Tenable Cyber Exposure Study - DORA

Last Revised: January 07, 2025

Table of Contents

DORA Regulation

The Digital Operational Resilience Act (DORA) is a European Union (EU) regulation intended to strengthen the Information and Communications Technology (ICT) of the financial sector.

Summary

In 2020 the European Commission introduced a set of regulatory proposals to support digital innovation and modernise the European Union's (EU) financial sector. The Digital Finance Package (DFP) strives to position the EU as a leader in digital finance innovation, while protecting customers and safeguarding financial stability. The DFP includes four main components:

1. **Regulation on Markets in Crypto-Assets (MiCA)** - The goal of MiCA is to establish a regulatory framework for crypto-assets and related services.
2. **Digital Operational Resilience Act (DORA)** - The goal of DORA is to ensure that financial institutions and service providers within the EU can withstand, respond, and recover from operational threats and disruptions.
3. **Pilot Regime for Distributed Ledger Technology (DLT)** - The goal of DLT is to create a temporary framework for financial institutions to experiment with blockchain and other DLTs to evaluate risks.
4. **Retail Payments Strategy (RPS)** - The goal of RPS is to support the development of efficient payment solutions for the EU.

The focus of this Cyber Exposure Study is on DORA. The regulation, which will come into force on 17th January 2025, imposes obligations on financial entities, but also on their digital service providers, which must review their procedures, contracts, mechanisms and tools on a regular basis to ensure information systems security. DORA was originally adopted in 2022. DORA ensures that financial institutions can withstand, respond, and recover from all types of ICT related disruptions, thereby enhancing the operational resilience of all financial systems across the EU. The Digital Operational Resilience Act (DORA) is a European Union (EU) regulation intended to strengthen the Information and Communications Technology (ICT) of the financial sector.

Scope

DORA applies to a wide range of financial entities including (See DORA Article 2 for a complete list):

- Banks
- Payment Services Provider
- Investment Firms
- Insurance Companies
- and other financial market infrastructures.
- ICT Service providers such as Cloud Providers, Data Centers, and Software Providers who support financial institutions are also included.
- HOWEVER, DORA does not apply to all financial institutions, as DORA does not apply to
    - Small enterprises, that employs 10 or more persons, but fewer than 50 persons, and have an annual turnover and/or annual balance sheet total that exceeds EUR 2 million, but do not exceed EUR 10 million;
    - medium-sized enterprises, that employ fewer than 250 persons and have an annual turnover that does not exceed EUR 50 million and/or an annual balance sheet that does not exceed EUR 43 million;
    - or
    - microenterprises, which employs fewer than 10 people and have an annual turnover and/or annual balance sheet total that do not exceed EUR 2 million

DORA represents the first attempt to streamline ICT risk management in the financial sector in the EU. Other EU legislation such as the General Data Protection Regulation (GDPR), and the Network and Information Systems Directive (NIS) is principle based. Rather, DORA contains detailed lists of requirements including additional documents called Regulatory Technical Standards (RTS). Where DORA differs from the NIS/NIS2 is the sectors that are applicable. NIS applies to the critical infrastructure sectors and DORA applies only to financial sectors and is critical for third-party ICT providers. Any overlap between the two are addressed via a *lex specialis* exemption, meaning that in case of conflict, DORA applies first.

Notes related to Requirement 3: This requirement is related to the controls around account data that is printed or stored in any form. Account data is both cardholder data and sensitive authentication data. While this requirement is not supported by Tenable directly, the recommended practice here is to keep storage of account data to a minimum. Do not store sensitive authentication data (SAD) after authorization. Restrict

he display of the full primary account number (PAN) and cardholder data. And secure the PAN, account data, and any cryptographic keys used to protect the data when they are stored.

Getting Started

Getting started with the Digital Operational Resilience Act involves developing a comprehensive approach to ICT risk management which aligns with DORA's requirements. DORA covers policies, procedures, tools, strategies, roles and responsibilities, to managing ICT risk within the financial sector. To begin, financial entities must understand the DORA regulation, especially sections relevant to an organisation's sector and size.

Key Pillars

Overall, DORA comprises nine Chapters, and contains 64 Articles, based on the current text at the time of this writing. In addition, the European Union has introduced regulations supplementing the above regulation. These are:

- Regulatory Technical Standards (RTS) and
- Implementing Technical Standards (ITS)

DORA contains 5 Key Pillars that provide a structured approach to enhance ICT agility and bolster ICT risk management frameworks for financial entities.

These pillars are:

1. ICT Risk Management (Chapter II, Article 5-16)
    a. Financial institutions are required to implement robust ICT risk management frameworks, and must assess and mitigate risks related to ICT systems and processes, to manage cyber threats and ensure business continuity.
2. ICT Incident Reporting (Chapter III, Article 17-33)
    a. DORA introduces mandatory reporting requirements for ICT related incidents. Financial entities must report, in a timely manner, major incidents to their national authorities.
3. Digital Operational Resilience Testing (Chapter IV, Article 24-27)
    a. Institutions must regularly test the effectiveness of their ICT systems to ensure resilience against disruptions, including stress tests and simulation exercises.
4. ICT Third Party Risk Management (Chapter V, Article 28-44)

a. Third party ICT Providers must meet the same operational requirements. There must be appropriate monitoring and oversight.

5. Information Sharing (Chapter VI, Article 45)

    a. Fostering information sharing and collaboration within the financial sector.

Comparisons Between DORA and NIS2

DORA and the NIS2 Directive are both part of the EU's efforts to enhance cybersecurity across critical sectors. However, they differ in scope, focus, and the industries they regulate. Article 1(2) of DORA provides that, in relation to financial entities covered by the NIS 2 Directive and the corresponding rules, DORA shall be considered sector-specific. This statement is mirrored in recital (28) of the preamble to the NIS 2 Directive, which states that DORA should be considered a sector-specific Union legal act in relation to the NIS Directive with regard to financial entities.

In terms of the financial institution, DORA will apply instead of NIS 2 in most of the cases. When dealing with ICT risk management (Article 6), management of ICT related incidents, and major ICT related incident reporting (Article 17), digital resilience testing (Article 24), information sharing (Article 25), and ICT third-party risk (Article 28), DORA provisions shall apply instead of those provided by the NIS 2 Directive for financial entities. Understanding how DORA and NIS 2 compare is an important step towards compliance.

Here is a comparison of the two.

First, what is the difference between a Directive and a Regulation?

Directives, such as the NIS 2, are legislative acts that set out a goal that EU countries must achieve.. Implementation of those standards are left to the member states, whether by law, regulation or other initiative. The EU merely sets the deadlines for implementation.

Regulations, such as DORA, are binding legislative acts. These must be applied in their entirety across the EU. as if they were a local law. Member states may pass their own laws for implementation, but the regulation will apply regardless.

Scope

DORA: Focus is exclusively on the financial sector.

NIS2: Focus is broader, covering essential and important entities in multiple sectors beyond just financial services (energy, transport, healthcare, and more).

Focus and Purpose

DORA: Specific focus within the financial sector is on managing ICT risks, such as cyberattacks, IT system failures, and third-party dependencies. DORA ensures that financial entities have frameworks in place to prevent, respond, and recover from disruptions. Specific reporting

requirements for ICT related incidents are defined. Stress testing and third party risk management are also included.

NIS2: Specific focus is on enhancing cybersecurity and network information systems security across all critical sectors in the EU. NIS2 strives to improve the overall resilience of essential services, making sectors less vulnerable to cybersecurity threats, improving cybersecurity and cross border collaboration between member states. NIS2 also establishes reporting obligations for entities with significant cybersecurity incidents that affect confidentiality, integrity, or availability of networks and systems.

Third-Party Risk Management

DORA: Introduces requirements for financial entities to manage risks arising from their third-party ICT service providers (cloud computing, software vendors)

NIS2: Similar requirements for third-party providers to meet security standards, but on a broader scale, aimed at protecting entities in a variety of critical sectors, not just financial services.

Supervision and Enforcement

DORA: Financial entities and their ICT providers will be supervised by both national financial authorities and European Supervisory Authorities (ESAs), which are European Banking Authority (EBA), European Insurance and Occupational Pensions Authority (EIOPA) and European Securities and Markets Authority (ESMA). Financial regulators will monitor compliance and impose sanctions on entities that fail to meet the operational resilience standards within DORA.

NIS2: Supervision and enforcement are conducted by national authorities in each EU member state, who are responsible for monitoring compliance across sectors. NIS2 penalties and sanctions for non-compliance are more stringent.

Summary of Key Differences

DORA is tailored to the financial industry's unique needs. The NIS2 Directive is a more general framework applicable across multiple critical sectors, strengthening the role of the EU Agency for Cybersecurity (ENISA). DORA while specific to the financial sector emphasises operational resilience, ICT risk management, and third-party dependencies within financial services. NIS2 is much broader, focuses on a range of critical industries, and an emphasis on network and information security. Both strengthen resilience to cyber threats.

How Tenable Helps

Tenable assists organisations who are required to comply with DORA by providing the information required to address compliance within Chapter II, ICT Risk Management, and Chapter IV Digital Operational Resilience Testing. Chapter V, Managing of ICT third-party risk, largely covers procedures, and contractual provisions, however, Tenable can assist financial institutions in the identification of third party software vendors, hardware vendors, and cloud service providers. In addition to that, Tenable offers solutions that can help meet the RTS requirements in terms of risk management.

ICT Risk Management

ICT Management can be broken down into 2 areas, risk management and incident reporting. Key elements within these areas is the organisation's ability to identify and prioritise gaps and risks, including implementation of plans to outline the steps, timelines, and resources required to address the identified risks. A significant portion of DORA outlines requirements for policies and procedures, and are therefore not measurable by scanning. However, a number of items can be checked, validated, measured, and tracked. Those requirements which can be supported in all or part include:

Chapter II, ICT Risk Management

- Article 5.1 2. The management body of the financial entity shall define, approve, oversee and be responsible for the implementation of all arrangements related to the ICT risk management framework referred to in Article 6(1).
- Article 8, Identification, says:
    - 1. As part of the ICT risk management framework referred to in Article 6(1), financial entities shall **identify, classify and adequately document** all ICT supported business functions, roles and responsibilities, the information assets and **ICT assets** supporting those functions, and their roles and dependencies in relation to ICT risk. Financial entities shall review as needed, and at least yearly, the adequacy of this classification and of any relevant documentation.
    - 2. Financial entities shall, on a continuous basis, identify all sources of ICT risk, in particular the risk exposure to and from other financial entities, and **assess cyber threats and ICT vulnerabilities relevant to** their ICT supported business functions, information assets and **ICT assets**. Financial entities shall review on a regular basis, and **at least yearly, the risk scenarios impacting them**.
    - 3. Financial entities, other than microenterprises, **shall perform a risk assessment upon each major change in the network** and information system infrastructure, in the processes or procedures affecting their ICT supported business functions, information assets or ICT assets.
    - 7. Financial entities, other than microenterprises, shall on a regular basis, and **at least yearly, conduct a specific ICT risk assessment on all legacy ICT systems** and, in any case before and after connecting technologies, applications or systems.

Chapter IV, **Digital operational resilience testing**, Article 25

1. (...) execution of appropriate tests, such as vulnerability assessments and scans;
2. Central securities depositories and central counterparties shall **perform vulnerability assessments before any deployment or redeployment of new or existing applications** and infrastructure components, and ICT services supporting critical or important functions of the financial entity;
3. Microenterprises shall perform the tests (...) on the one hand, and the urgency, **type of risk, criticality of information assets and of services provided**, as well as any other relevant factor, including the financial entity's ability to take calculated risks, on the other hand.

In addition to DORA, Regulatory Technical Standards called ***Commission Delegated Regulation (EU) 2024/1774 of 13 March 2024*** supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework states in the **Article 10 on Vulnerability and patch management** the following:

1. As part of the ICT security policies, procedures, protocols, (...) financial entities shall **develop, document, and implement vulnerability management procedures**.
2. (b) ensure the performance of **automated vulnerability scanning and assessments** on ICT assets (...), For the purposes of point (b), financial entities shall perform the automated vulnerability scanning and assessments on ICT assets for the ICT assets supporting critical or important functions on **at least a weekly basis**.
    - (c) verify whether:

      (i) **ICT third-party service providers handle vulnerabilities** related to the ICT services provided to the financial entity;
    - (f) **prioritise the deployment of patches** and other mitigation measures **to address the vulnerabilities identified**;
    - (g) **monitor and verify the remediation of vulnerabilities**;
    - (h) require the **recording of any detected vulnerabilities affecting ICT systems** and the monitoring of their resolution.

Prioritising Risk

One of the hardest tasks to accomplish is proper risk prioritisation and communication of risks and vulnerabilities. In addition to the Articles previously listed, the following DORA Articles are related to risk prioritisation efforts including risk based vulnerability management:

- Article 8.3, Financial entities, other than microenterprises, shall perform a risk assessment upon each major change in the network and information system infrastructure
- Article 9.4(b), Financial entities shall follow a risk-based approach, establish a sound network and infrastructure management structure using appropriate techniques, methods and protocols
- Article 16.1 (d), allow sources of ICT risk and anomalies in the network and information systems to be promptly identified and detected

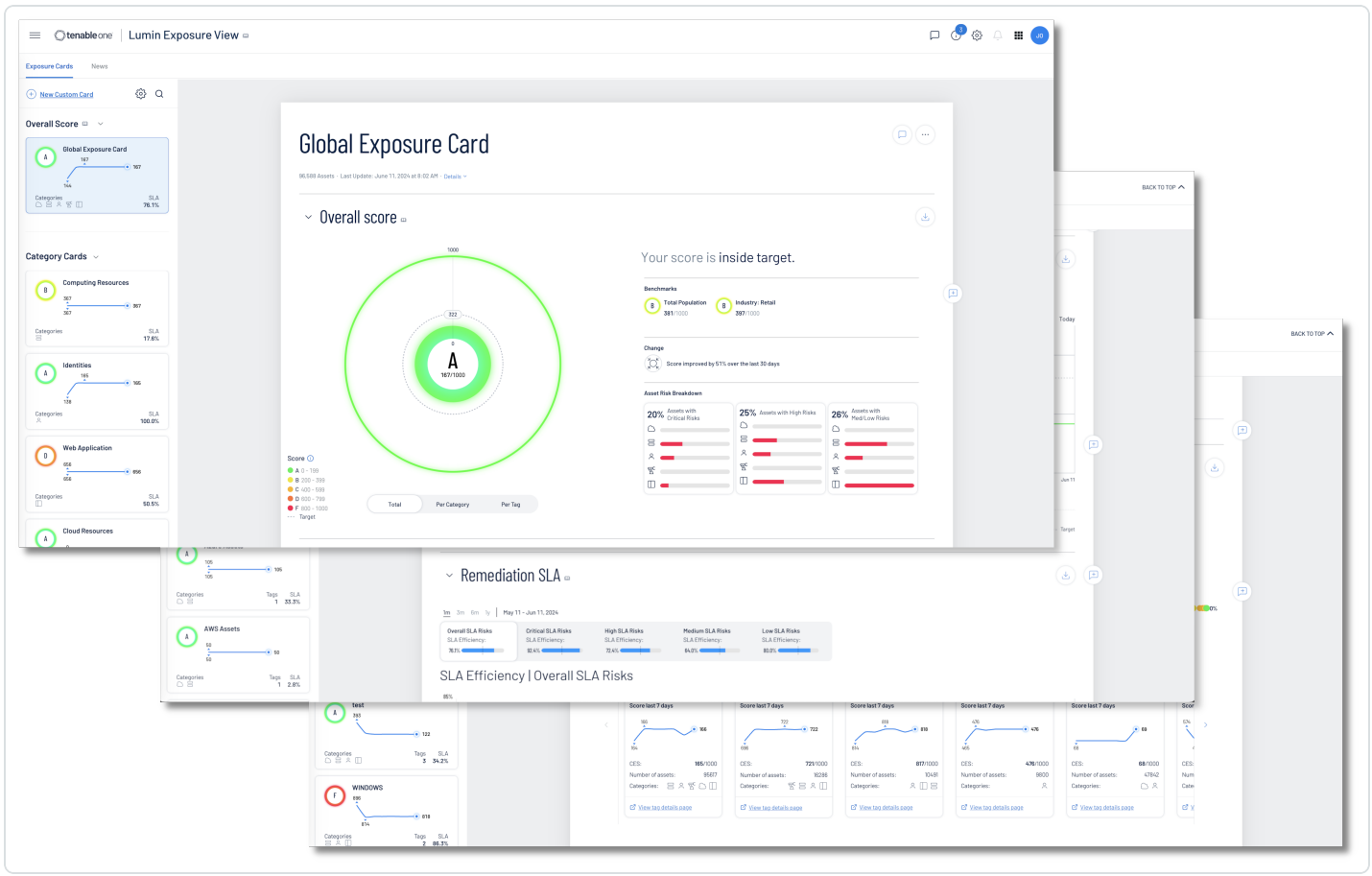
In this section the following Tenable products will be highlighted:

- Lumin Exposure View
- Tenable Security Center
- Tenable Vulnerability Management

Lumin Exposure View

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



For more in-depth information on prioritising risk with Lumin Exposure view, refer to the following Risk Assessment section of the NIS 2 Cyber Exposure Study. Also, you can follow this link for more information on Lumin Exposure View.

Risk Based Vulnerability Management

Risk-Based Vulnerability Management (RBVM) is a process that reduces vulnerabilities across the attack surface by prioritising remediation based on the risks they pose to the organisation. Unlike legacy vulnerability management, risk-based vulnerability management goes beyond discovering vulnerabilities, by helping organisations understand vulnerability risks, by introducing threat context and insight into potential business impact.

RBVM eliminates guesswork, by taking a risk-based approach to vulnerability management, security teams can focus on the vulnerabilities and assets that matter most and address the organization's true business risk instead of wasting valuable time on vulnerabilities attackers may not likely exploit. If you're new to risk-based vulnerability management, check out this comparison guide. The guide breaks down the differences between legacy vulnerability management and risk-based vulnerability

management with insight into how a risk-approach can make your organisation's vulnerability management program more efficient and effective. In addition to the Articles previously listed, the following DORA Articles are related to vulnerability management efforts:

- Article 8.2, Financial entities shall, on a continuous basis, identify all sources of ICT risk
- Article 8.3,Financial entities shall identify all information assets and ICT assets, including those on remote sites, network resources and hardware equipment
- Article 9.1, Financial entities shall continuously monitor and control the security and functioning of ICT systems and tools
- Article 10.1, Financial entities shall have in place mechanisms to promptly detect anomalous activities
- Article 16.1 (b), continuously monitor the security and functioning of all ICT systems

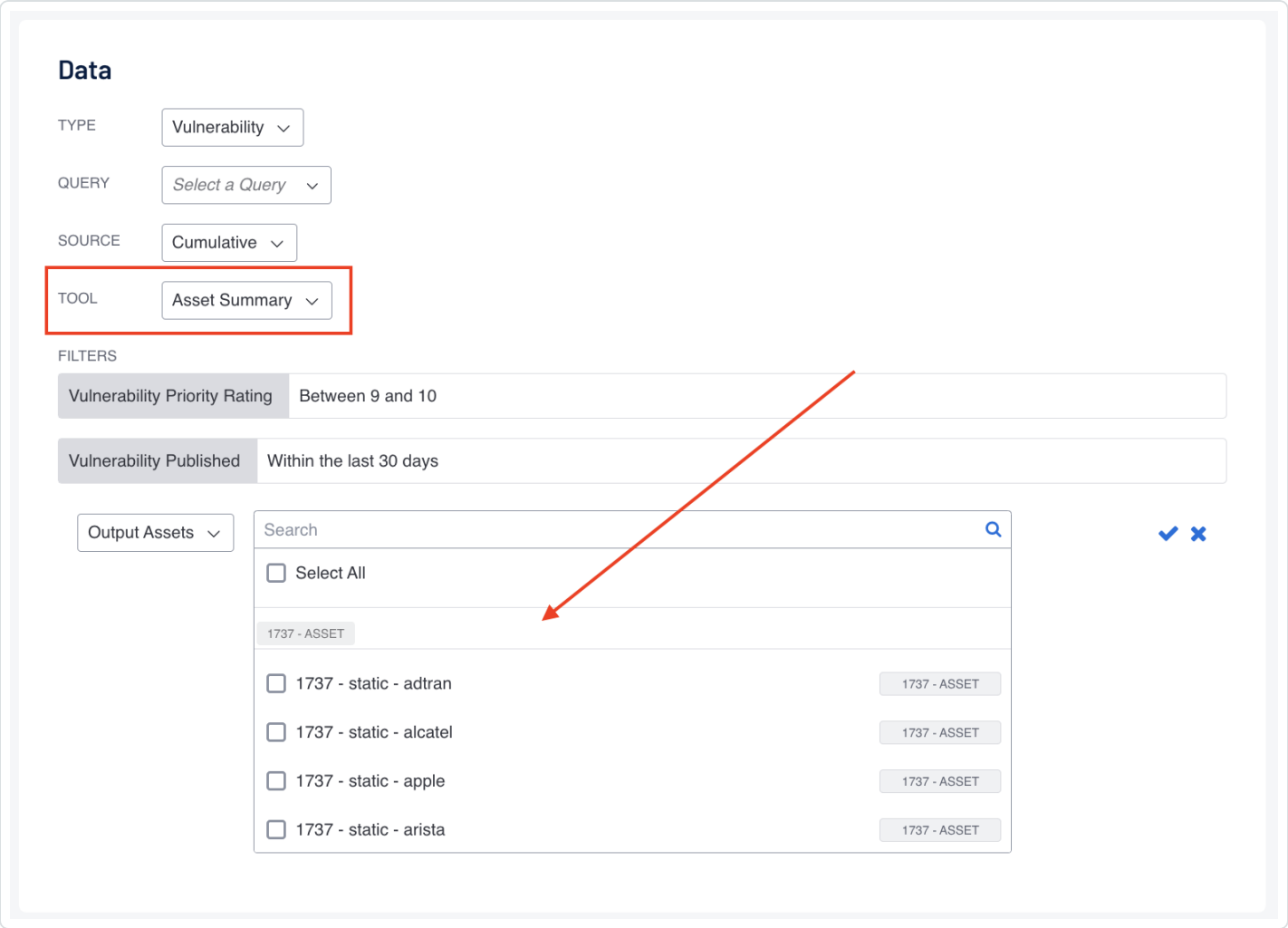
In this section the following Tenable products will be highlighted:

- Tenable Security Center
- Tenable Vulnerability Management

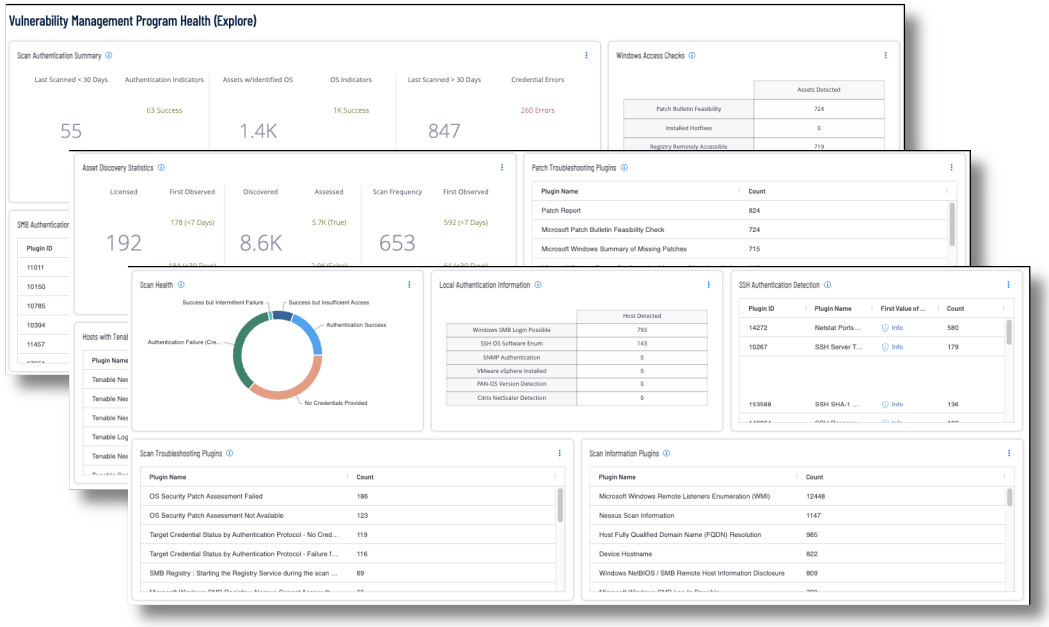
With the principles of Cyber Exposure Management in mind, dashboards, such as the InfoSec Team - One Stop Shop Comprehensive Attack Surface dashboard for Tenable Security Center helps the organisation team maintain a high level of awareness and vigilance. The filters and components are tailored to guide teams in detecting, predicting, and acting to reduce risk across their entire attack surface. Information security teams are empowered to analyse findings, remediate identified risks, track progress, and measure success against the organisation's charter and SLAs.

Organizations 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. 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.



For Tenable Vulnerability Management, dashboards such as the Vulnerability Management Program Health dashboard 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 more information, see the Vulnerability Management Cyber Exposure Study.

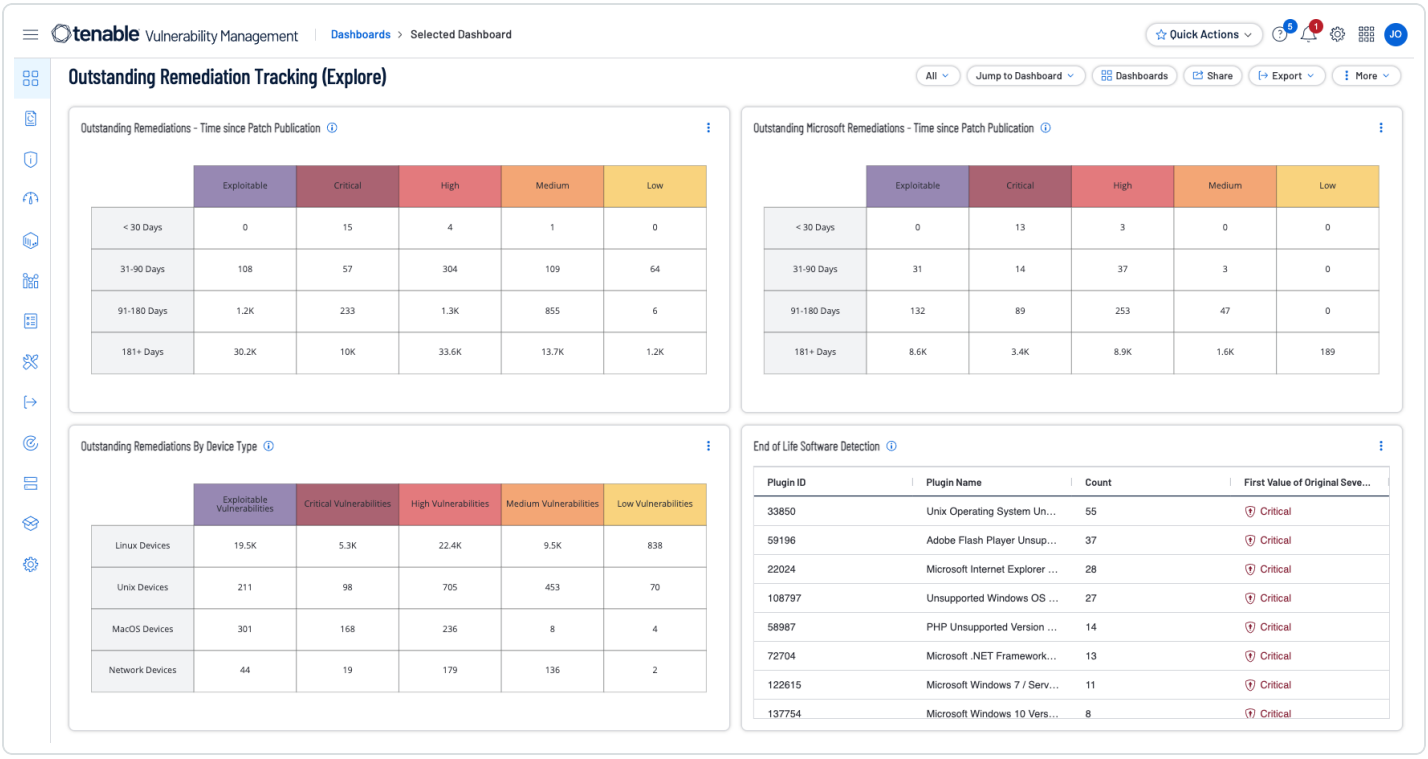
Remediation Tracking

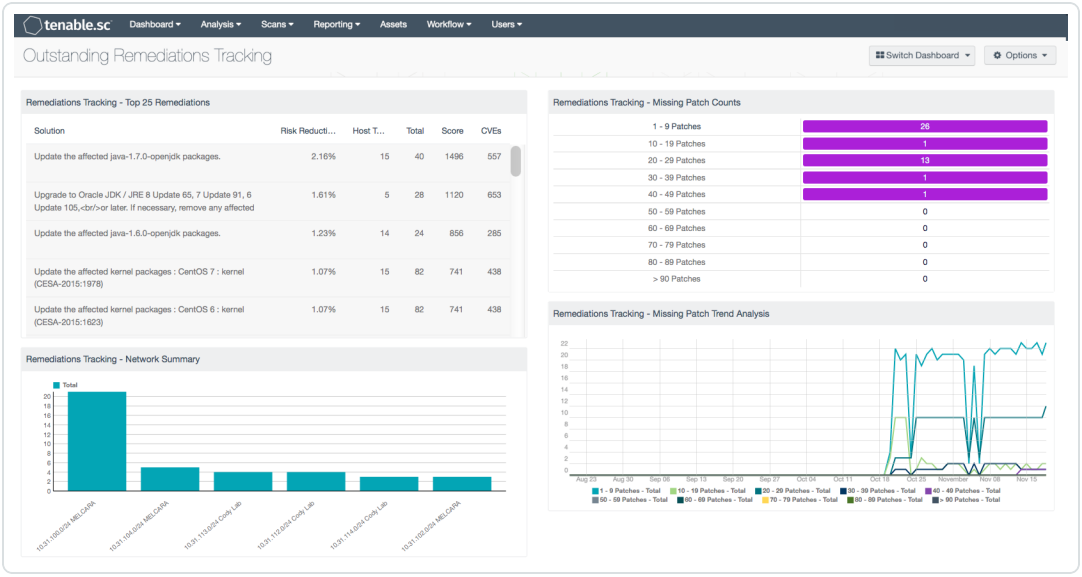
Unpatched assets expose organisations to vulnerabilities that are actively being exploited. End of life assets may pose the greatest risk since they are unsupported and no longer receiving security updates or support from the vendor. Tenable provides the Outstanding Remediation Tracking dashboard for Tenable Vulnerability Management and Outstanding Remediations Tracking. In addition to the Articles previously listed, the following DORA Articles are related to remediation tracking efforts:

- Article 9.4(f), have appropriate and comprehensive documented policies for patches and updates

In this section the following Tenable products will be highlighted:

- Tenable Security Center
- Tenable Vulnerability Management



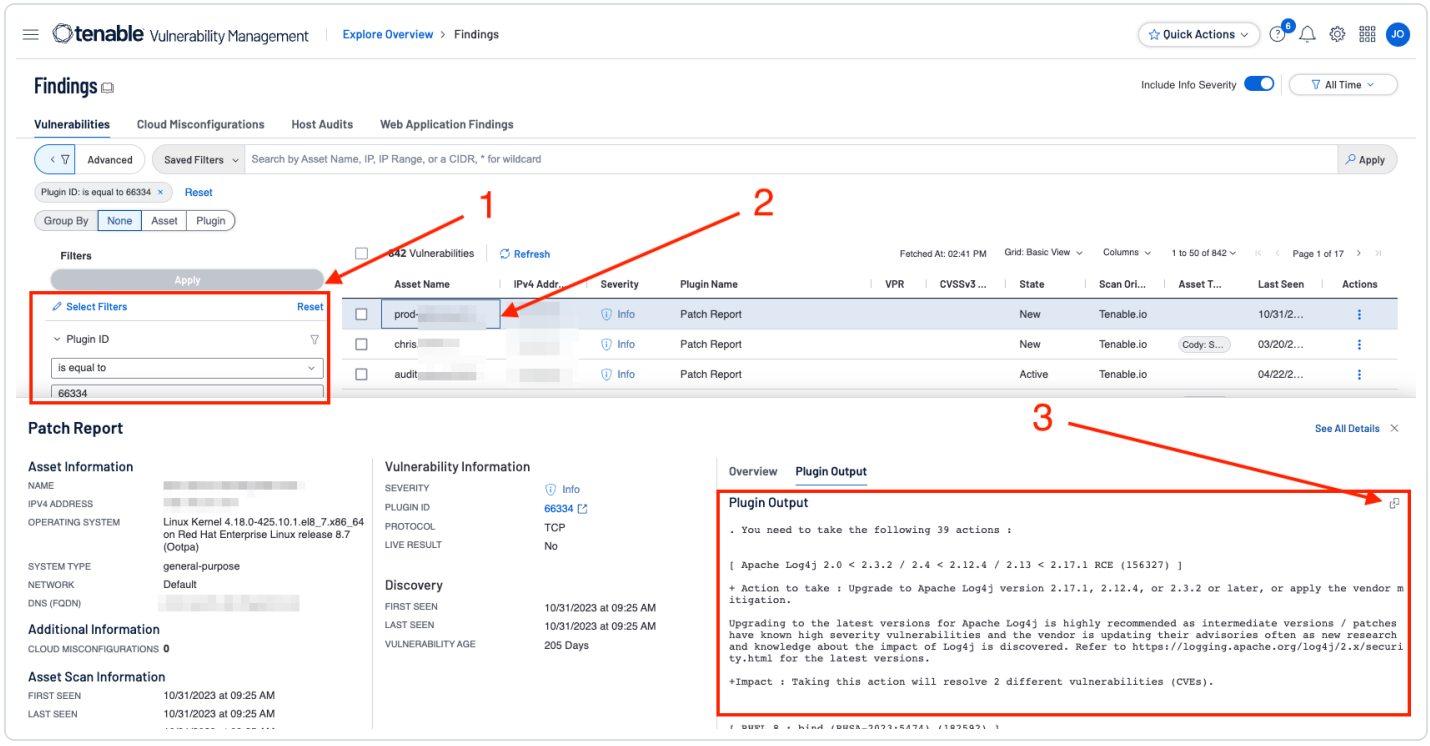


The Outstanding Remediations Tracking dashboard provides risk guidance using the “Remediation Summary” tool. This tool works by employing a concept called “top patch”. Tenable.sc uses proprietary technology to identify a chain of patches. The first patch in the chain is called the “top patch.” If the “top patch” is applied, all subsequent vulnerabilities will also be remediated at the same

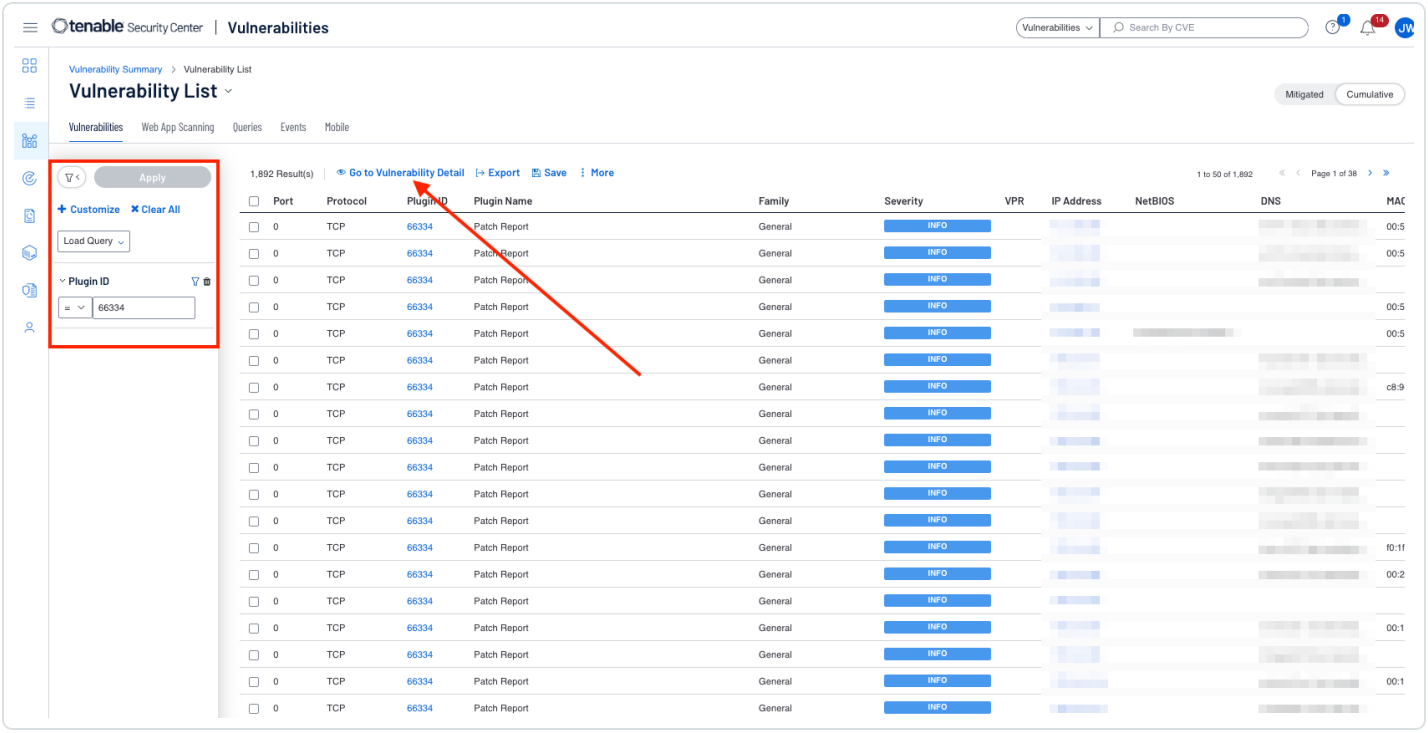
time. Using both the Remediation Summary tool and “Patch Report” plugin, the organisation can better plan remediation efforts. Within Tenable Vulnerability Management several filters are used including those for unsupported products, patch publication date ranges.

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.

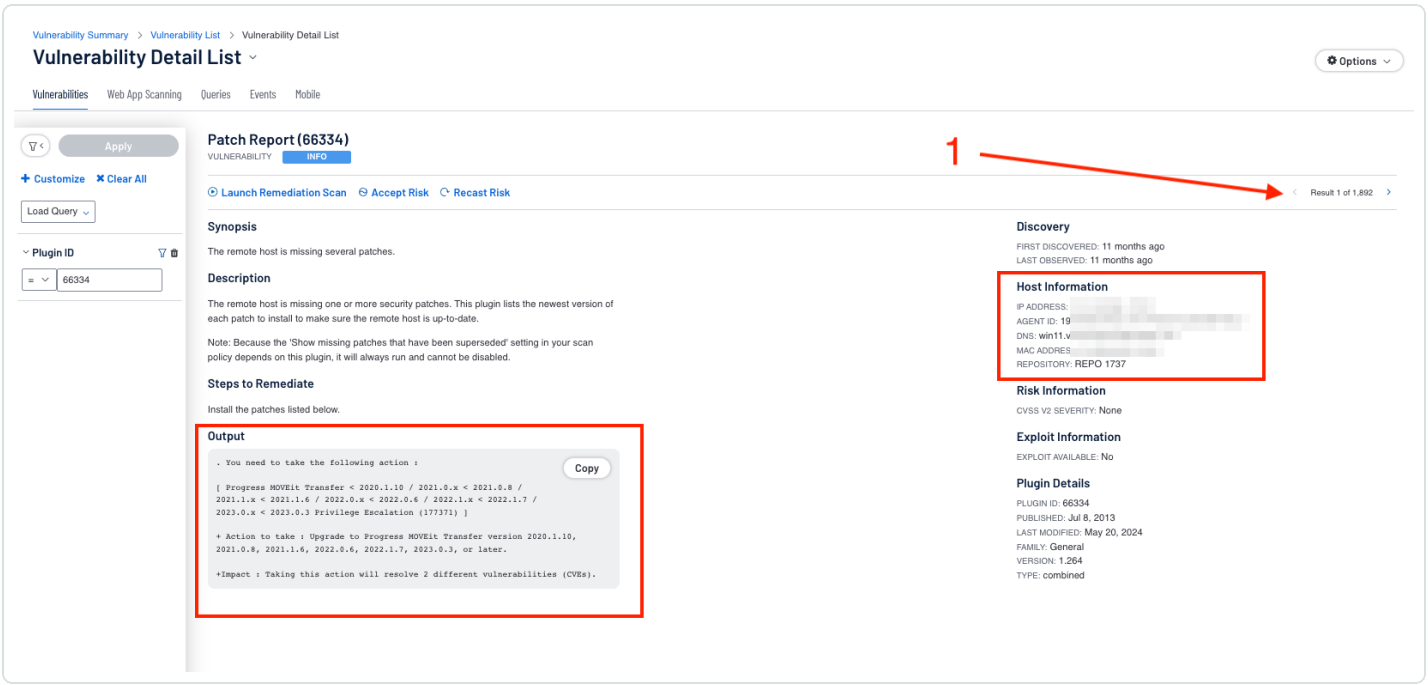
Within **Tenable Vulnerability Management**, analysts can create a filter for plugin 66334 within the filters component on the **Findings** page as shown following (1). Once results have appeared, selecting an asset (2) by clicking on the asset name opens the details window at the bottom of the page. Selecting Plugin Output reveals the detailed Actions to undertake, including the Impact those actions have. The information can easily be exported to the clipboard 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.



For more information related to Remediation Tracking refer to the NIS 2 Cyber Exposure Study section on IT Security Maintenance located here.

Asset Inventory and Discovery

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:

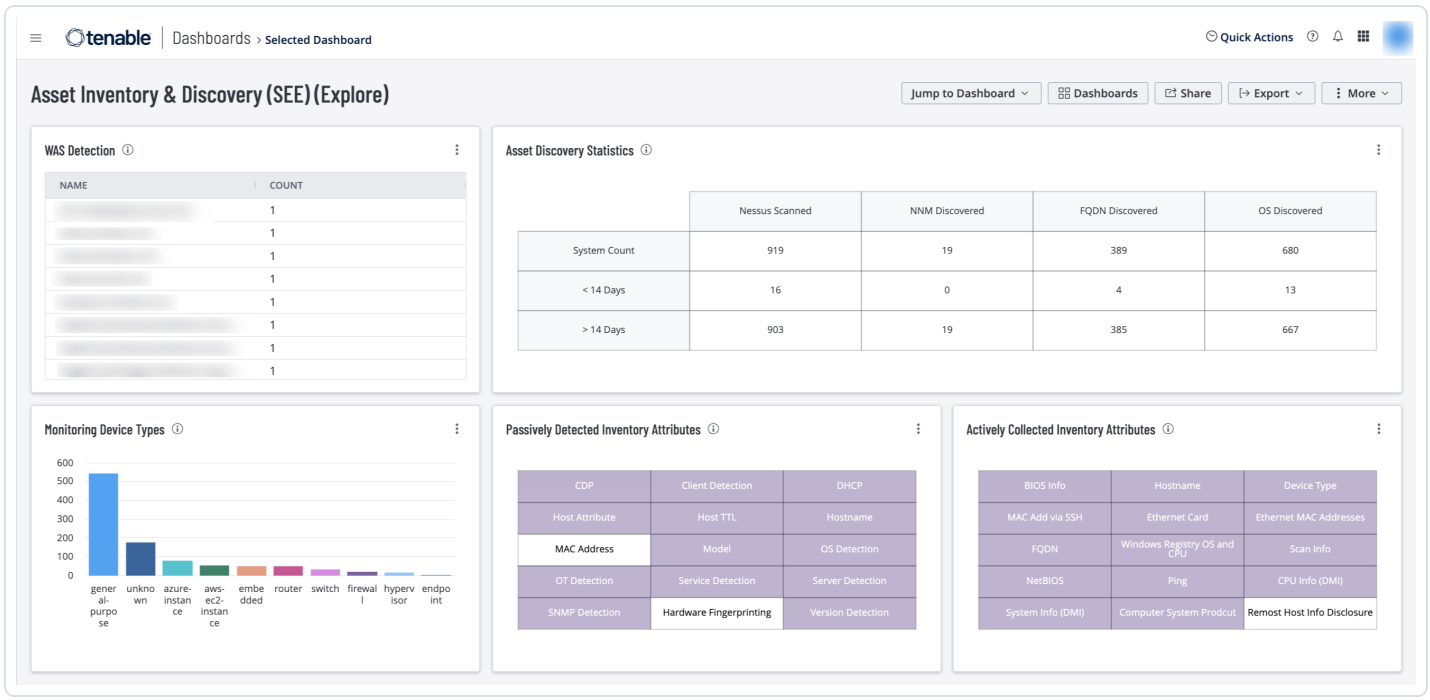
- Actively and passively detected assets
- Asset discovery statistics
- Detected web applications
- Indications for device types (printers, cameras, routers, firewalls, WAPs)

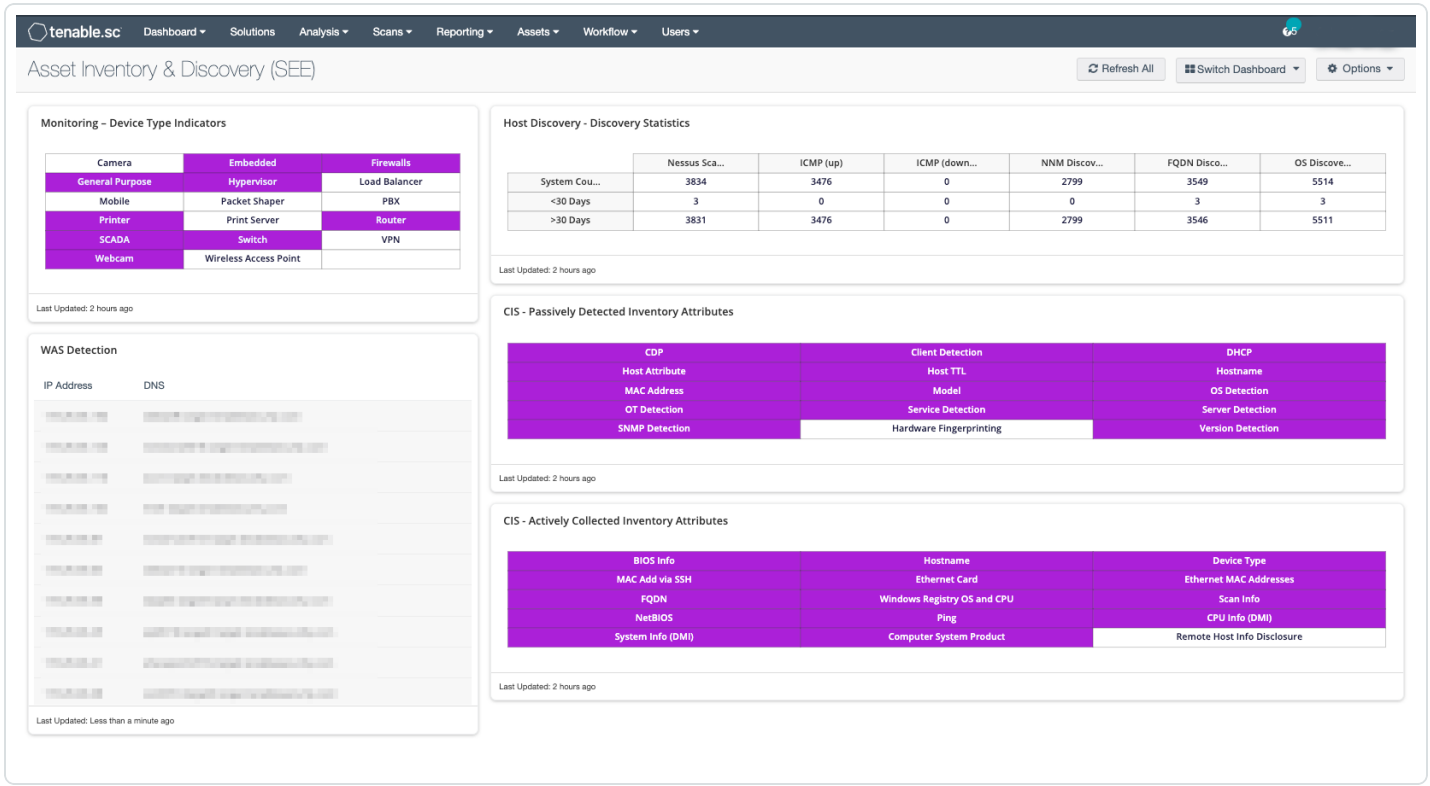
In addition to the Articles previously listed, the following DORA Articles are related to Asset Inventory and Discovery efforts:

- Article 8.2, Financial entities shall, on a continuous basis, identify all sources of ICT risk
- Article 8.3,Financial entities shall identify all information assets and ICT assets, including those on remote sites, network resources and hardware equipment
- Article 16.1 (d), allow sources of ICT risk and anomalies in the network and information systems to be promptly identified and detected

In this section the following Tenable products will be highlighted:

- Tenable Security Center
- Tenable Vulnerability Management
- Tenable OT Security





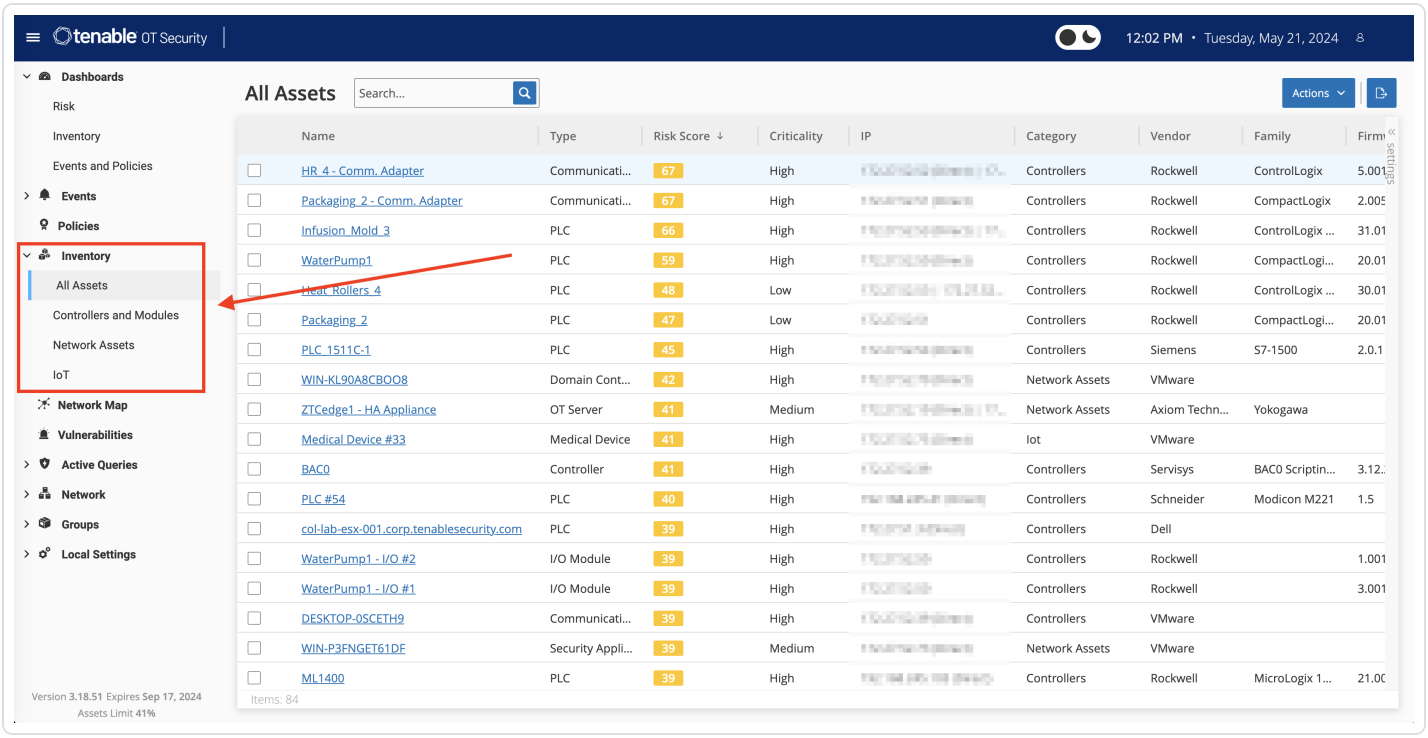
For more information on Asset Discovery and Classification see the [Asset Inventory and Discovery Cyber Exposure Study](#).

Tenable OT

Industrial controls are not the first things that come to mind when working with the financial industry. However, there are many IoT devices that may be present. IoT sensors and smart devices are known to be installed to monitor bank branches, ATMs, POS Terminals,and data centres, such as building automation and building management. IoT devices are being used to deliver real-time data on financial interactions between customers and banks to generate analytics. And with the advancements of artificial intelligence (AI) and machine learning, we can expect to see more of these devices being connected.

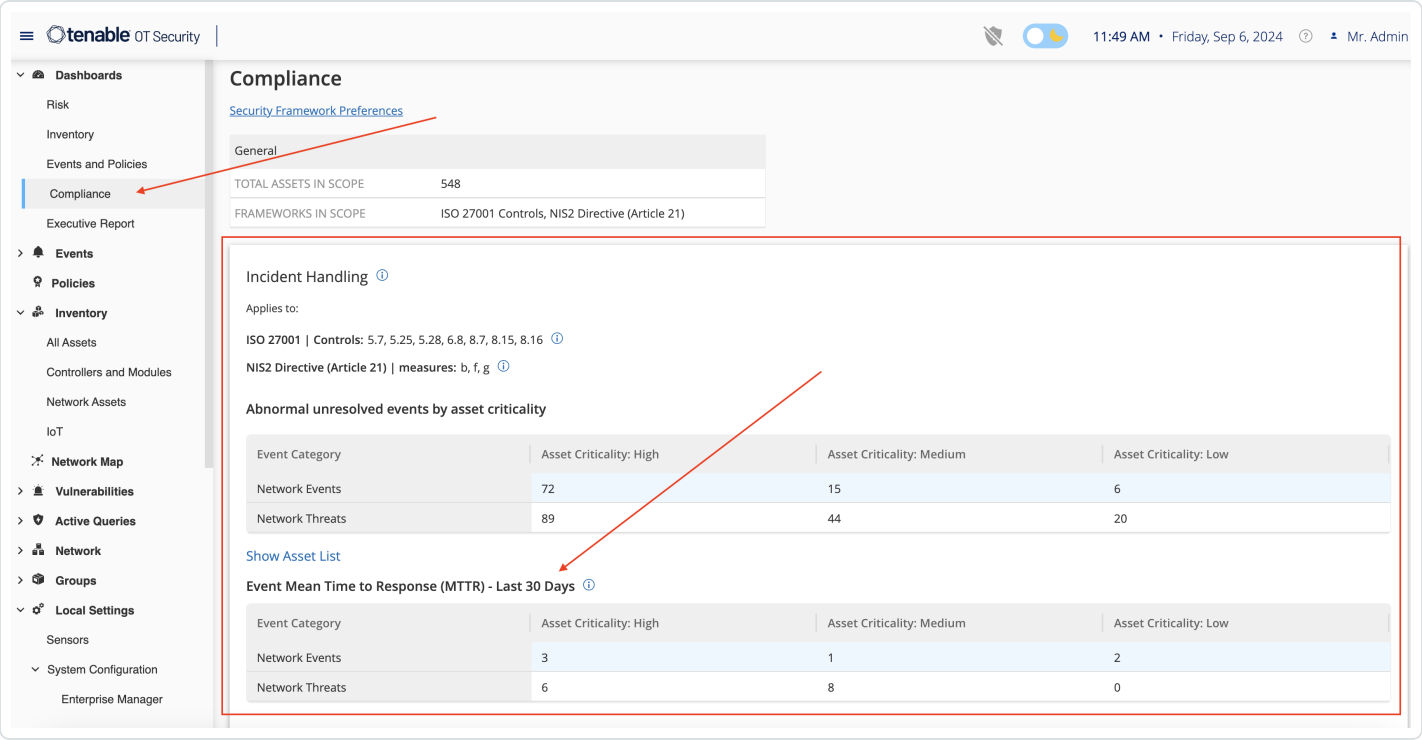
Identification of IoT assets is accomplished with Tenable OT Security. Native communication protocols are used to query both Information Technology (IT) and Operational Technology (OT) devices in your Industrial Control Systems (ICS) environment in order to identify all of the activities and actions 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.



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.

Identity Management 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.

In addition to the Articles previously listed, the following DORA Articles are related to Identity Management and Access Control efforts:

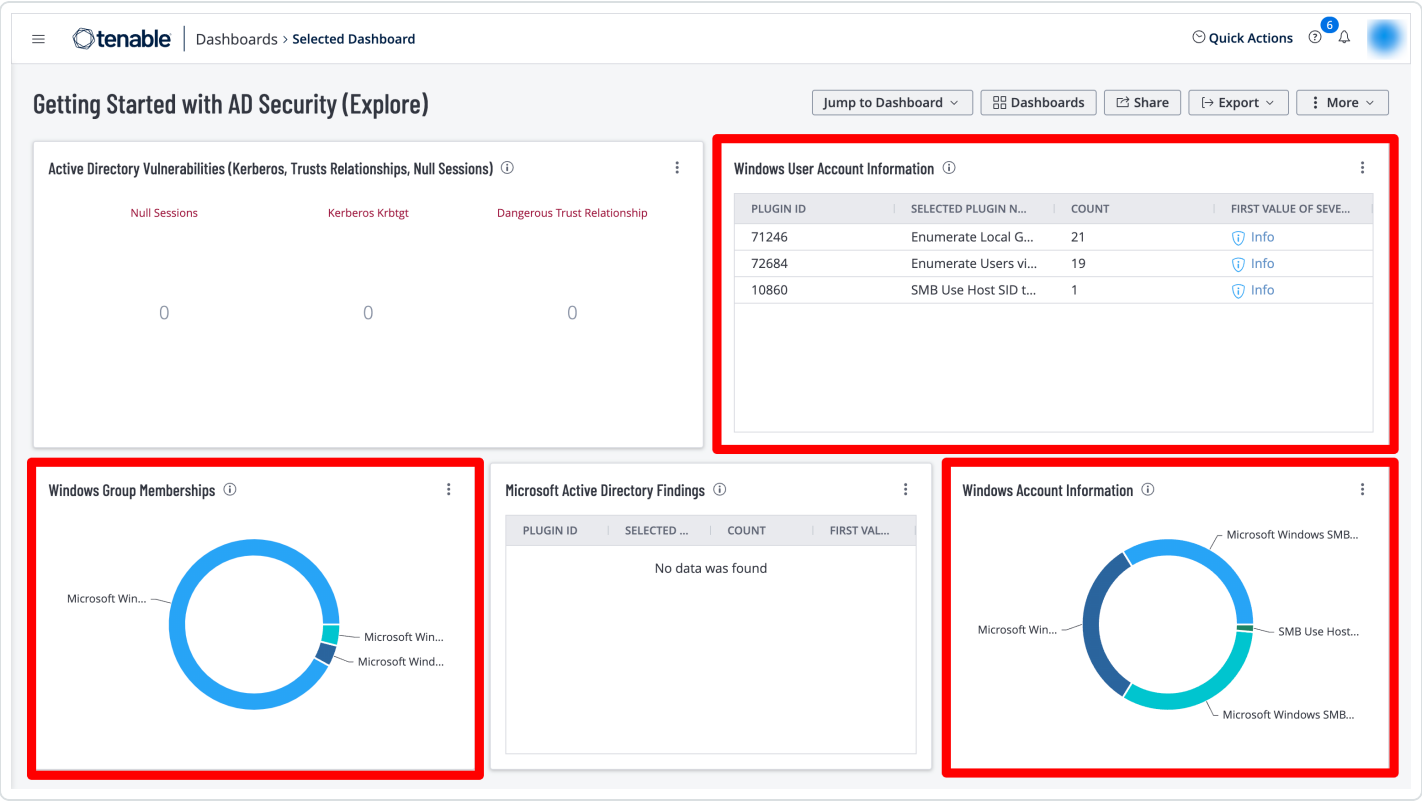
- Article 9.4(c), Establish to that end a set of policies, procedures and controls that address access rights and ensure a sound administration thereof
- Article 9.4(d), Implement policies and protocols for strong authentication mechanisms, based on relevant standards and dedicated control systems, and protection measures of cryptographic keys whereby data is encrypted based on results of approved data classification and ICT risk assessment processes
- Article 10.3, Financial entities shall devote sufficient resources and capabilities to monitor user activity

In this section the following Tenable products will be highlighted:

- Tenable Identity Exposure
- Tenable Security Center
- Tenable Vulnerability Management
- Tenable Cloud Security

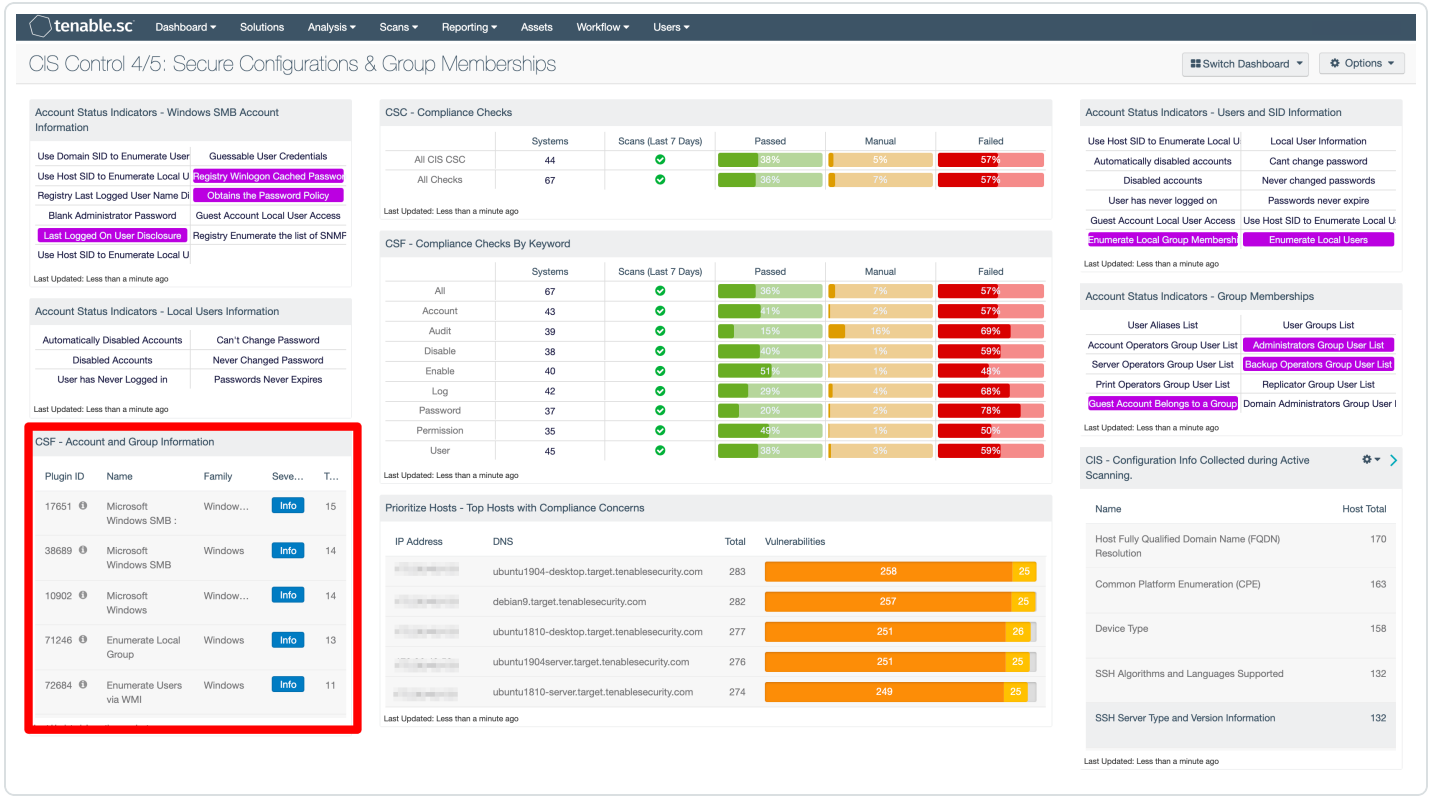
Tenable Identity Exposure provides various methods to access the information collected through the Indicators of Exposure (IoE) and Indicators of Attack (IoA) panes. Tenable Vulnerability Management provides the ability to use the Explore Findings through the use of dashboards and reports.

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.

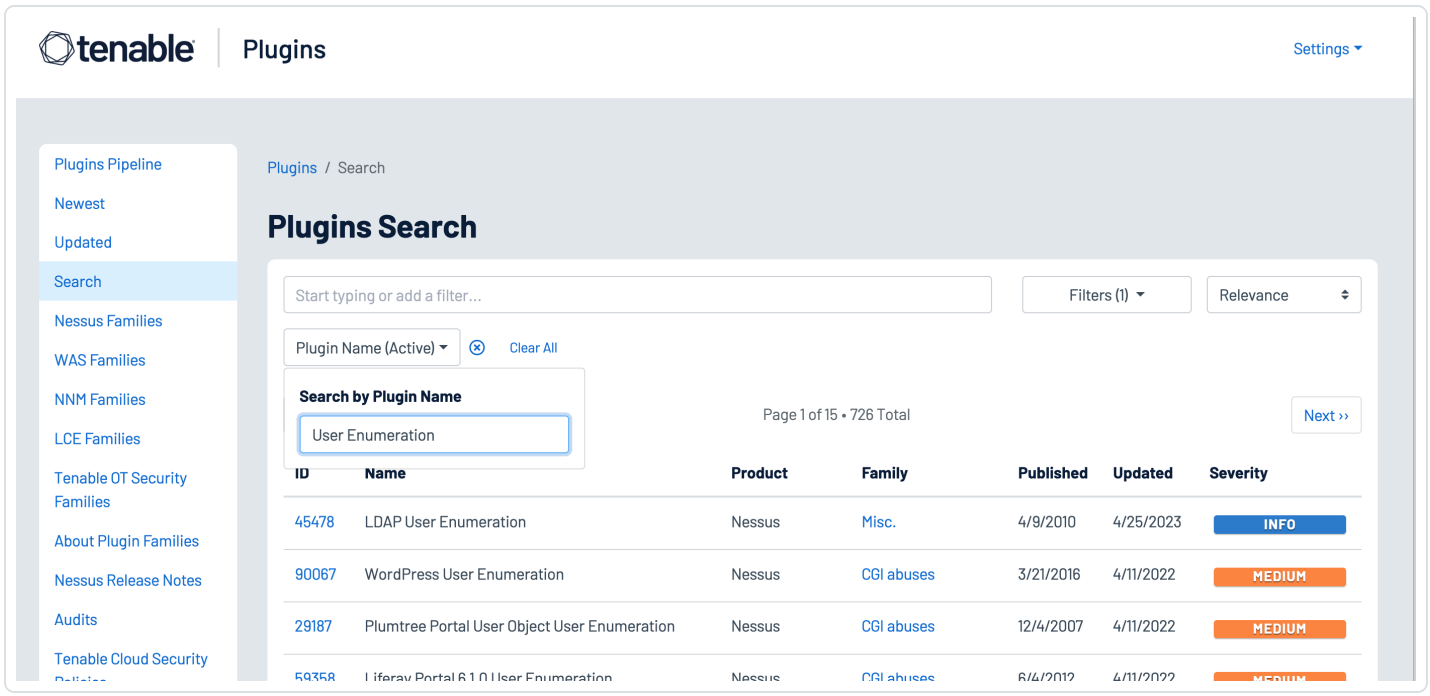
The Cyber Security Framework (CSF), developed by the National Institute of Standards and Technology, and the CIS Critical Security Controls, developed by the Center for Internet Security, are both globally applied standards. Therefore, organisations can also reference widgets such as the **CSF - Account 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.



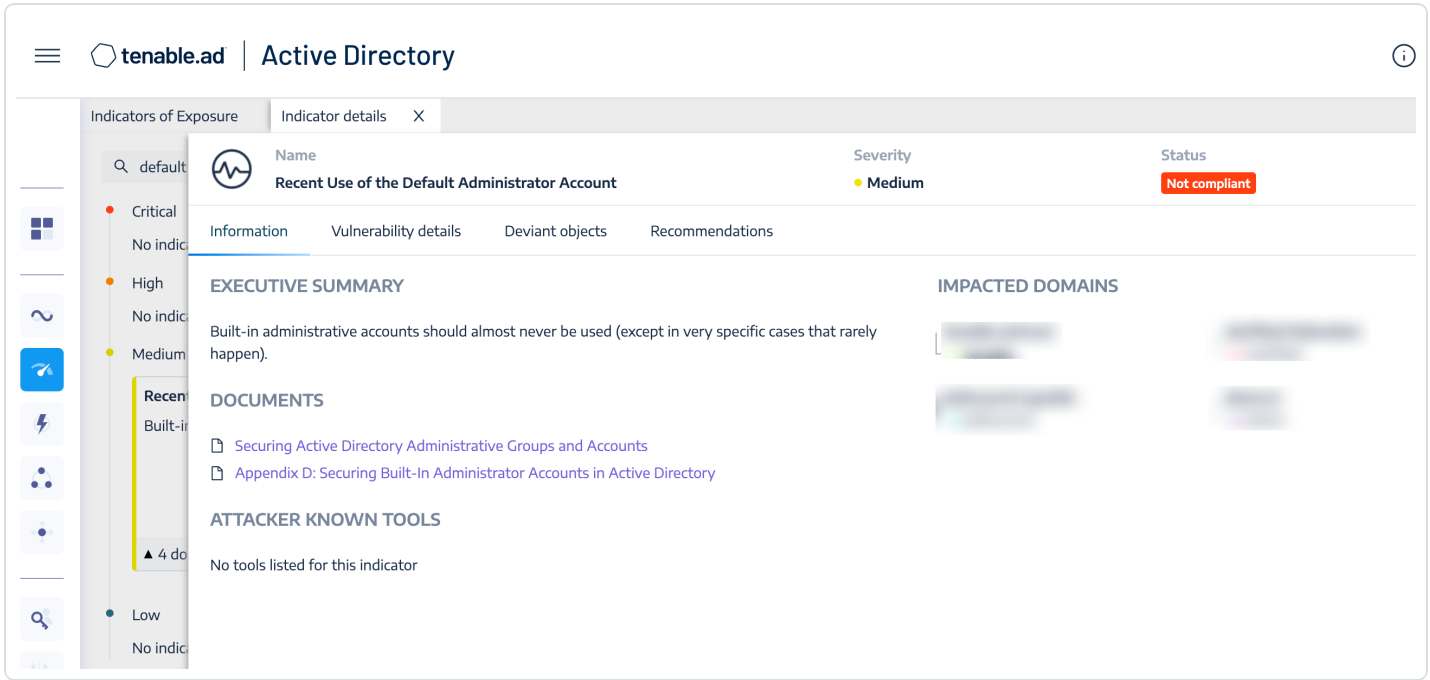
Operating Systems and applications are often distributed with service and default accounts that are either not password-protected or have a default password that is well known. Tenable Nessus and Tenable Identity Exposure help identify these accounts, enabling organisations to review and disable any 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

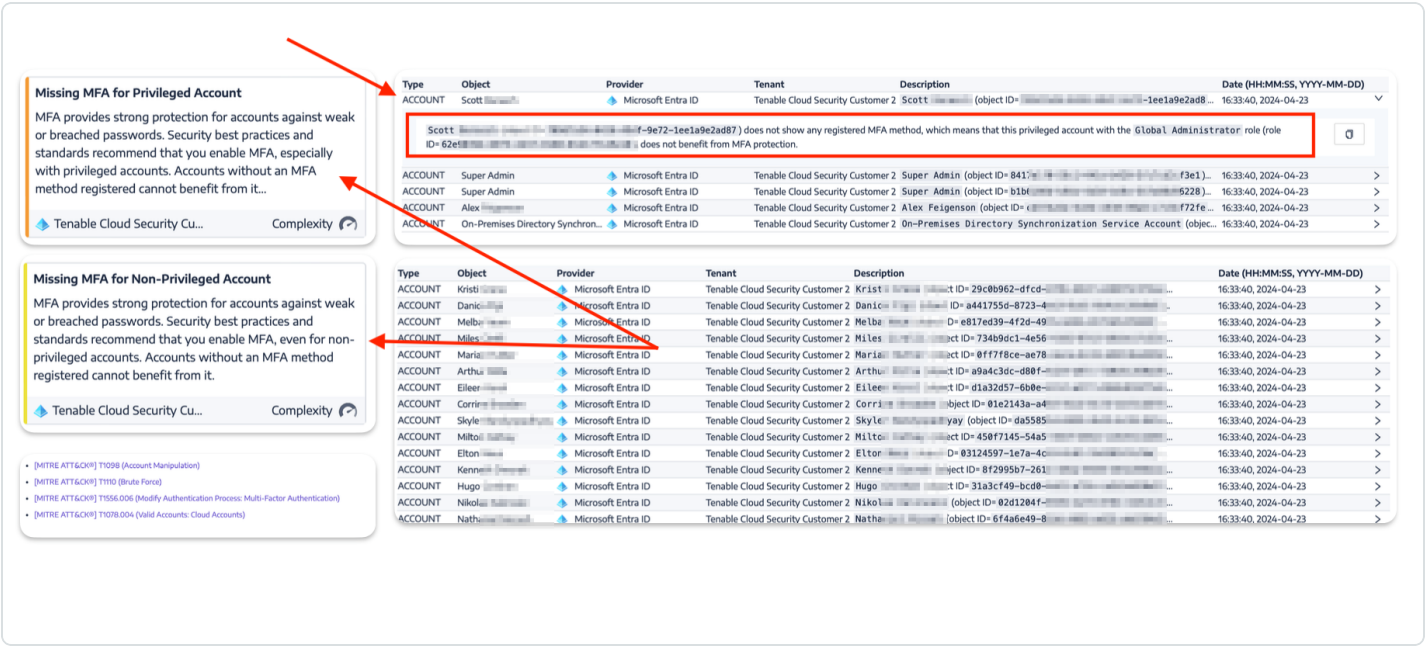
Several hundred plugins can be identified by searching for “Default Account” from the **Nessus Plugins Search** page using the Enable Default Logins filter. Nessus default account plugins are available for Databases, Web Servers, SCADA devices, Unix/Linux devices, Cisco devices and more. Many of the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



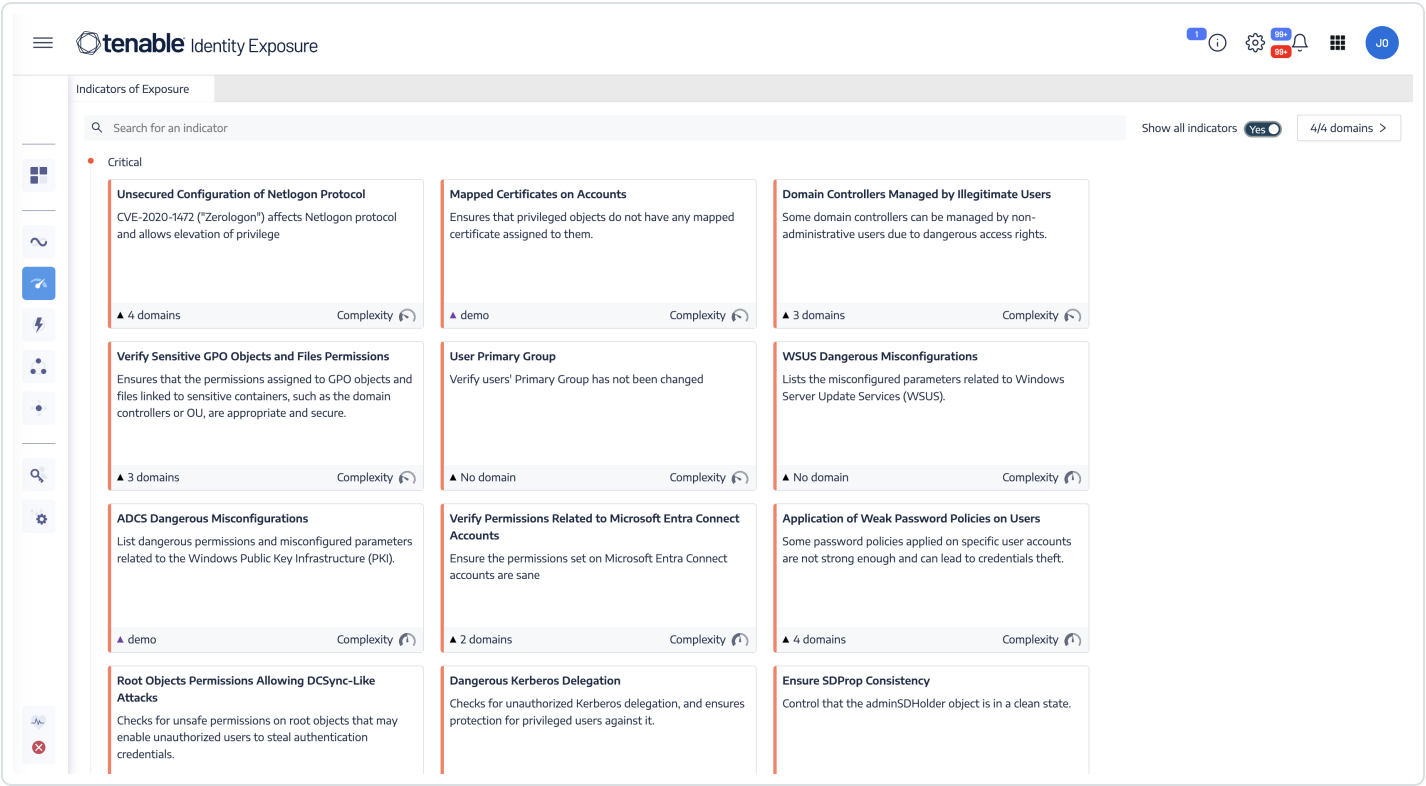
In addition, Tenable Identity Exposure provides the ability to determine if a default administrator account was recently used in the environment, as shown in the image below:



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.



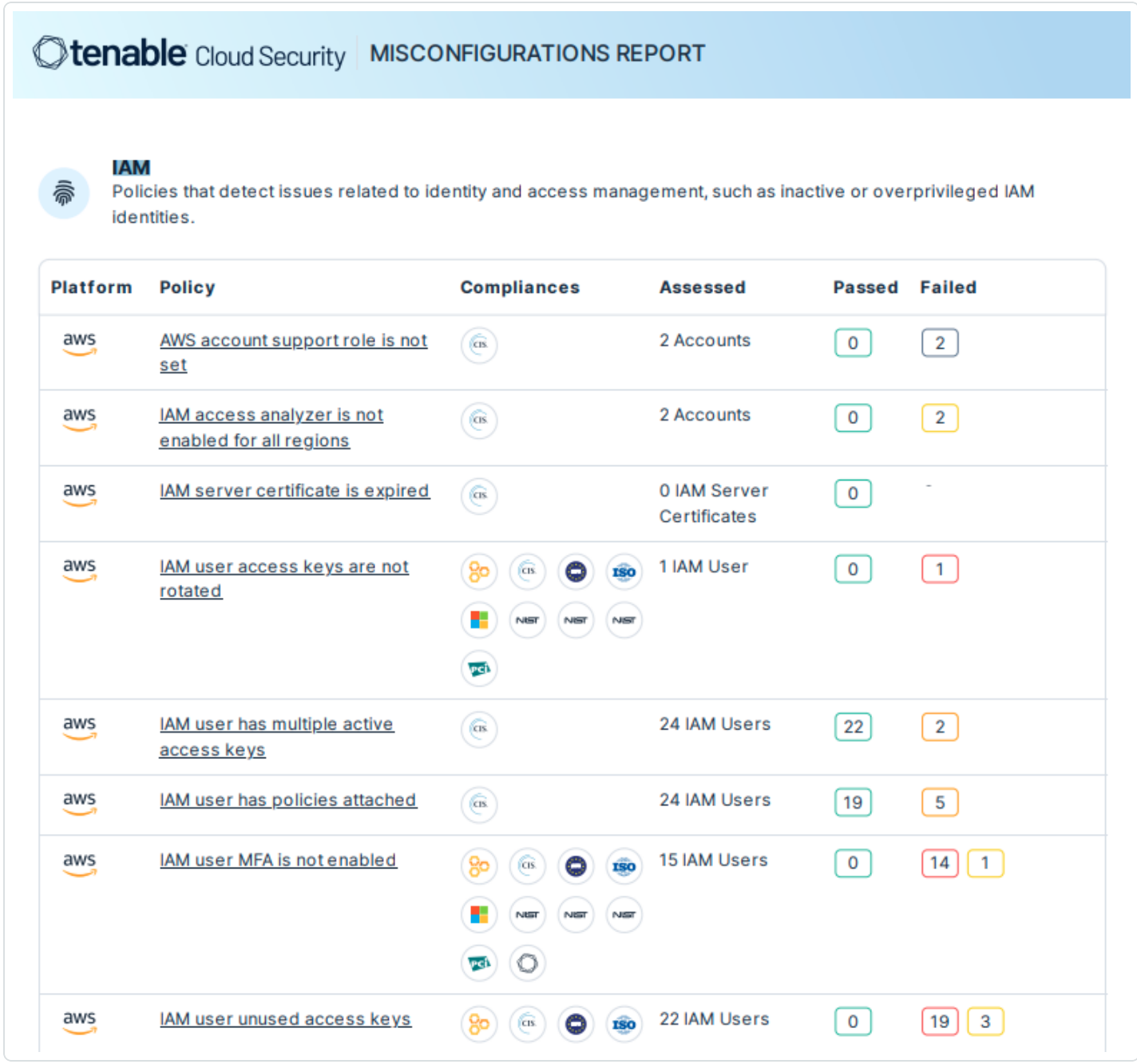
For more information on Tenable Identity Exposure review the documentation located here.

For more detailed information review the Identity and Access Management Cyber Exposure guide.

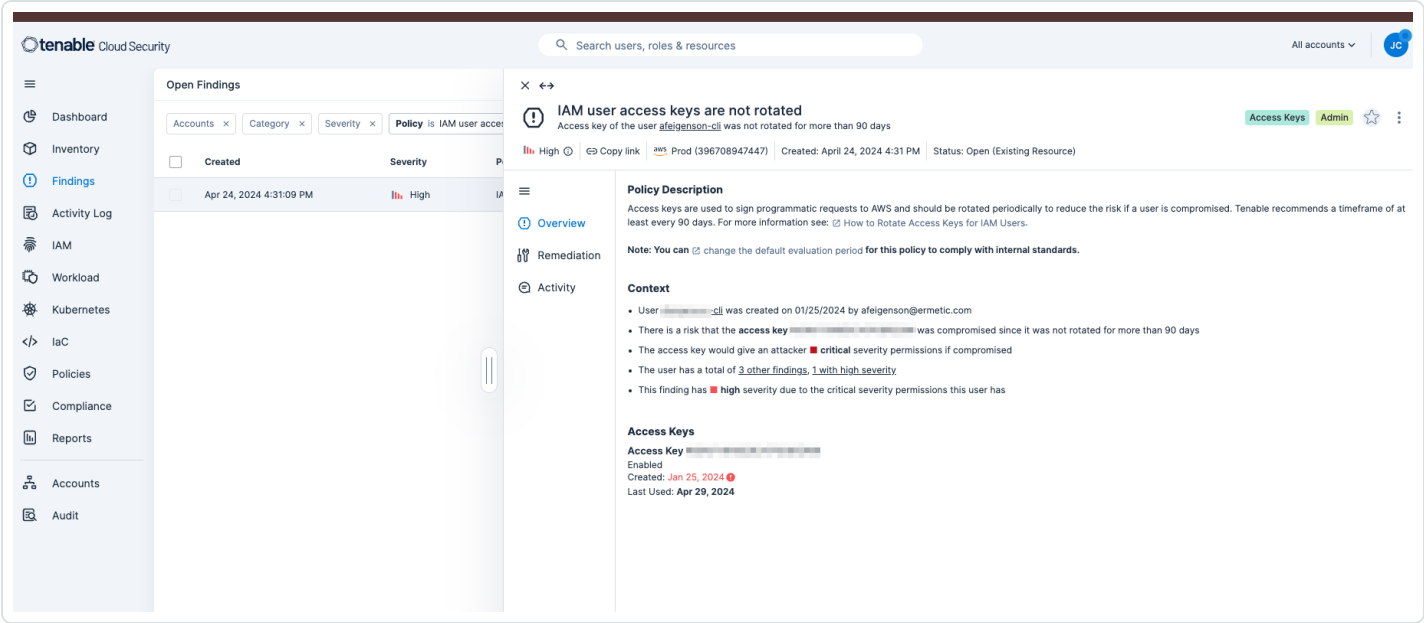
Additionally, the Identity and Access Control section of the NIS 2 Directive Cyber Exposure Study can be referenced.

Cloud Provider Misconfigurations

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.



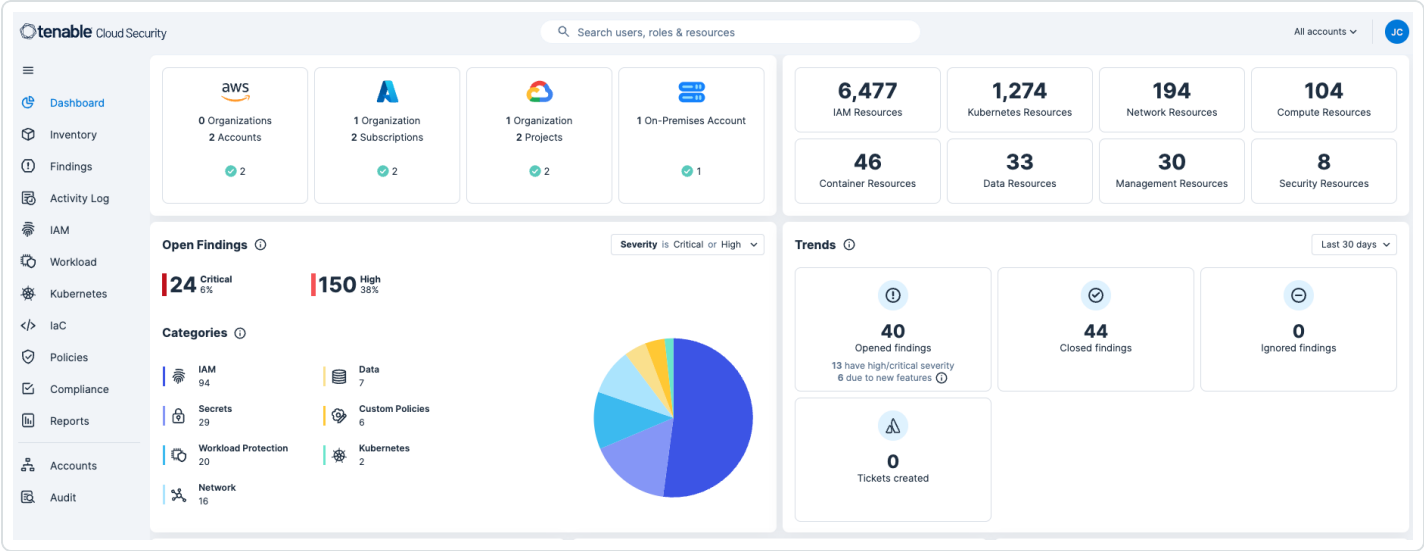
Details within each policy violation contain an overview, policy violation details, and policy remediation strategies, as well as defining any impacted resources. Policies are used to identify misconfigurations and vulnerabilities present on cloud resources. Tenable Cloud Security has built-in policies 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 here.

Additionally, 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.



More information on getting started with Tenable Cloud Security is available here.

Additional Resources: Exposure Management

Exposure Management is the process of identifying, assessing, and mitigating risks and vulnerabilities within an organisation's environment to protect against threats. By adopting exposure management, organisations stay ahead of evolving threats and maintain operational resilience. This is critical in environments where there is a mix of on-premises, cloud, and IoT systems.

In this section the following Tenable products will be highlighted:

- Tenable One
- IoT and Tenable One
- Tenable Vulnerability Management
- Tenable Security Center

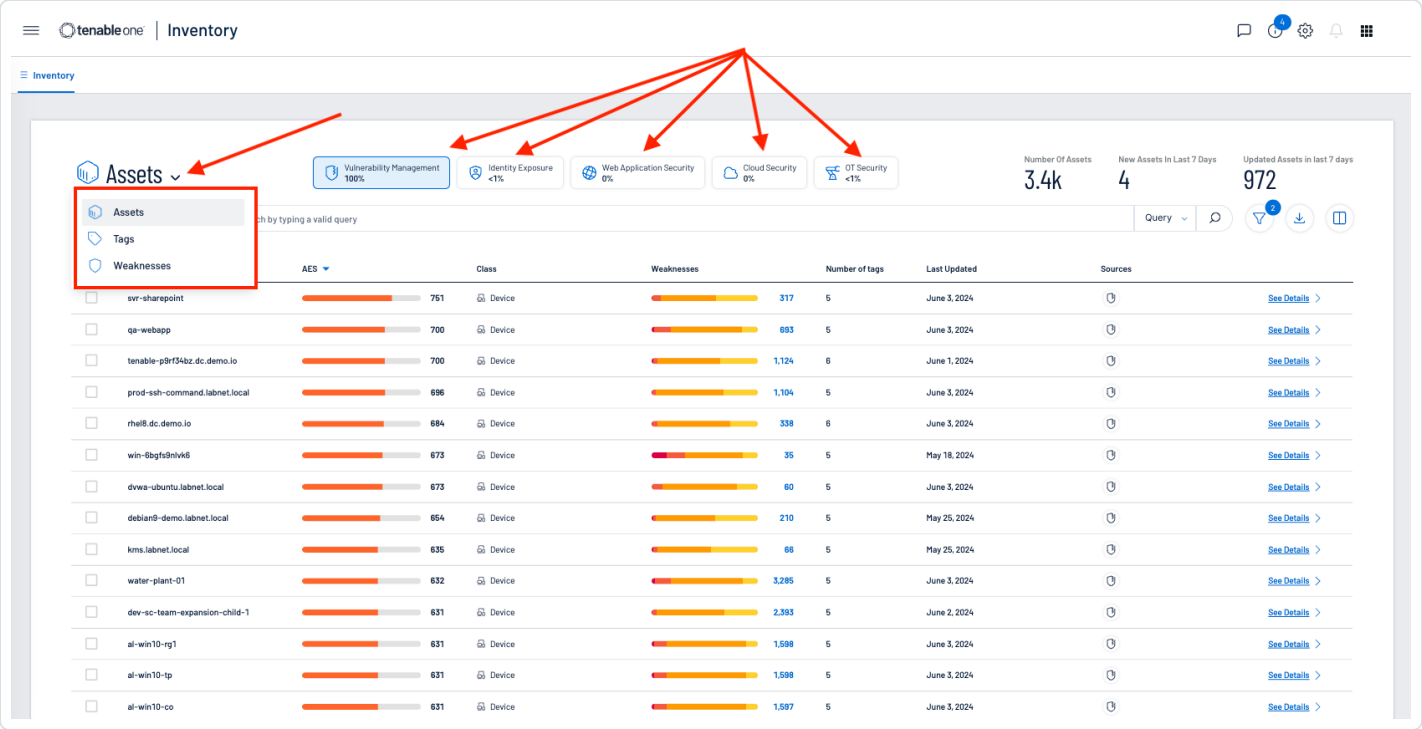
Tenable One

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.

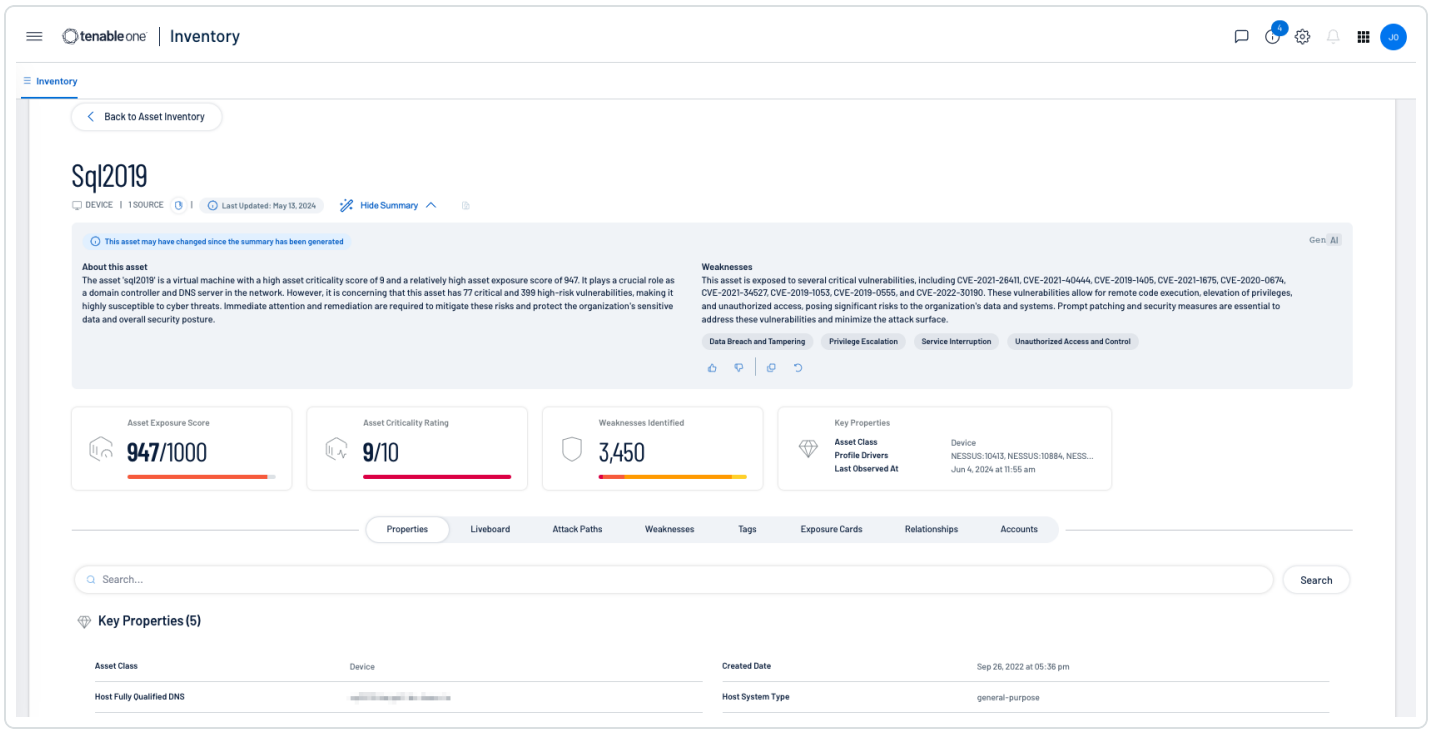
Tenable One Asset Inventory provides a comprehensive view of all assets across the entire attach surface. Sensors pull data from multiple applications across the platform, providing details on all known systems. At the highest level on the Asset Inventory page is shown the Number of Assets

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.



For more information on Tenable One, click here.

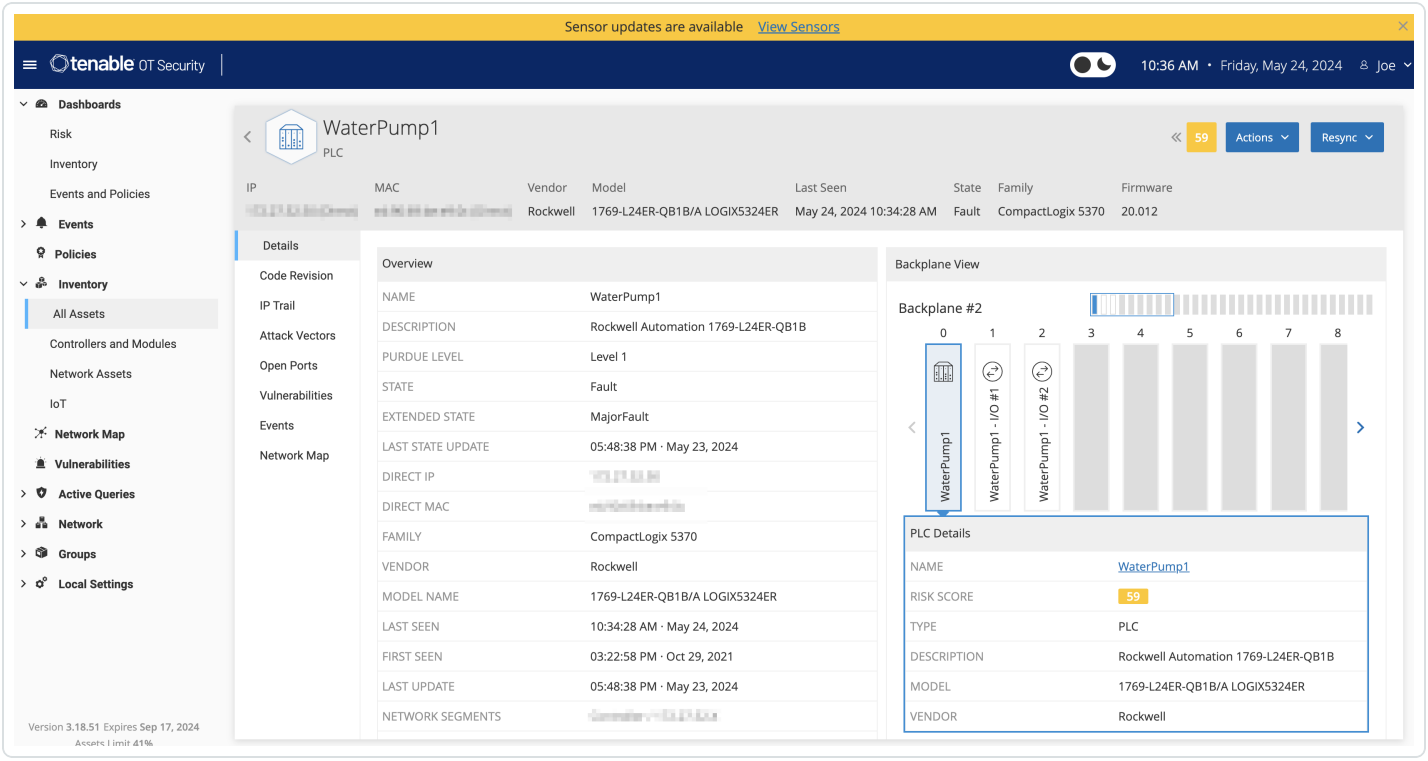
IoT and Tenable One

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.

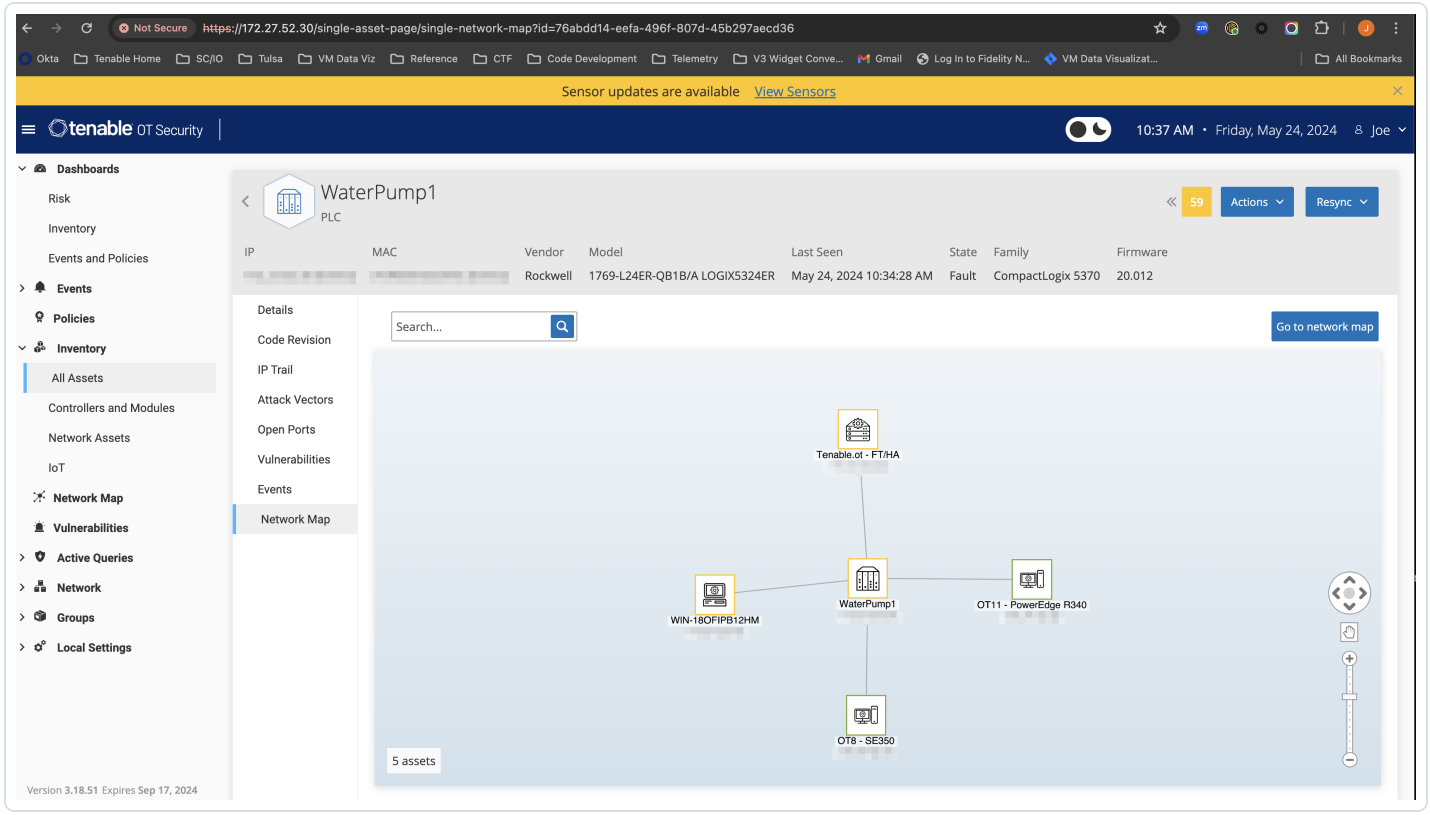
Information Technology (IT) primarily deals with data processing and communications. Operational Technology (OT) generally refers to the hardware and software that is used to monitor and control devices and processes within industry, manufacturing, energy, transportation, and utility environments. OT 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

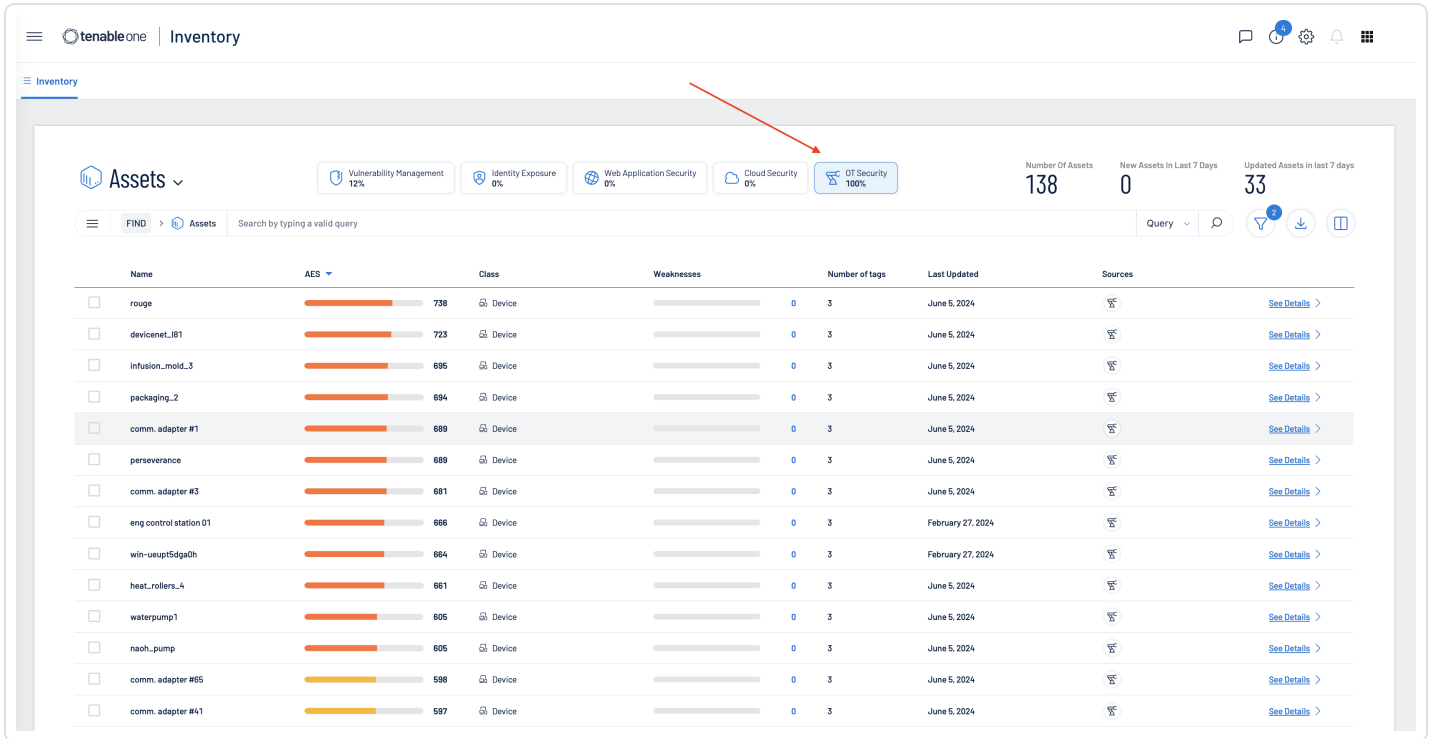
important. Security teams can now get visibility into device make and model, as well as firmware version and status.



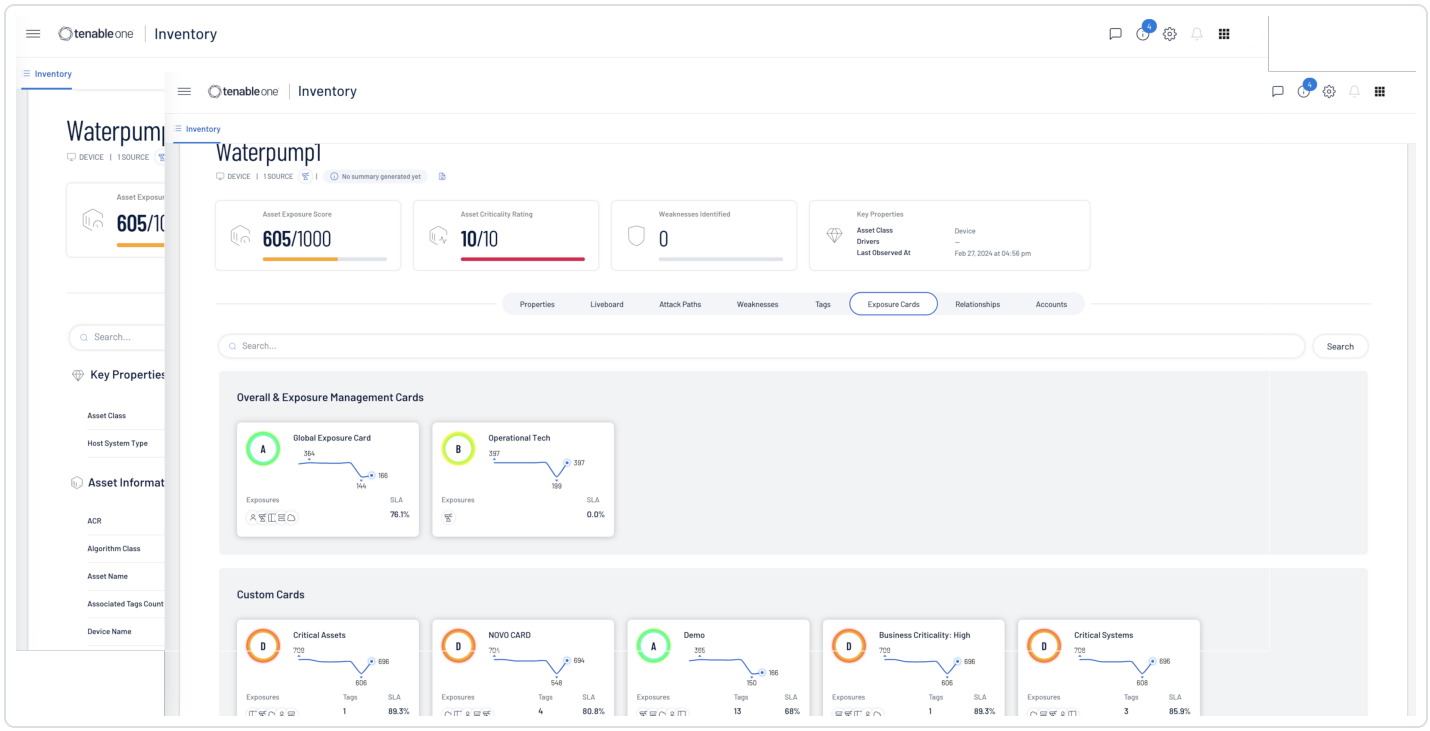
Connections can also be mapped to other devices on the network.



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.



Digital Operational Resilience Testing

Digital Operational Resilience Testing refers to the practices and procedures implemented to ensure that systems and infrastructure can withstand, recover, and adapt to disruptions, cyber attacks, and other challenges. In addition to the Articles previously listed, the following DORA Articles are related to Digital Operational Resilience Testing efforts:

CHAPTER IV, Digital operational resilience testing

- The digital operational resilience testing programme shall include a range of assessments, tests, methodologies, practices and tools to be applied in accordance with Articles 25 and 26:
    - Article 24.3, Financial entities, other than microenterprises, shall follow a risk-based approach.
    - Article 25.1, the execution of appropriate tests, such as vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews

where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing and penetration testing.

- Article 26.2, Financial entities shall identify all relevant underlying ICT systems, processes and technologies supporting critical or important functions and ICT services.

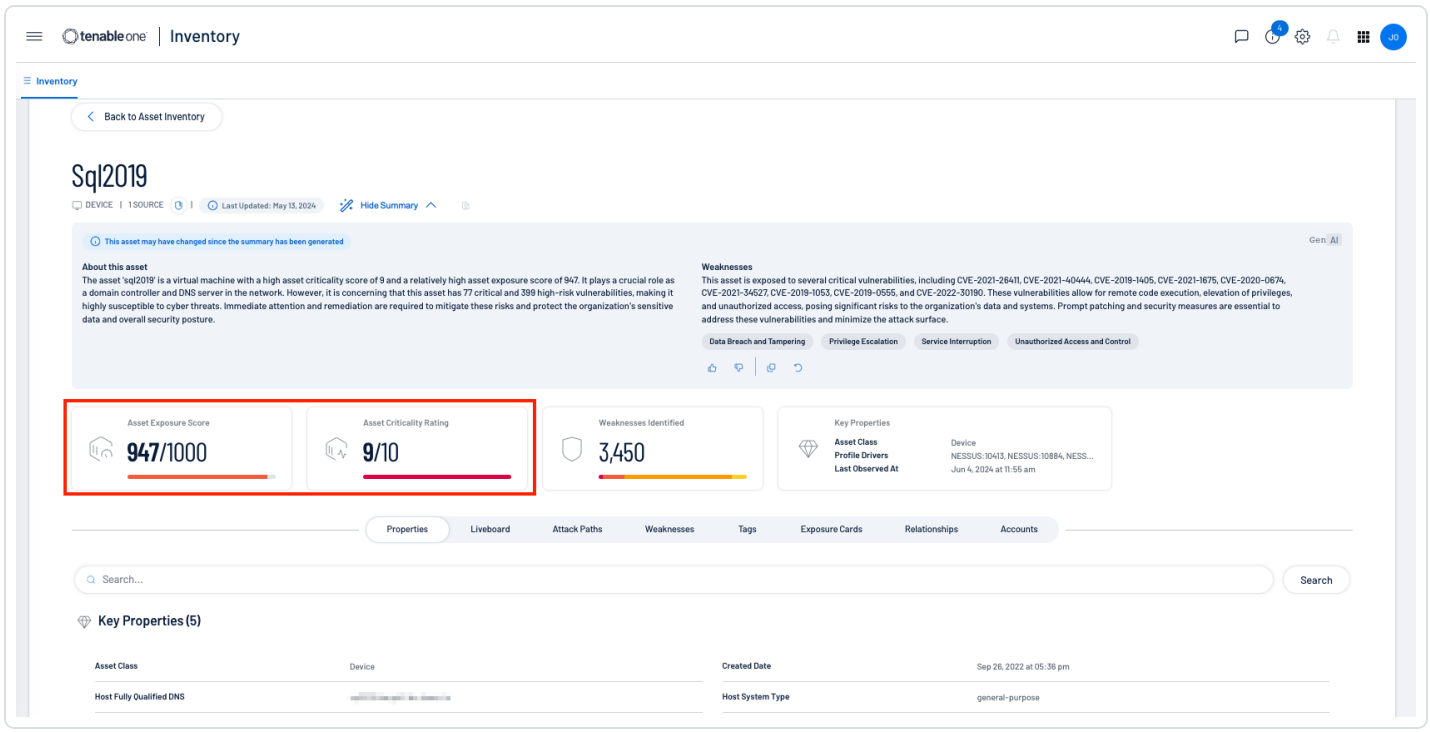
Periodic risk assessment is the primary tool for engineers and security analysts to manage risks by maintaining good cyber hygiene, reducing operational downtime and mitigating the potential impact of threats.

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.

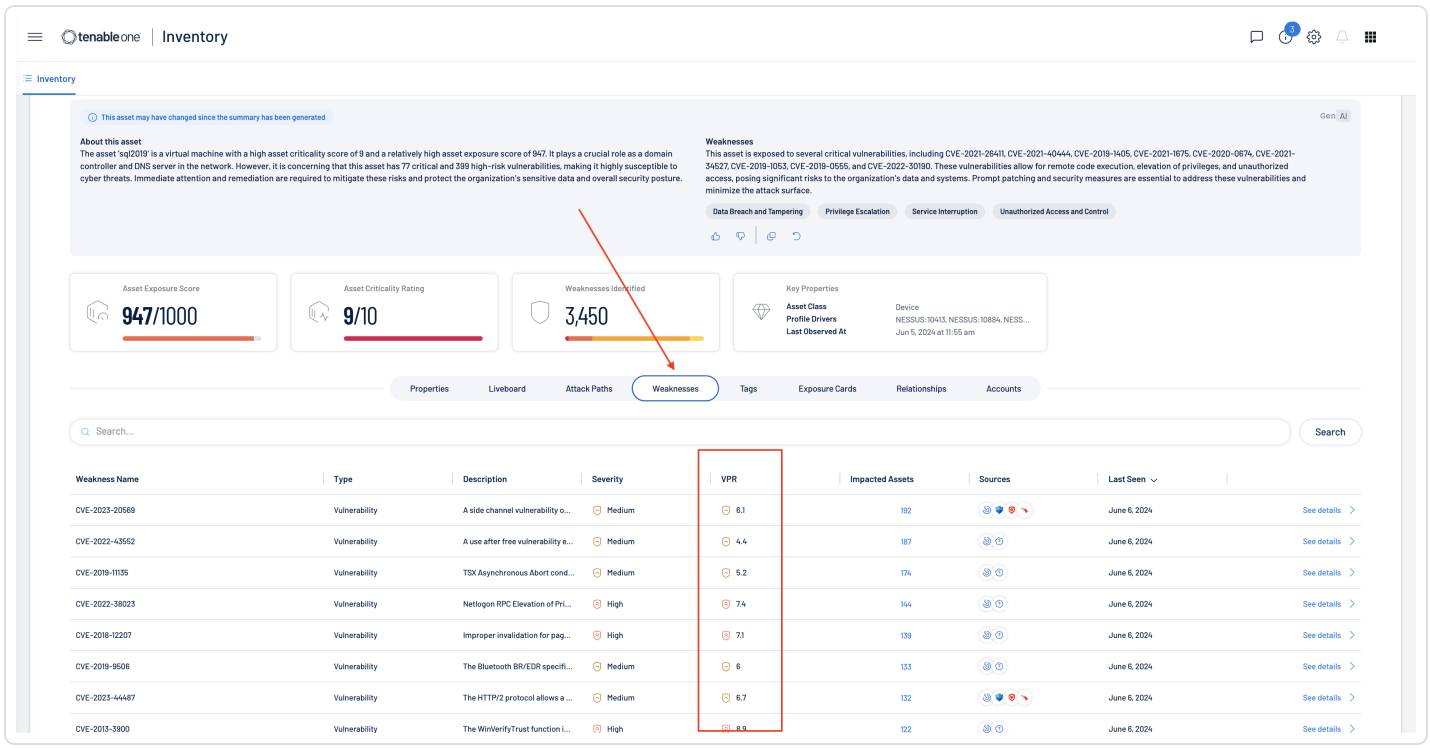
Risk assessments are critical for helping organisations make informed decisions, prioritising resources, and proactively managing risks, while minimising potential negative impacts. While the vulnerability management section deals specifically with identification aspects, this section provides guidance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

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.

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



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



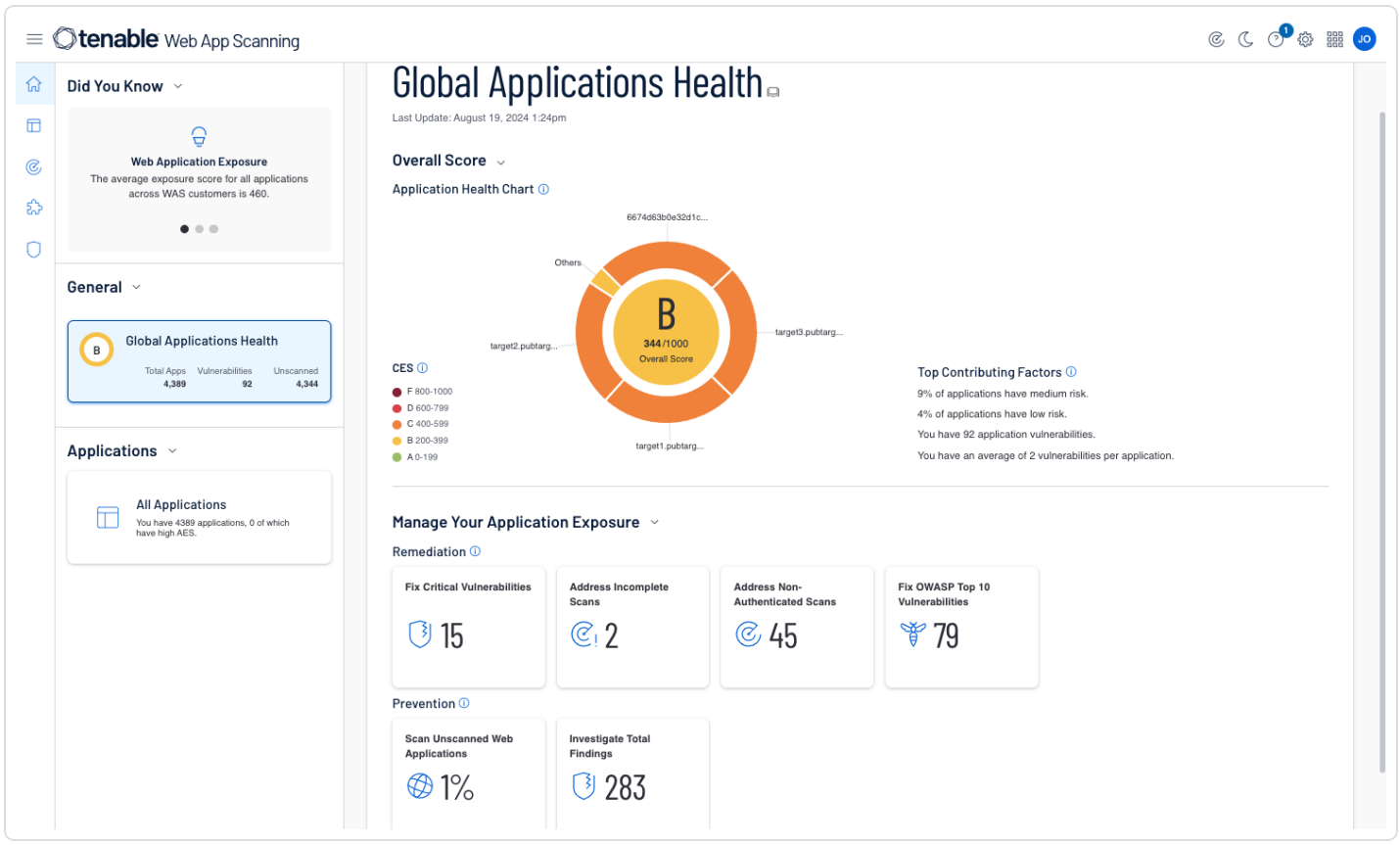
For more details on AES, ACR, and VPR, please see the [Risk Assessment section of the NIS 2 Cyber Exposure study].

Scan Health

For more details on AES, ACR, and VPR, please see the Risk Assessment section of the NIS 2 Cyber Exposure study.

- Article 9.1, Financial entities shall continuously monitor and control the security and functioning of ICT systems and tools

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.

Third-Party Risk Management

One key area that DORA regulates is Third-Party Risk Management. Third-party risk is significant, often because third parties have access to privileged information, such as customer data, and internal systems. Organisations can be negatively impacted in the form of data breaches, operational disruptions, and reputational damage. DORA requires that financial institutions identify their third party service providers. Tenable can assist organisations identify third-party vendors by identifying software, hardware, and cloud services that have been identified within the organisation. In addition to the Articles previously listed, the following DORA Articles are related to Third-Party Risk Management efforts:

- Article 8.2, Financial entities shall, on a continuous basis, identify all sources of ICT risk.
- Article 8.3, Financial entities shall identify all information assets and ICT assets, including those on remote sites, network resources and hardware equipment.
- Article 9.4(e), Controls for ICT change management, including changes to software, hardware, firmware components, systems or security parameters are documented.

In this section the following Tenable products will be highlighted:

- Tenable Vulnerability Management
- Tenable Security Center
- Tenable Cloud Security

Tenable has previously published a Cyber Exposure Study for the Network and Information Security 2 (NIS 2) Directive. While DORA and NIS 2 have a different focus, the two are related and work together to enhance cybersecurity and operational resilience in the EU. DORA builds on the standards set by the NIS 2 for ICT and resilience. The NIS 2 provides general guidelines and DORA tailors those specifically to the financial sector. The incident reporting requirements are aligned with NIS 2, and both DORA and the NIS 2 place a strong emphasis on third-party risk management.

Identifying installed applications is a key factor in the identification of third-party vendors, reducing risk, and securing the organisation from unwanted attacks. A software inventory helps demonstrate compliance with regulatory controls and Service Level Agreements (SLA) for software used in the environment. From the perspective of “less is more,” a software inventory also identifies unnecessary software running in the environment, which increases the attack surface without

providing a business advantage. Tenable Vulnerability Management and Tenable Security Center help organisations identify software vendors and build a software inventory.

There are several software discovery plugins that run by default in the following scan templates:

- Basic and Advanced Agent Scans
- Basic and Advanced [Network] Scans
- Credentialed Patch Audit
- Internal PCI Network Scan
- Collect Inventory Agent Scan (see below)

Inventory Agent Scanning in Tenable Vulnerability Management contains a Collect Inventory template which provides faster scan results and minimises the Nessus Agent load and installed footprint on the endpoint. Leveraging this new scan policy ensures the agent only runs an inventory collection plugin locally and sends results to Tenable Vulnerability Management for processing. Scan results are presented in the same format as traditional scans. While there is a coverage differential compared to using a traditional agent, the Inventory Agent provides a great option for host-based scanning on hosts with limited resources.

> **Note:** Inventory Agent Scanning is supported on the following platforms:
>
> - Tenable Vulnerability Management Agent scans
> - Tenable Security Center imports of Tenable Vulnerability Management cloud agent scans

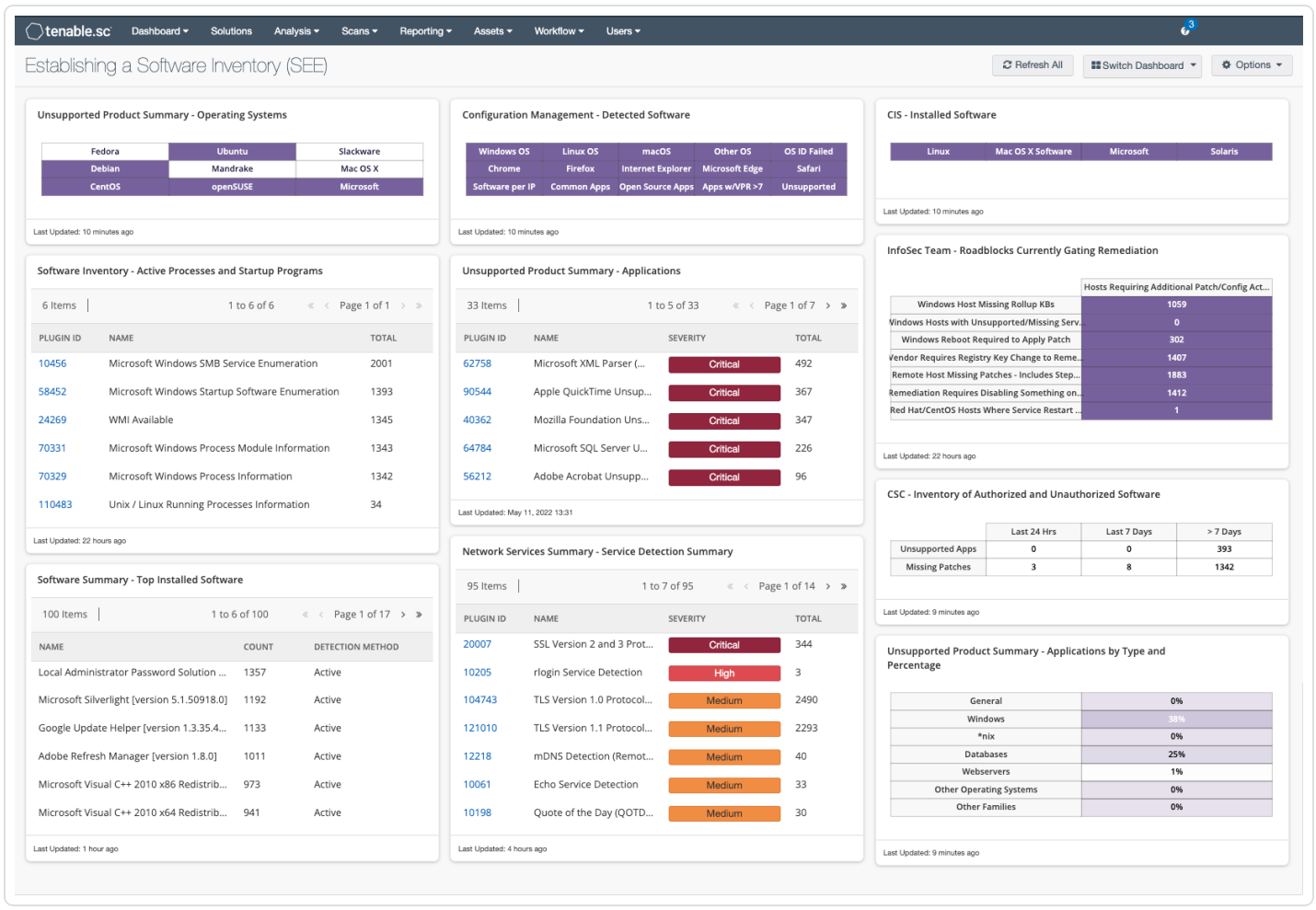
Other methods of application identification to utilise software enumeration plugins. The most common software enumeration plugins are OS Identification (11936), Microsoft Windows Installed Software Enumeration (credentialed check) (20811), Software Enumeration (SSH) (22869), and List Installed Mac OS X Software (83991). There are several other software enumeration plugins that provide information that can help build a software inventory:

- OS Fingerprinting via DHCP (7120)
- Oracle Installed Software Enumeration (Linux / Unix) (71642)
- Oracle Installed Software Enumeration (Windows) (71643)

- OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library) (97993)
- Unix Software Discovery Command Checks (152741)
- Unix Software Discovery Commands Available (152742)
- Unix Software Discovery Commands Not Available (152743)

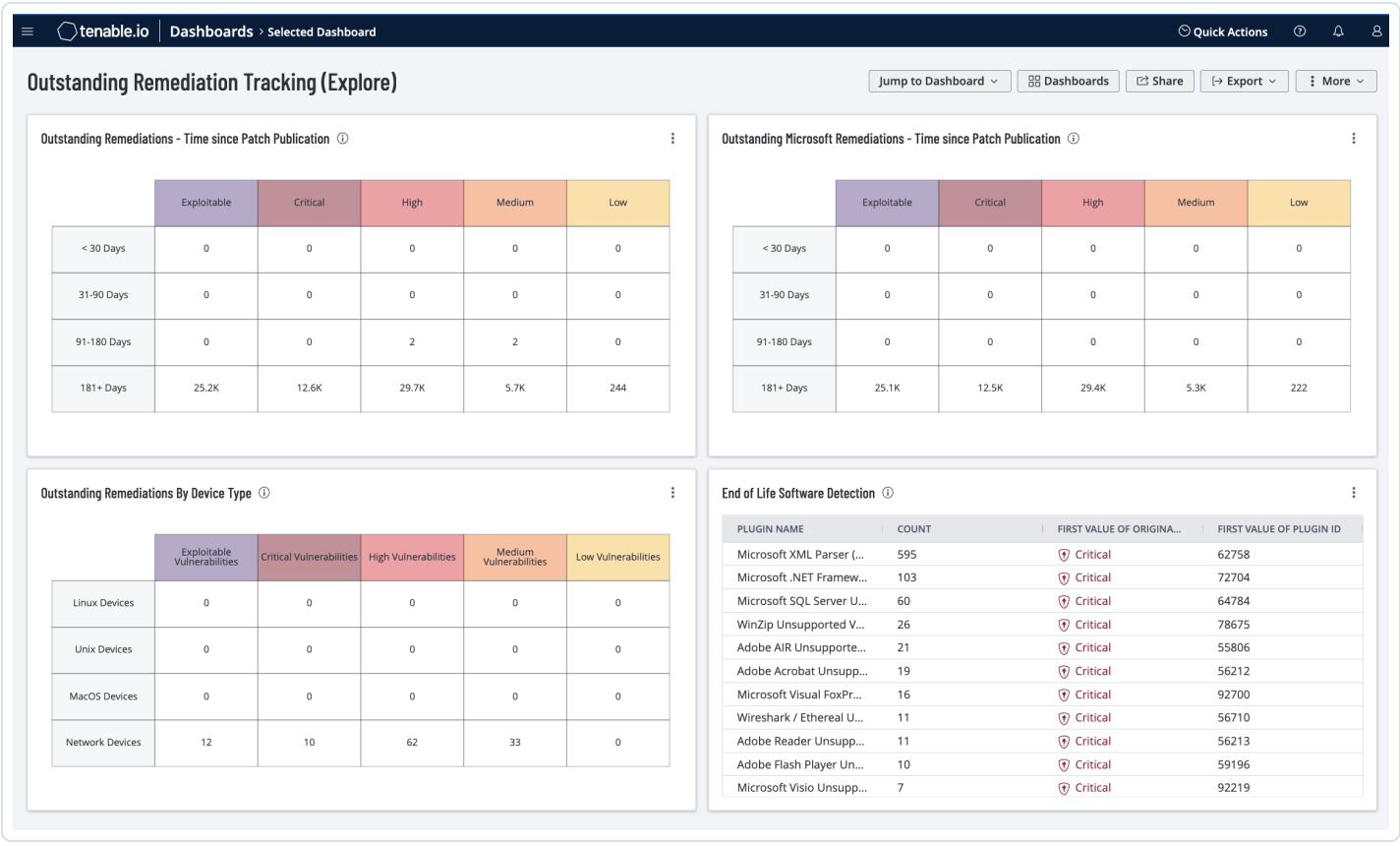
> **Note:** Plugin Spotlight: Plugin ID 22869, Software Enumeration (SSH), identifies the package list on Linux systems, which includes package name, version, epoch information for each package installed on the system, and (on RPM-based systems) the date the operating system reports that a package was installed. This information is included in the plugin output (also referred to as “vulnerability text") in the scan results.

Dashboards and Reports, such as Establishing a Software Inventory (SEE), for Tenable Security Center, helps demonstrate compliance with regulatory controls and Service Level Agreements (SLAs) for software used in the environment. From the perspective of “less is more,” a software inventory also identifies unnecessary software running in the environment, which increases the attack surface without providing a business advantage.



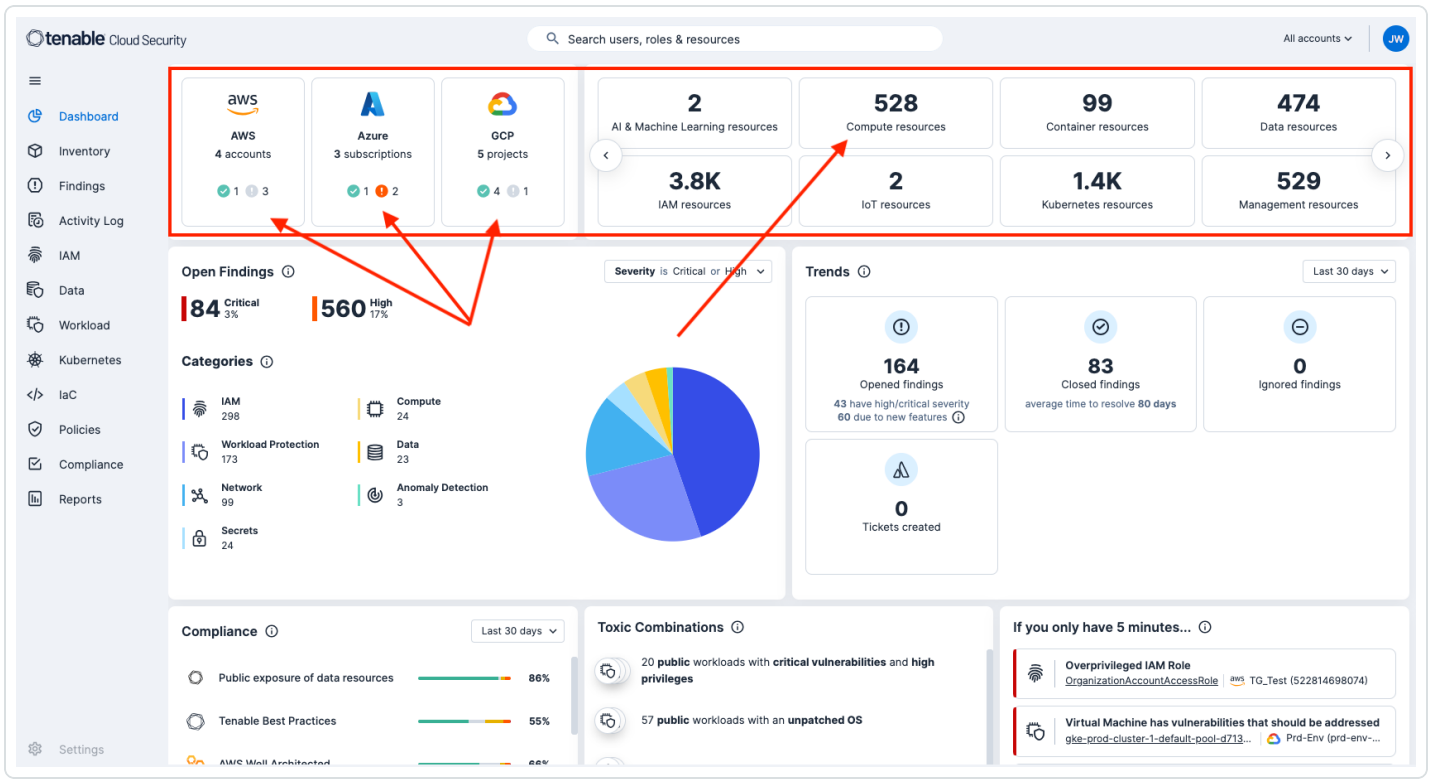
For more information on Software Inventory see the Establishing a Software Inventory Cyber Exposure Study here.

The Outstanding Remediations Tracking dashboards for Tenable Security Center and Tenable Vulnerability Management address third-party risk associated with unsupported, out-dated, and end-of-life software. These dashboards also address risk associated with third-party products by identifying software/applications that are out of compliance or present risk to the organisation.

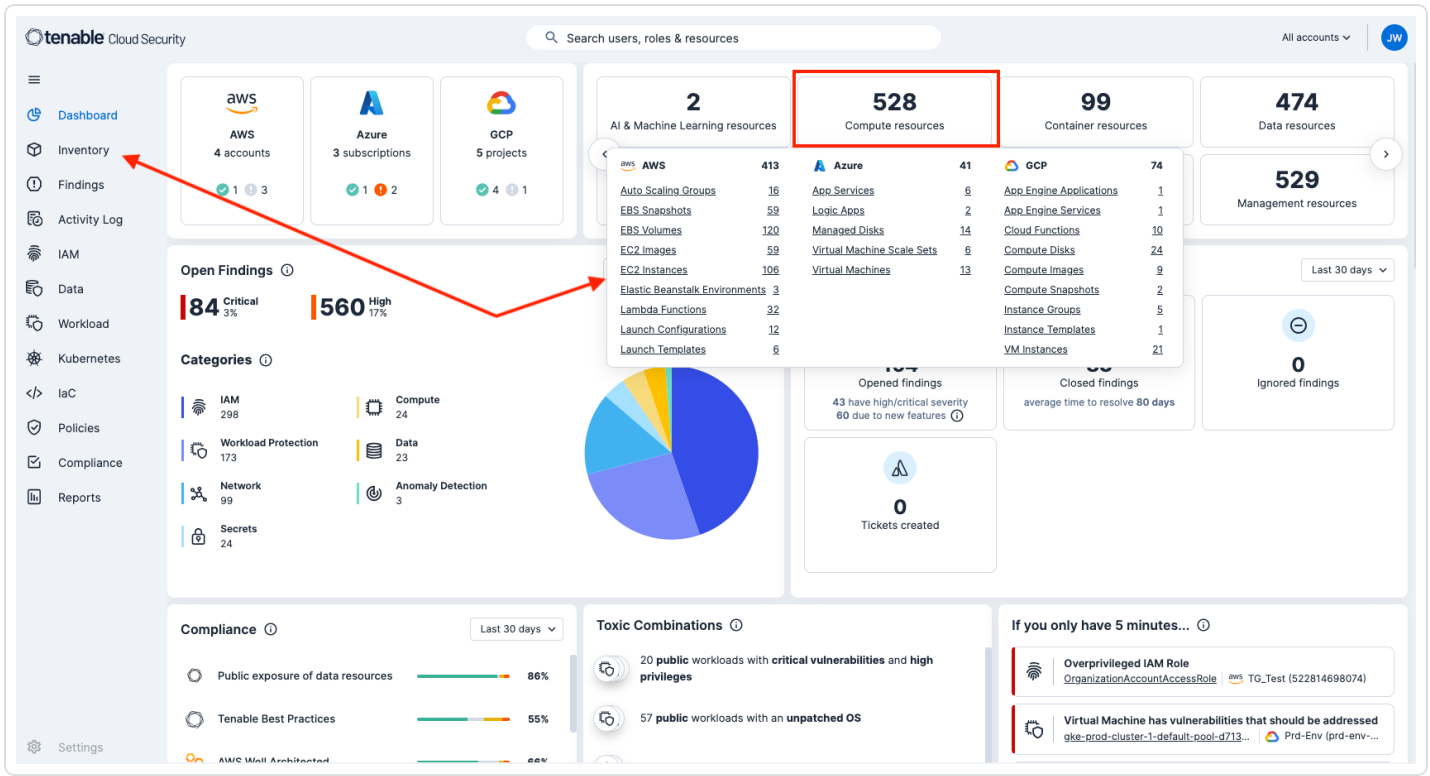


Tenable Cloud Security not only automates threat detection and remediation to eliminate noise, but also identifies cloud services and prioritises risk by continuously monitoring the cloud environment. Tenable analyses cloud provider logs to reveal the identity behind each activity and affected accounts, resources, and services.

From the Tenable Cloud Security dashboard, organisations can immediately begin to identify resources that have been identified such as Compute, Container, and more. Organisations can identify vendors such as AWS, Azure, and GCP.



Clicking on Compute resources provides a shortcut to the Inventory tab, displaying important inventory items such as Volumes, Images, Instances, Virtual Machines, and more allowing fast and easy third-party vendor and application identification.



For more information on Tenable Cloud Security, reference the following documentation.

Learn More

REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011

Implementing act:

- Implementing and delegated acts - DORA
- Commission's adopted implementing and delegated acts

Implementing and delegated acts in the official journal:

- RTS on ICT risk management framework
- RTS on ICT incidents classification
- RTS on ICT third-party policy
- DR on CTPPs designation criteria
- DR on DORA oversight fees