Agreements (SLAs). Reviewing remediated vulnerabilities and the remediation timeframe provides valuable information to the organisation on the effectiveness of the risk remediation program. Vulnerabilities that are known to be exploitable are dangerous, since there are exploit frameworks readily available to exploit them.

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.



The focus of these Cyber Hygiene dashboards is:

Inventory Authorised and Unauthorised Devices: Identifying systems on the network can be a monumental task, as many organisations have different groups responsible for system inventories. This collection of components provides information to analysts and auditors about systems discovered on the network and device inventory.

Inventory Authorised and Unauthorised Software: A good vulnerability management program requires that an organisation also know the software installed on its systems. This dashboard and its components provide information to analysts about software that is discovered on the network.

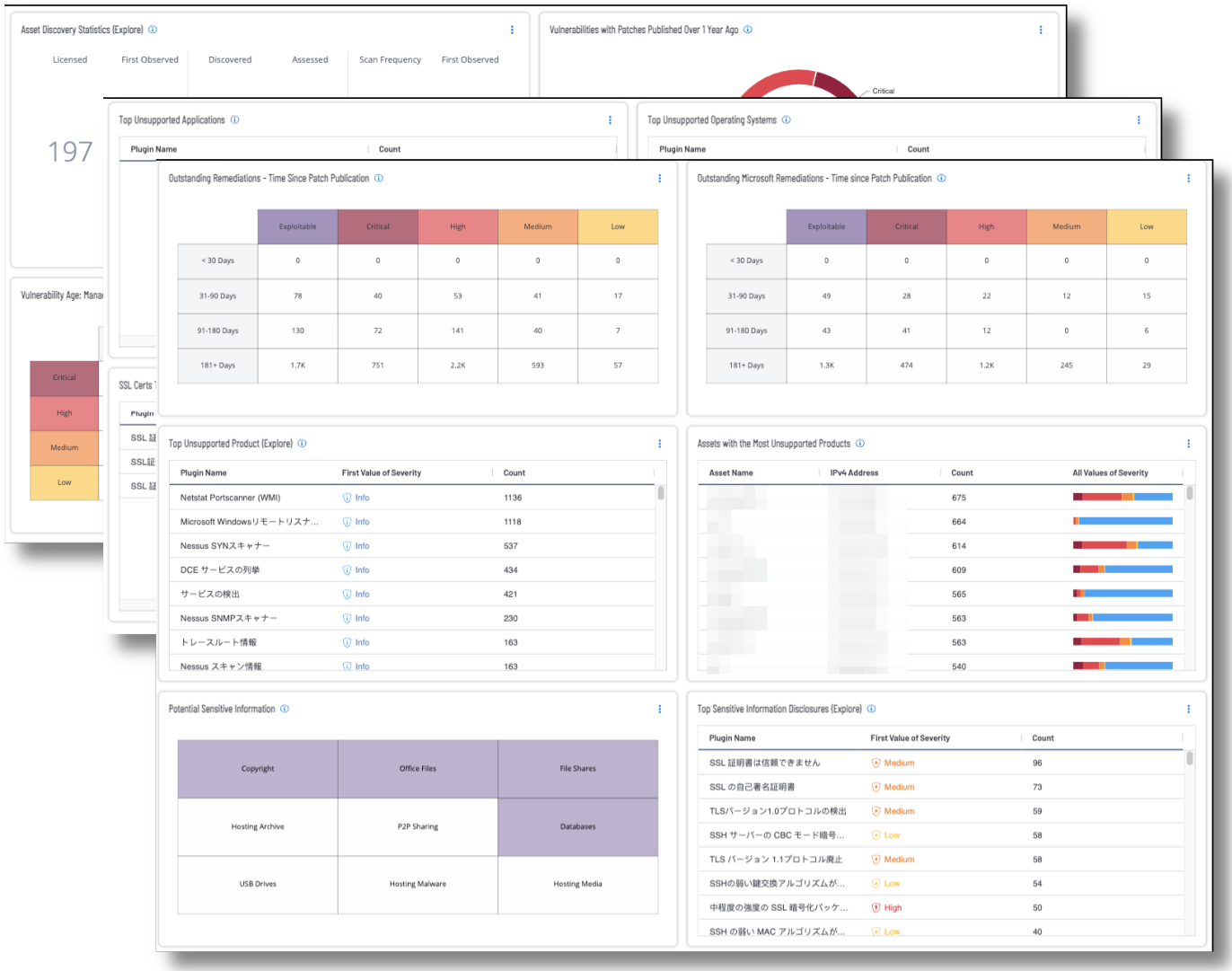
Develop and Manage Secure Configurations for all Devices: Hardening and configuration guidelines can be difficult to create and to maintain. There are several industry standards available to organisations such as NIST 800-53, CIS, and CSC. Tenable has the ability to audit system configurations according 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: Detecting vulnerabilities requires a diligent information security team and the ability to detect vulnerabilities in several ways. 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.

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

Unsupported products, operating systems and applications are a major cause of data breaches. The proliferation of unsupported and end-of-life (EOL) products is a common security problem experienced across all organisations. As applications and operating systems reach EOL, vendors stop offering support, causing security and stability to decrease over time. A comprehensive summary of unsupported products in the environment is provided.

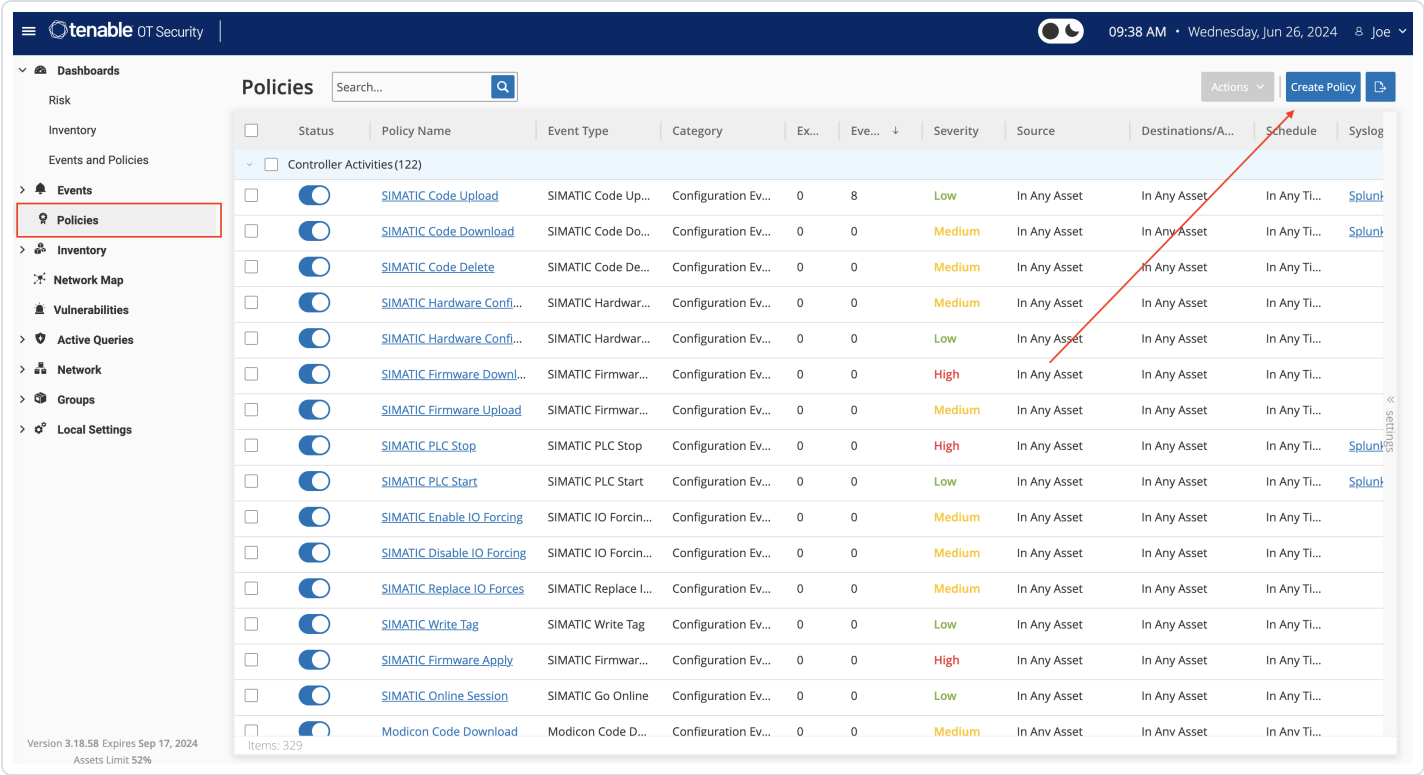


Another major concern is visibility into the assets in the environment and how effectively vulnerabilities on those assets are managed. As vulnerabilities are identified, remediation must be prioritised and tracked in accordance with organisational goals and Service Level Agreements (SLAs). Reviewing remediated vulnerabilities and the remediation timeframe provides valuable information to the organisation on the effectiveness of the risk remediation program. Vulnerabilities that are known to be exploitable are dangerous, since there are exploit frameworks readily available to exploit them. Details are included on vulnerabilities where a patch to remediate the exposure was available more than a year ago.

Data on secure communication controls for sensitive information is provided. The status on SSL certificates that are aged out or soon to be aged out is shown, along with SSL and TLS insecure communication exposures in the environment. Information about exposure of various types of potentially sensitive information is provided. Many organisations are unaware how much sensitive information is exposed, which enables attackers to tailor an attack path specifically targeting the organisation, leading to data loss exposures.

Tenable OT Security includes policies that define specific types of events (aged out certificates, Clear Text transmission, No MFA, and many more) that are suspicious, unauthorised, anomalous, or otherwise noteworthy that occur in the network. When an event occurs that meets all of the Policy Definition conditions for a particular policy, the system generates an event. The system logs the event and sends notifications in accordance with the Policy Actions configured for the policy. Triggered events based on these policies are then available in the Events page, along with additional details and mitigation techniques.

To configure a policy navigate to the **Policy** Page, then select the **Create Policy** icon in the top-right area of the dashboard. Follow the prompts to create and then enable the policy. Each policy consists of a series of conditions that define a specific type of behaviour in the network. This includes considerations such as the activity, the assets involved, and the timing of the event. Only an event that conforms to all the parameters set in the policy triggers an event for that policy. Each policy has a designated Policy Actions configuration, which defines the severity, notification methods, and logging of the event.



The Configuration and Change Management widget for Tenable OT, located on the compliance dashboard provides an overview of all configuration change events which occur after the baseline for Controller and Modules devices such as PLCs. When a "Baseline" version is set, any changes to the controller configuration are displayed here. When not part of regular operations, a configuration upload can be used as a reconnaissance activity to gather information about the controller's behaviour. Critical controller status activities are reported, such as when the device is stopped. These change and configuration notifications ensure operational continuity and quick recovery during service disruptions.

For more information on creating policies, and policy configuration options, see the [Tenable OT Security documentation on Policy creation located here].

The following cross-reference information is provided to derive a more comprehensive and effective approach to managing information security requirements. NIS 2 Article 21(2)(g) and Article 21(2)(h) references cyber hygiene and cryptography.

Security domains define how information is classified, categorised, or administered. The following Security Domains, Sub-Domains, and Measures are related to NIS 2 Article 21(2)(g), and can assist organisations already using other standards and frameworks to comply with NIS 2.

SECURITY DOMAIN: Protection

SECURITY SUB-DOMAIN: IT Security Maintenance

SECURITY MEASURE: IT security maintenance procedure

In an effort to foster higher consistency and reliability across multiple frameworks and the NIS 2, Article 21(2)(g) can be associated with the ISO 27001, NIST CSF, and ISA/IEC 62443 utilising the following cross-references for security maintenance. Cyber hygiene is best attributed to proper maintenance as they are a set of practices and tasks an organisation can execute to keep systems, data, and users safe and well-protected. The following cross-references cover the processes and procedures related to cyber hygiene.

CROSS REFERENCES:

The ISO 27001 references sections within Support, Operation, Improvement, and Annex A, Information Security Controls Reference, specifically the following sections:

- ISO 27001 (7.5.3, 8.1, 10.1, A.11.2.4, A.12.1.2, A.12.6.1, A.14.1.1, A 14.2, A.15.2.2)

The NIST CSF references the following sections within Identify, and Protect.

- NIST CSF (PR.MA -1, 2, PR.IP -1, 2, 3,4, 7, PR.DS -3, 4, ID.SC -4)

The ISA/IEC 62443 references the following sections within Security Function Verification, Software and Information Integrity, Audit Log, and Network and Security Configuration Settings.

- ISA/IEC 62443 (SR 3.1, SR 3.3, SR 3.4, SR 3.8, SR 6.1, SR 7.6)

Additionally, the following cross-references are also related to Security Risk Analysis and should be considered as a reference within NIS 2 Article 21(2)(h) for cryptography.

SECURITY DOMAIN: Protection.

SECURITY SUB-DOMAIN: IT Security Architecture.

SECURITY MEASURE: Cryptography.

In an effort to foster higher consistency and reliability across multiple frameworks and the NIS 2, Article 21(2)(h) can be associated with the ISO 27001, NIST CSF, and ISA/IEC 62443 utilising the following cross-references for vulnerability handling and disclosure. The following cross-references cover the processes and procedures related to cryptography.

CROSS REFERENCES:

The ISO 27001 references sections within Annex A, Information Security Controls Reference, specifically the following sections:

- ISO 27001 (A.10.1, A.18.1.5)

The NIST CSF references the following sections within Identify, and Protect.

- NIST CSF (ID.GV -3, PR.DS -1, 2, 5, 6, 8, PR.PT -4)

The ISA/IEC 62443 references the following sections within Zone Boundary Protection.

- ISA/IEC 62443 (SR 5.2)

Identity and Access Control

Identity and access control are fundamental concepts within information security and system management. Identity refers to the digital representation of a person, device, or entity accessing a system or network. Examples include usernames, email addresses, and digital certificates. Access control is the process of regulating and restricting access to resources or services based on the identity of users or devices. Access control ensures that only authorised users, processes, or systems can access certain resources or perform specific tasks.

Concepts within identity and access control include identity management which is the process and technologies used to create, manage, and authenticate identities throughout the identity lifecycle. Access control typically includes mechanisms such as authentication, authorization, and auditing. These mechanisms verify the identity of users, determine what resources are available to authorised users, and monitor access for security and compliance purposes.

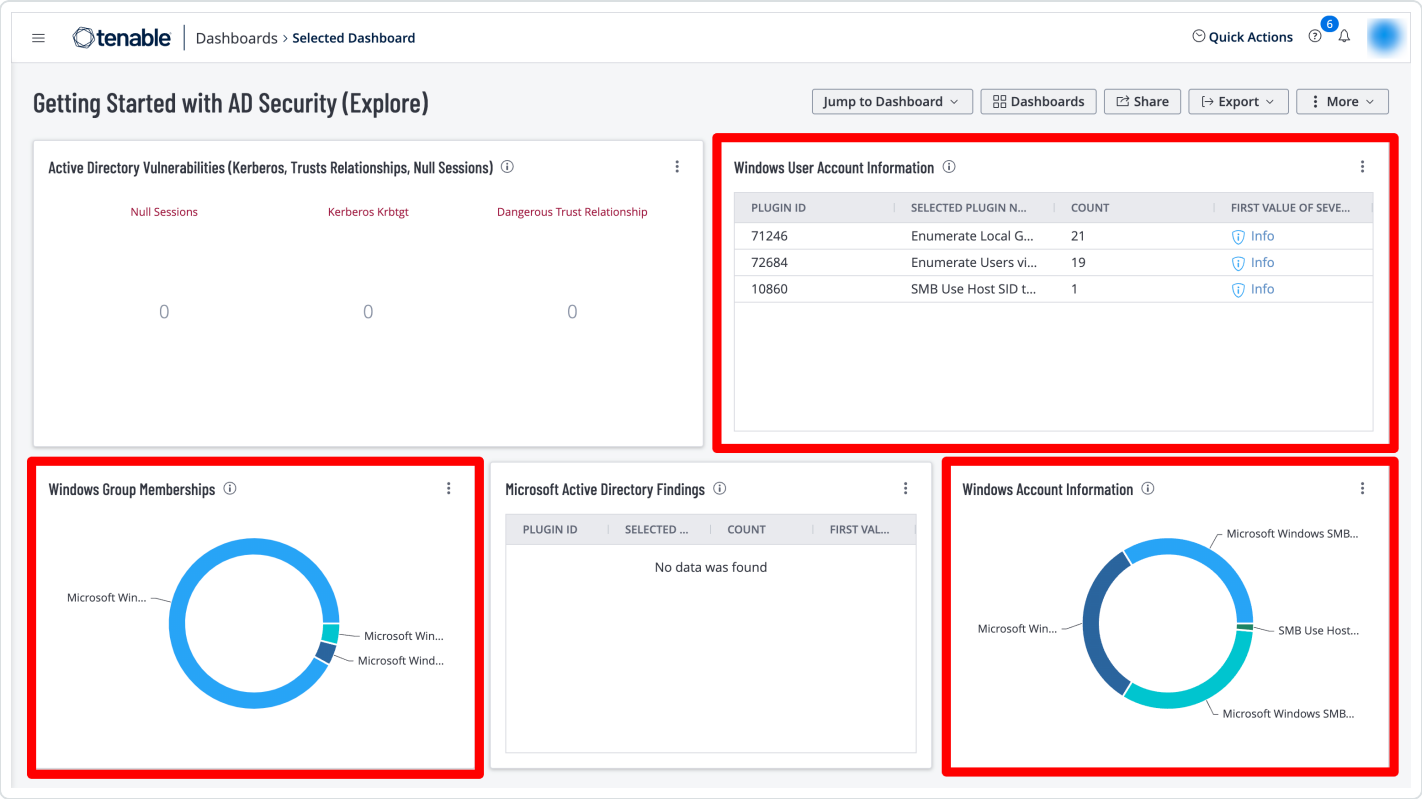
Identity and access control work together to ensure that the correct individual or systems have the appropriate access to resources, while safeguarding against unauthorised access and potential security breaches. These concepts are crucial for maintaining the confidentiality, integrity, and availability of information within the organisation's network.

The following sections within the NIS 2 may be best suited to fall into the Identity and Access Control category:

- Article 21(2)(j): Use of Multi-Factor Authentication or Continuous Authentication Solutions: Multi-factor Authentication (MFA)

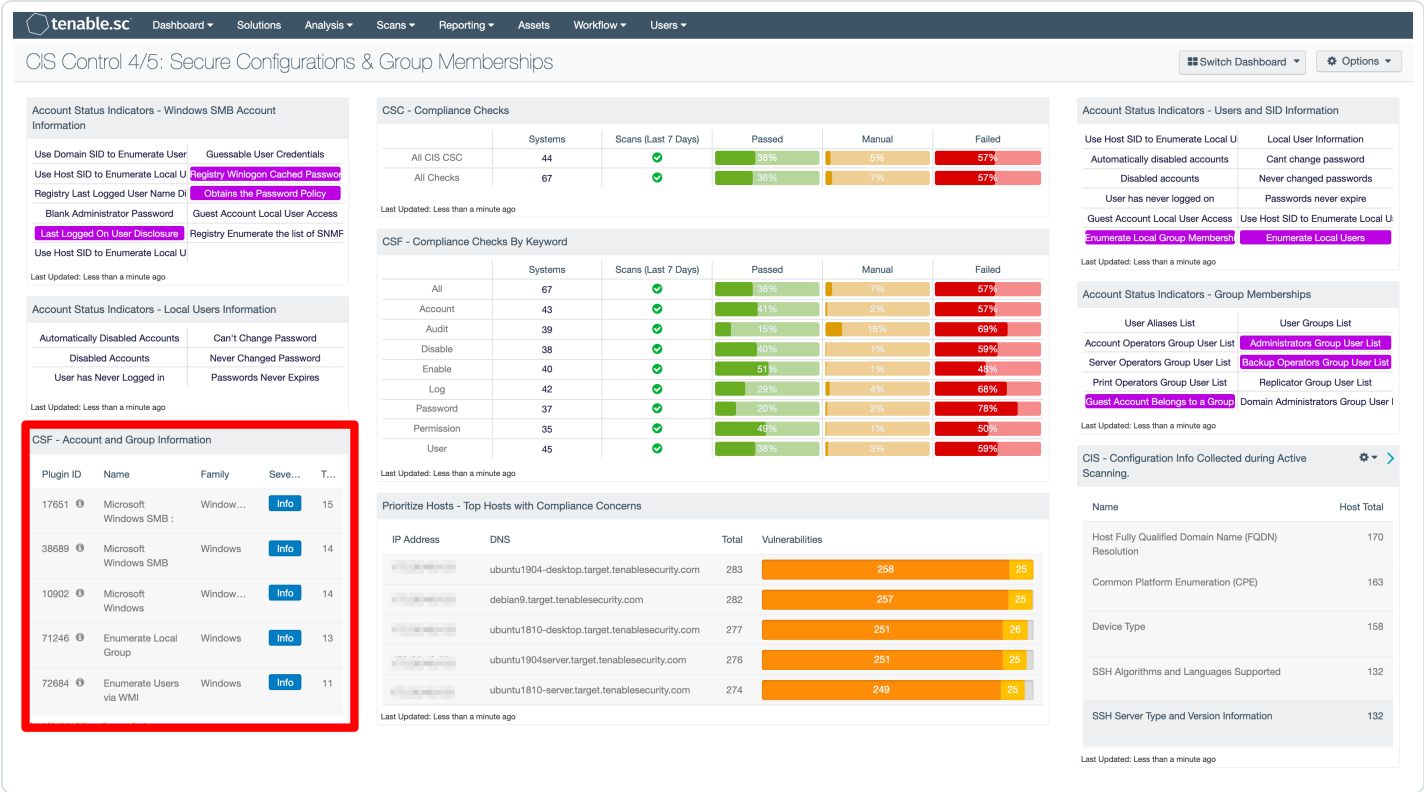
Tenable Identity Exposure provides various methods to access the information collected through the Indicators of Exposure (IoE) and Indicators of Attack (IoA) panes. Tenable Vulnerability Management provides the ability to use the Explore Findings through the use of dashboards and reports.

To begin taking control of the organisation’s Identity Management, every account within the environment must be enumerated. The level of access for each account must also be determined. All 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 widgets to enumerate user accounts.

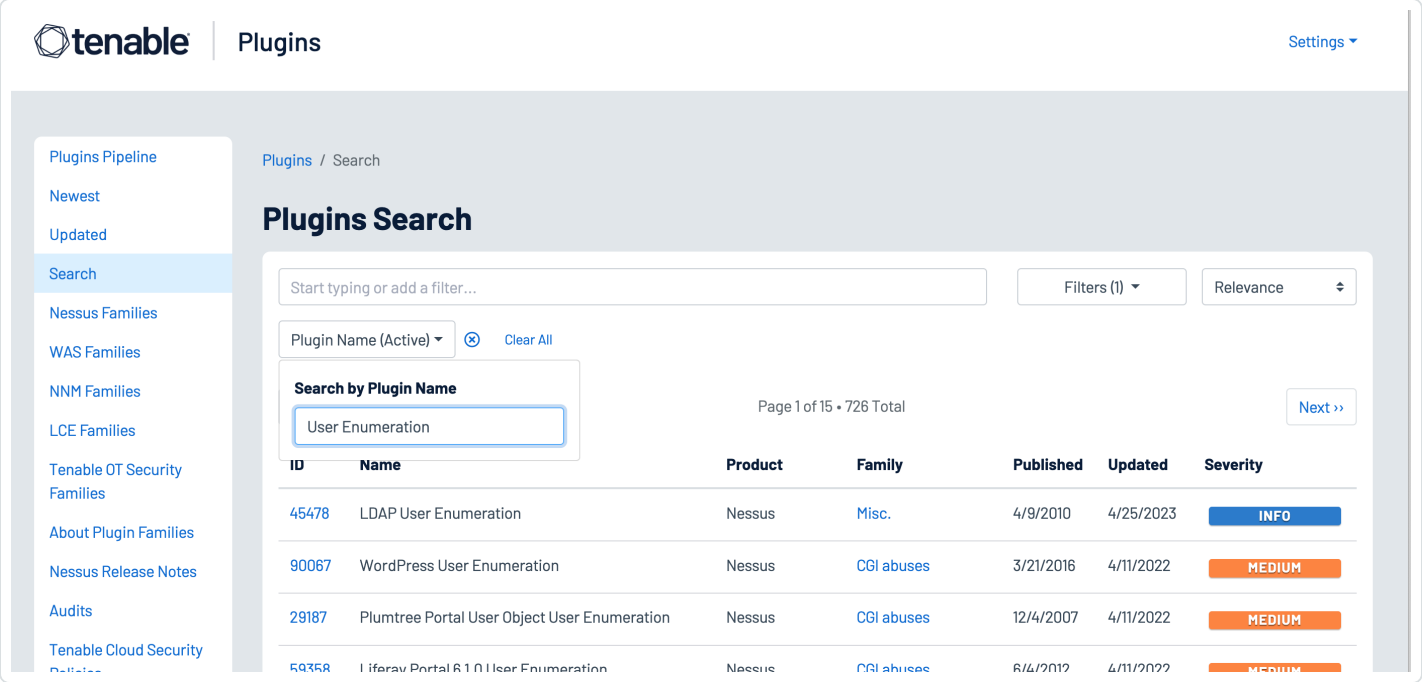
Organisations can also use the CSF - **Account and Group Information** widget located in the **CIS Control 4/5**: **Secure Configurations & Group Memberships** dashboard in Tenable Security Center, which leverages plugins that enumerate Windows account information.



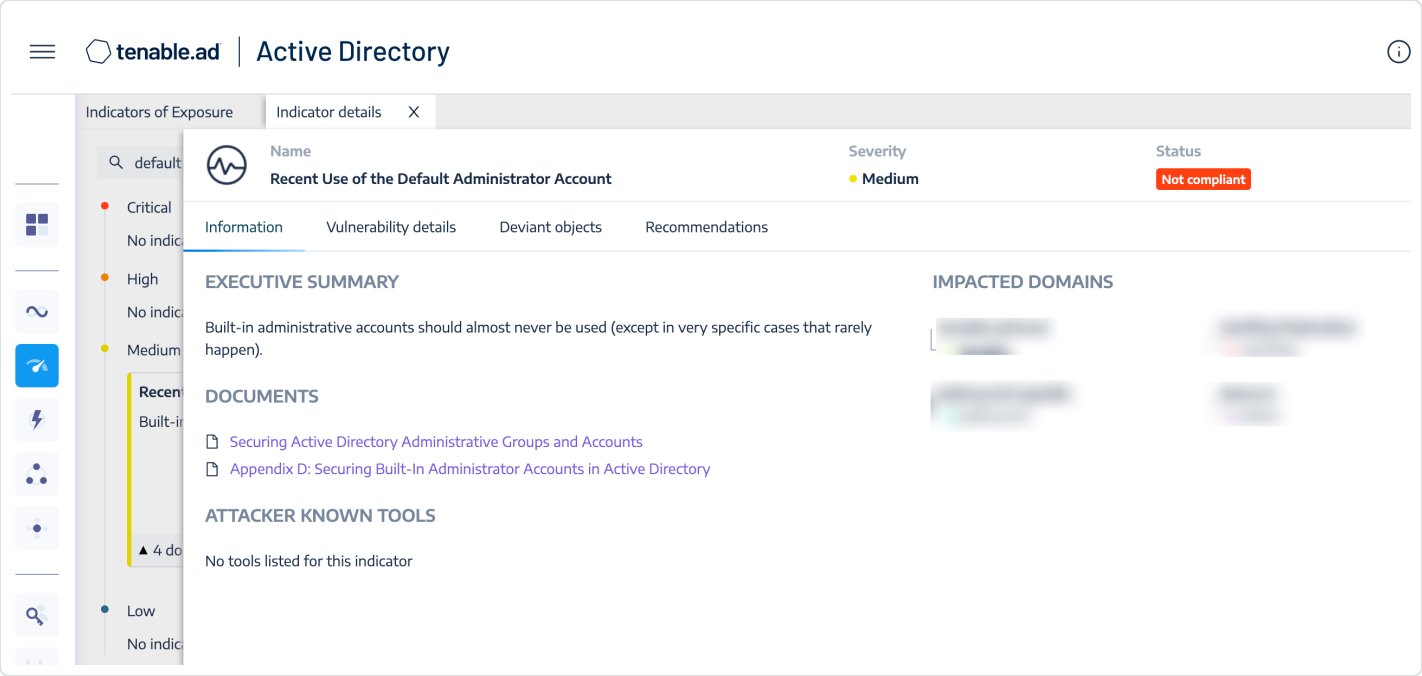
Operating Systems and applications are often distributed with service and default accounts that are either not password-protected or having a default password that is well known. Tenable Nessus and Tenable Identity Exposure help identify these accounts, enabling organisations to review and disable any 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.
- 171959 Windows Enumerate Accounts – This plugin enumerates all Windows Accounts

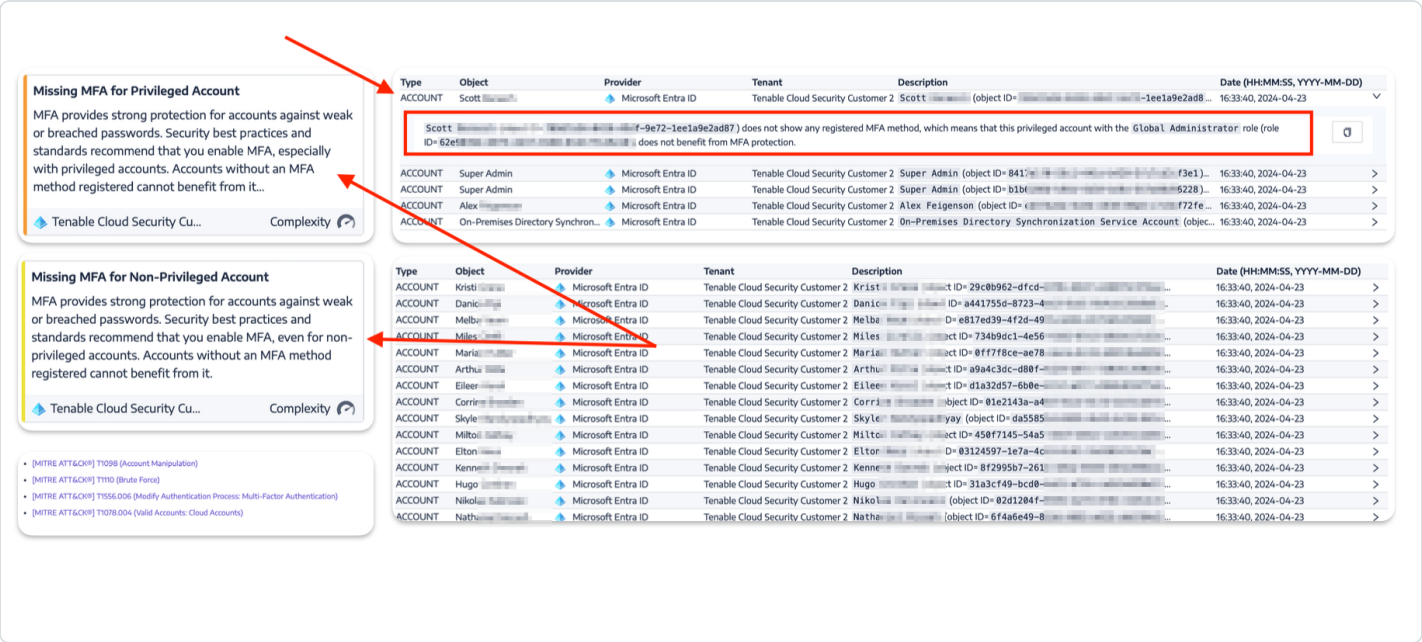
Several hundred plugins can be identified by searching for "Default Account" from the **Nessus Plugins Search** page using the **Enable Default Logins** filter. Nessus default account plugins are available for Databases, Web Servers, SCADA devices, Unix/Linux devices, Cisco devices and more. Many of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



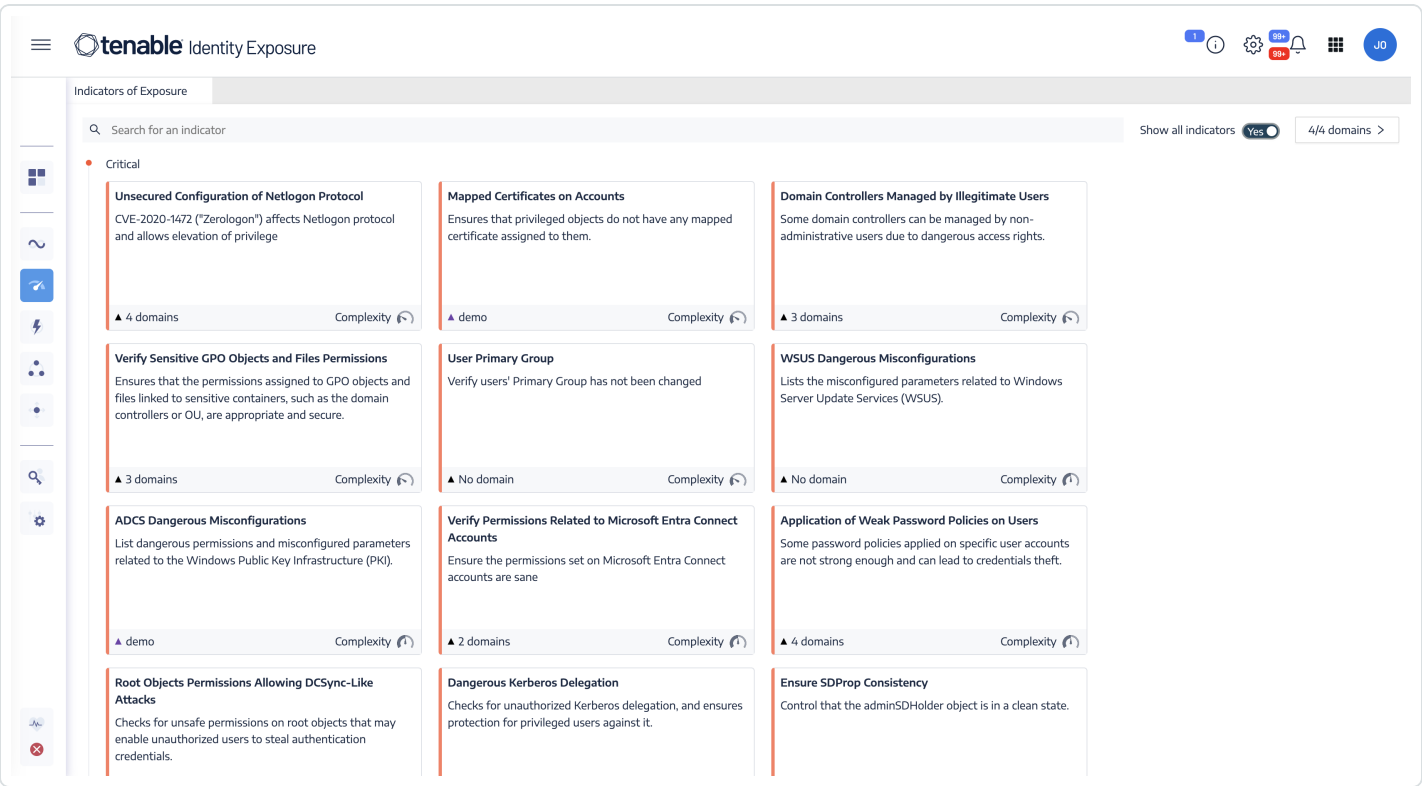
In addition, Tenable Identity Exposure provides the ability to determine if a default administrator account was recently used in the environment, as shown in the image below:



Tenable Identity Exposure is also able to determine if items such as MFA are being used. In this example, a privileged account with a Global Administrators role does not have a registered MFA method. The user account and detailed information on the vulnerability are present to assist organisations mitigate the identified concerns.



Depending on the threat level of the misconfiguration, the Indicator of Exposure (IOE) will rise in a different category: Critical – High – Medium – Low. This provides the context required to minimise distractions. Organisations are able to effectively investigate incidents, hunt for threats, and manage and prioritise security challenges that pose the greatest threats.



For more information on Tenable Identity Exposure review the [documentation located here](#).

For more detailed information review the [Identity and Access Management Cyber Exposure guide found here](#).

Tenable can discover Identity assets and check access policies violation, or excessive privileges on both on-premises AD/EntraID and public clouds (AWS, Azure, GCP) Tenable Cloud Security provides this information via misconfiguration reports for identity and access management, as shown below.

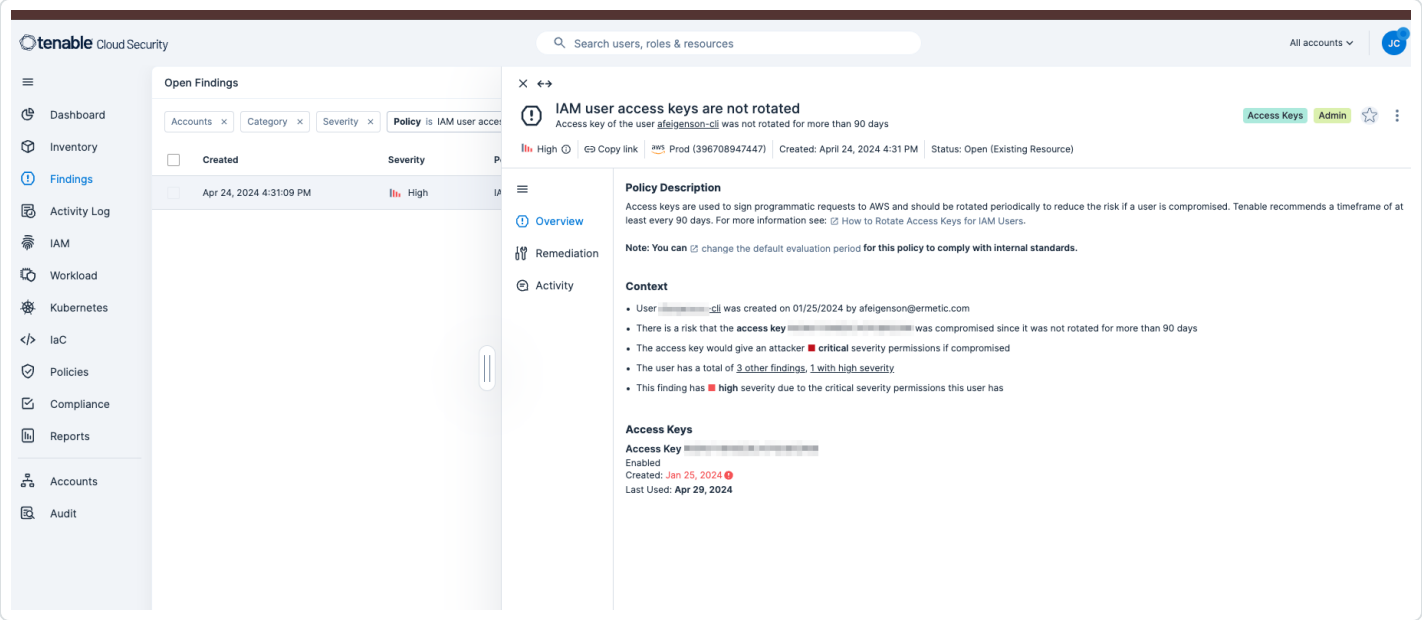
tenable Cloud Security | MISCONFIGURATIONS REPORT

IAM
Policies that detect issues related to identity and access management, such as inactive or overprivileged IAM identities.

Platform	Policy	Compliances	Assessed	Passed	Failed
aws	AWS account support role is not set	CIS	2 Accounts	0	2
aws	IAM access analyzer is not enabled for all regions	CIS	2 Accounts	0	2
aws	IAM server certificate is expired	CIS	0 IAM Server Certificates	0	-
aws	IAM user access keys are not rotated	CIS, ISO, NIST, NIST, NIST, PCI	1 IAM User	0	1
aws	IAM user has multiple active access keys	CIS	24 IAM Users	22	2
aws	IAM user has policies attached	CIS	24 IAM Users	19	5
aws	IAM user MFA is not enabled	CIS, ISO, NIST, NIST, NIST, PCI	15 IAM Users	0	14 1
aws	IAM user unused access keys	CIS, ISO	22 IAM Users	0	19 3

Details within each policy violation contain an overview, policy violation details, and policy remediation strategies, as well as defining any impacted resources. Policies are used to identify

misconfigurations and vulnerabilities present on cloud resources. Tenable Cloud Security has built-in policies for cloud and IaC resources that define the compliance standards for your cloud and IaC infrastructure. Related policies are combined within a policy group. A policy can support multiple benchmarks. Therefore, a policy group includes all the benchmarks supported by the policies in the group.



A full list of Tenable Cloud Security policies is available online located here.

For more information on getting started with Tenable Cloud Security, see the *Tenable Cloud Security User Guide*.

The Insecure Cryptography widget for Tenable OT, located on the compliance dashboard provides an overview of suspicious unauthorised activities at the network's different levels. This widget assists organisations monitor and detect insecure cryptographic events to prevent compromise of sensitive information and service disruption. Key items displayed are Successful Unsecured Logins and Logins Using Unencrypted Credentials, and high risk assets with these events.

The Insecure Communication widget also for Tenable OT, located on the compliance dashboard assists organisations in avoiding any insecure communications and suspicious unauthenticated access. Insecure communications can leave sensitive information or critical assets vulnerable to interception and exploitation by attackers. Unauthenticated access may be a trigger to alert organisations to problems resulting from a potential breach, misconfigured security settings, or unauthorised activity. Key items displayed are Failed Logins and Connections with No Authentication.

Insecure Communication Monitoring

Applies to:

ISO 27001 | Controls: 5.16, 5.17, 6.8

NIS2 Directive (Article 21) | measures: j

Suspicious Authentication Events

Risk Type	Purdue Level 0-1 Assets	Purdue Level 2-3 Assets	Purdue Level 4 Assets
Failed Login	12	6	0
Connection with No Authentication	0	0	0

Show Asset List

The following cross-reference information is provided to derive a more comprehensive and effective approach to managing information security requirements. NIS 2 Article 21(2)(j) references security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure.

Security domains define how information is classified, categorised, or administered. The following Security Domains, Sub-Domains, and Measures are related to NIS 2 Article 21(2)(j), and can assist organisations already using other standards and frameworks to comply with NIS 2.

SECURITY DOMAIN: Protection

SECURITY SUB-DOMAIN: Identity and access management

SECURITY MEASURE: Authentication and identification

In an effort to foster higher consistency and reliability across multiple frameworks and the NIS 2, Article 21(2)(j) can be associated with the ISO 27001, NIST CSF, and ISA/IEC 62443 utilising the following cross-references for identity and access management. The following cross-references cover the processes and procedures related to identity, access management, and authentication and identification.

CROSS REFERENCES:

The ISO 27001 references sections within Annex A, Information Security Controls Reference, specifically the following sections:

- ISO 27001 (A.9.1, A.9.3, A.9.4.1, A.9.4.2, A.9.4.3)

The NIST CSF references the following sections within Protect.

- NIST CSF (PR.AC-1, 4,6, 7, PR.DS -5)

The ISA/IEC 62443 references several sections related to Identification and Authentication, Use Control, and Zone Boundary Protection.

- ISA/IEC 62443 (SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7, SR 5.2)

Learn More

For more information about these topics, see the following resources:

- Cyber Exposure Study, Vulnerability Management
- ENISA Minimum Security Measures for Operators of Essentials Services
- Cyber Exposure Study, Asset Inventory and Discovery