



Tenable Cyber Exposure Study - DORA

Last Revised: July 17, 2025

Table of Contents

| | |
|---|-----------|
| DORA Regulation | 4 |
| Summary | 4 |
| Scope | 4 |
| Getting Started | 7 |
| Key Pillars | 7 |
| Comparisons Between DORA and NIS2 | 9 |
| Scope | 9 |
| Focus and Purpose | 9 |
| Third-Party Risk Management | 10 |
| Supervision and Enforcement | 10 |
| Summary of Key Differences | 10 |
| How Tenable Helps | 11 |
| ICT Risk Management | 12 |
| Prioritising Risk | 14 |
| Lumin Exposure View | 14 |
| Risk Based Vulnerability Management | 15 |
| Remediation Tracking | 18 |
| Asset Inventory and Discovery | 22 |
| Identity Management and Access Control | 25 |
| Additional Resources: Exposure Management | 34 |
| Tenable One | 34 |
| IoT and Tenable One | 36 |
| Digital Operational Resilience Testing | 39 |

Scan Health 42

Third-Party Risk Management 45

Learn More 52



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 the 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

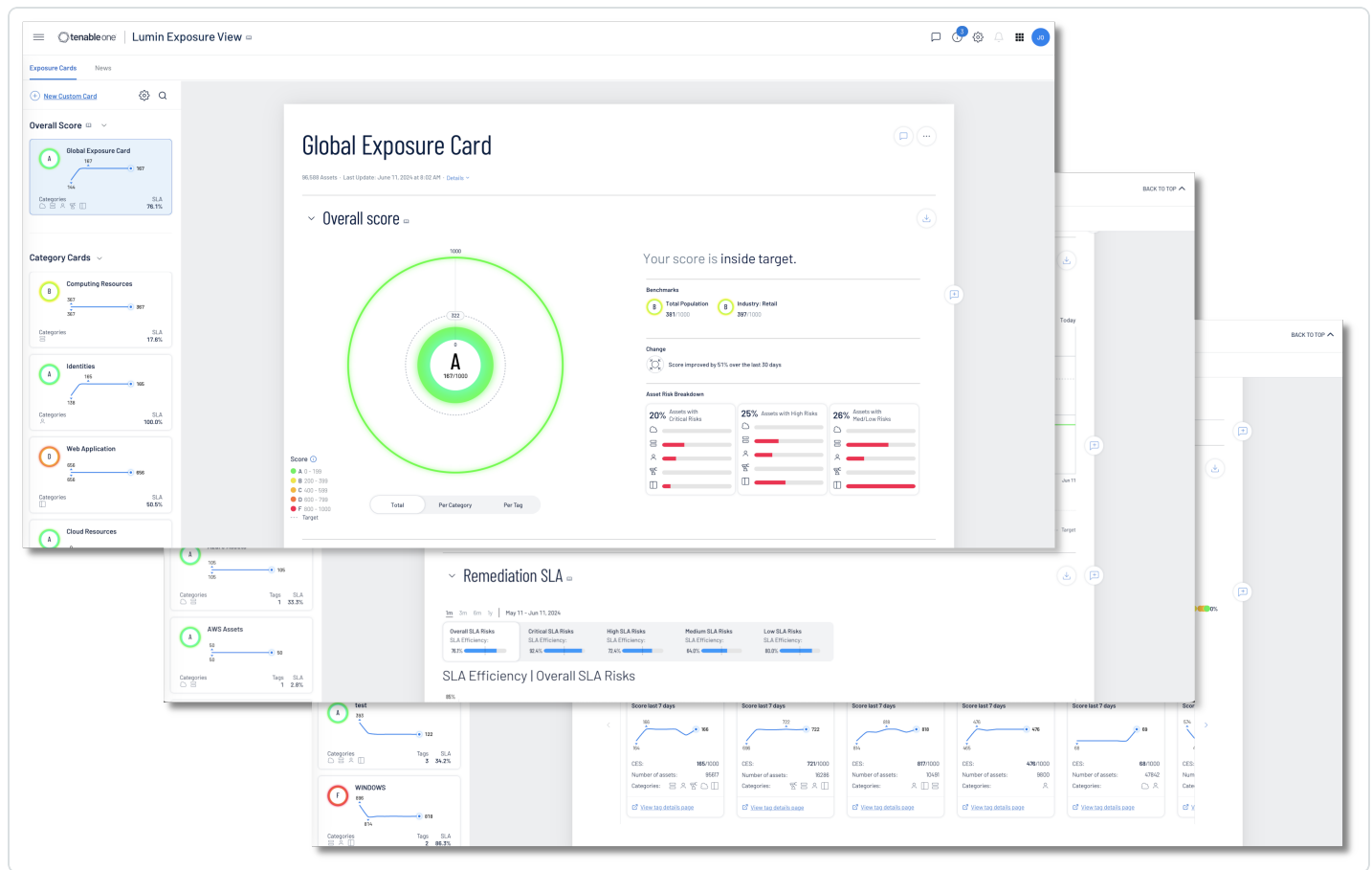
In this section the following Tenable products will be highlighted:

- 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.



Data

TYPE

Vulnerability

QUERY

Select a Query

SOURCE

Cumulative

TOOL

Asset Summary

FILTERS

Vulnerability Priority Rating

Between 9 and 10

Vulnerability Published

Within the last 30 days

Output Assets

Search

☐ Select All

1737 - ASSET

☐ 1737 - static - adtran

1737 - ASSET

☐ 1737 - static - alcatel

1737 - ASSET

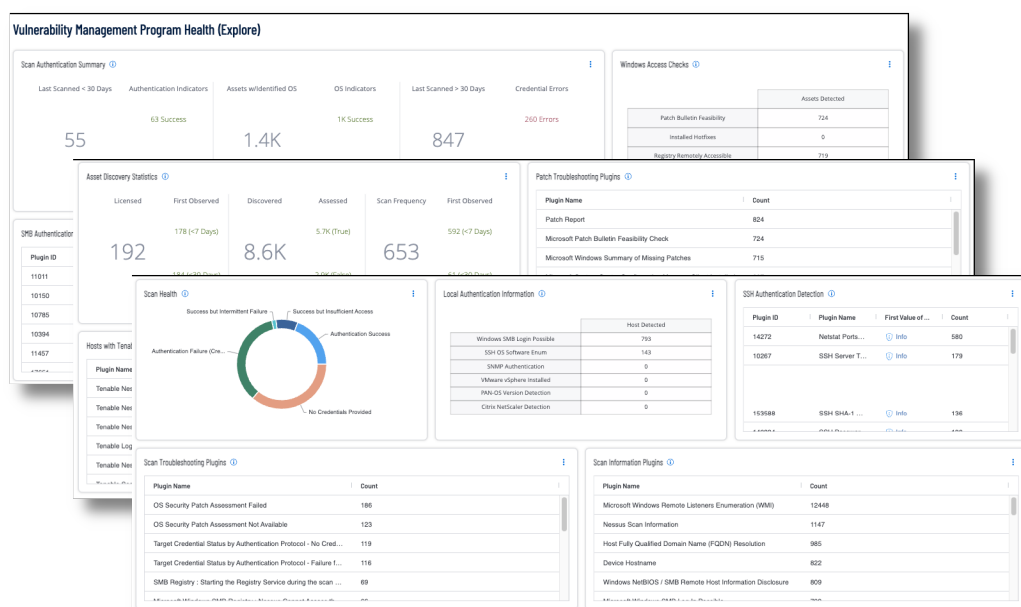
☐ 1737 - static - apple

1737 - ASSET

☐ 1737 - static - arista

1737 - ASSET

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](#).

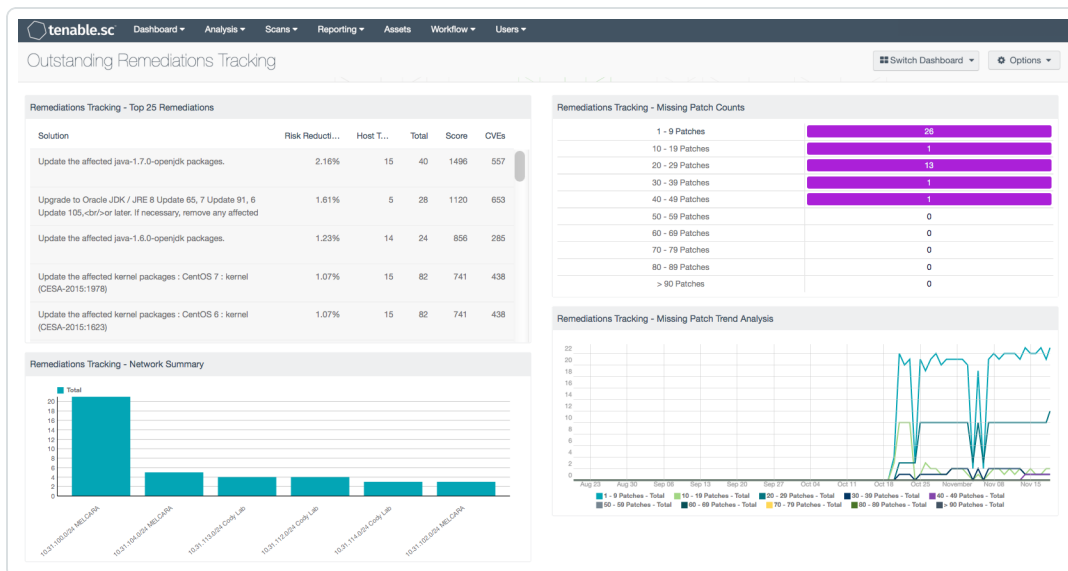
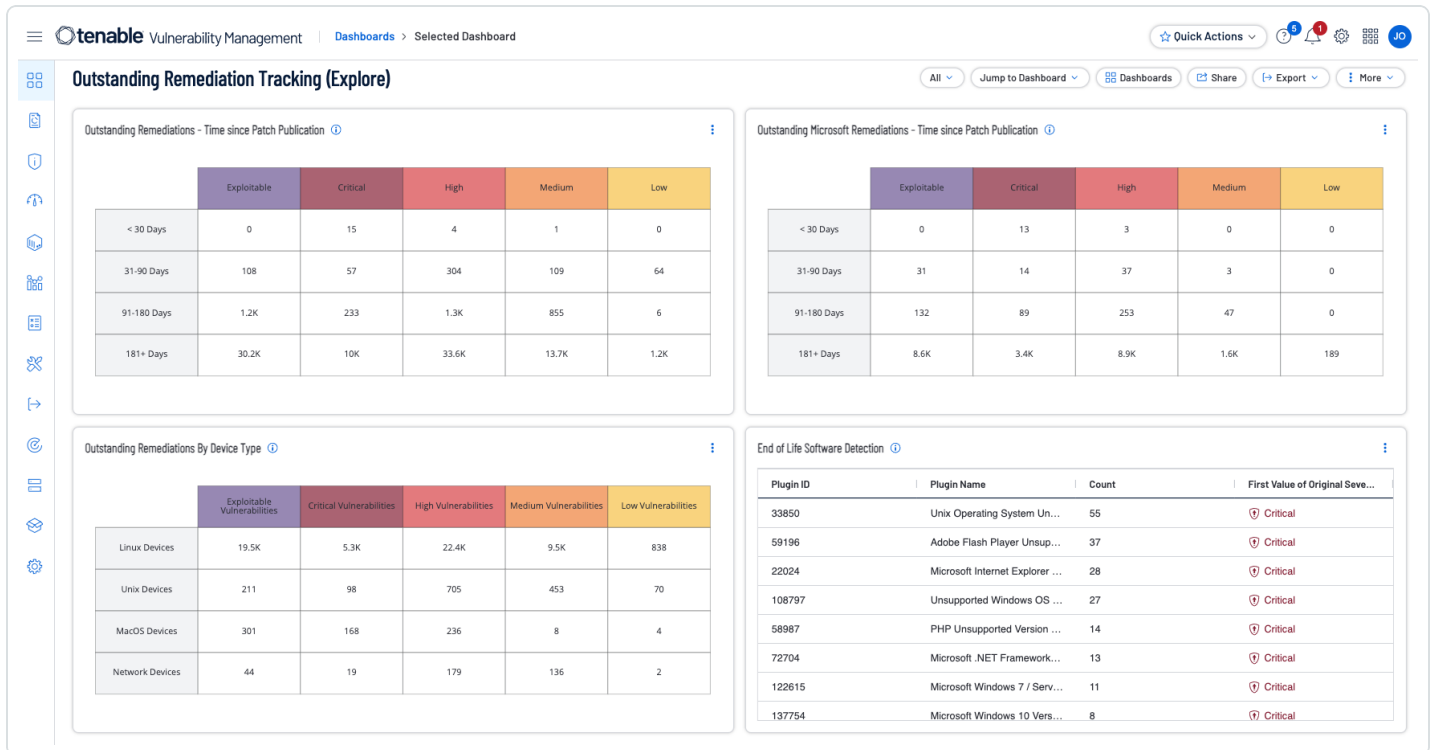
Remediation Tracking

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 screenshot displays the Tenable Vulnerability Management interface. At the top, the 'Findings' page is active, showing a list of vulnerabilities. A filter is applied for 'Plugin ID: is equal to 66334'. The table below shows three findings, with the first one selected. The 'Patch Report' section is expanded, showing details for the selected asset. The 'Plugin Output' tab is selected, displaying the remediation actions and impact for the Apache Log4j vulnerability.

Findings

Advanced | Saved Filters | Search by Asset Name, IP, IP Range, or a CIDR, * for wildcard

Plugin ID: is equal to 66334 | Reset

Group By: None | Asset | Plugin

Filters: Apply

| Asset Name | IPv4 Addr | Severity | Plugin Name | VPR | CVSSv3... | State | Scan Ori... | Asset T... | Last Seen | Actions |
|------------|-----------|----------|--------------|-----|-----------|--------|-------------|------------|------------|---------|
| prod-... | | Info | Patch Report | | | New | Tenable.io | | 10/31/2... | |
| chris-... | | Info | Patch Report | | | New | Tenable.io | Cody: S... | 03/20/2... | |
| audit-... | | Info | Patch Report | | | Active | Tenable.io | | 04/22/2... | |

Patch Report

Asset Information

NAME: ...
IPV4 ADDRESS: ...
OPERATING SYSTEM: Linux Kernel 4.18.0-425.10.1.el8_7.x86_64 on Red Hat Enterprise Linux release 8.7 (Otopa)
SYSTEM TYPE: general-purpose
NETWORK: Default
DNS (FQDN): ...

Additional Information

CLOUD MISCONFIGURATIONS: 0

Asset Scan Information

FIRST SEEN: 10/31/2023 at 09:25 AM
LAST SEEN: 10/31/2023 at 09:25 AM

Vulnerability Information

SEVERITY: Info
PLUGIN ID: 66334
PROTOCOL: TCP
LIVE RESULT: No

Discovery

FIRST SEEN: 10/31/2023 at 09:25 AM
LAST SEEN: 10/31/2023 at 09:25 AM
VULNERABILITY AGE: 205 Days

Overview | Plugin Output

Plugin Output

You need to take the following 39 actions :

[Apache Log4j 2.0 < 2.3.2 / 2.4 < 2.12.4 / 2.13 < 2.17.1 RCE (156327)]

+ Action to take : Upgrade to Apache Log4j version 2.17.1, 2.12.4, or 2.3.2 or later, or apply the vendor mitigation.

Upgrading to the latest versions for Apache Log4j is highly recommended as intermediate versions / patches have known high severity vulnerabilities and the vendor is updating their advisories often as new research and knowledge about the impact of Log4j is discovered. Refer to https://logging.apache.org/log4j/2.x/security.html for the latest versions.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

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**.



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:

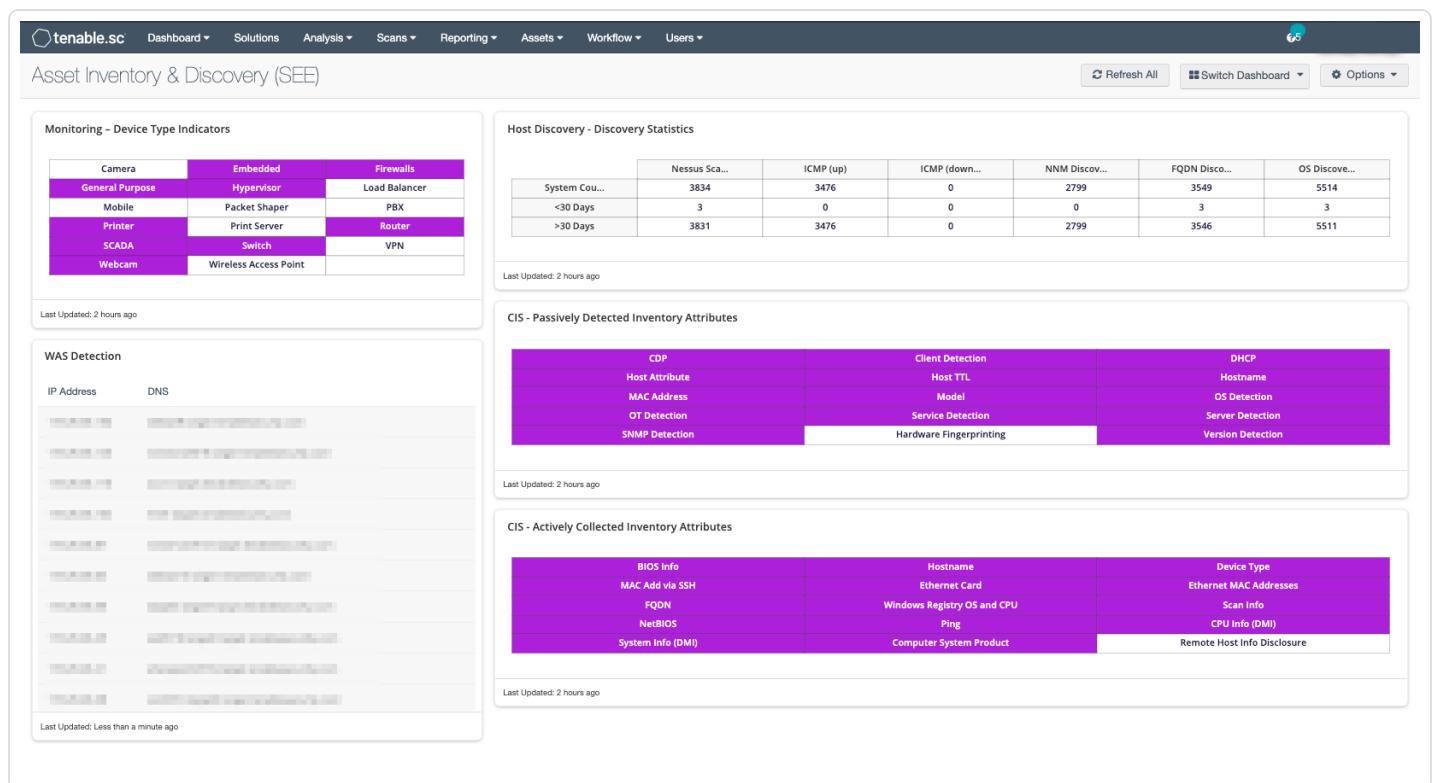
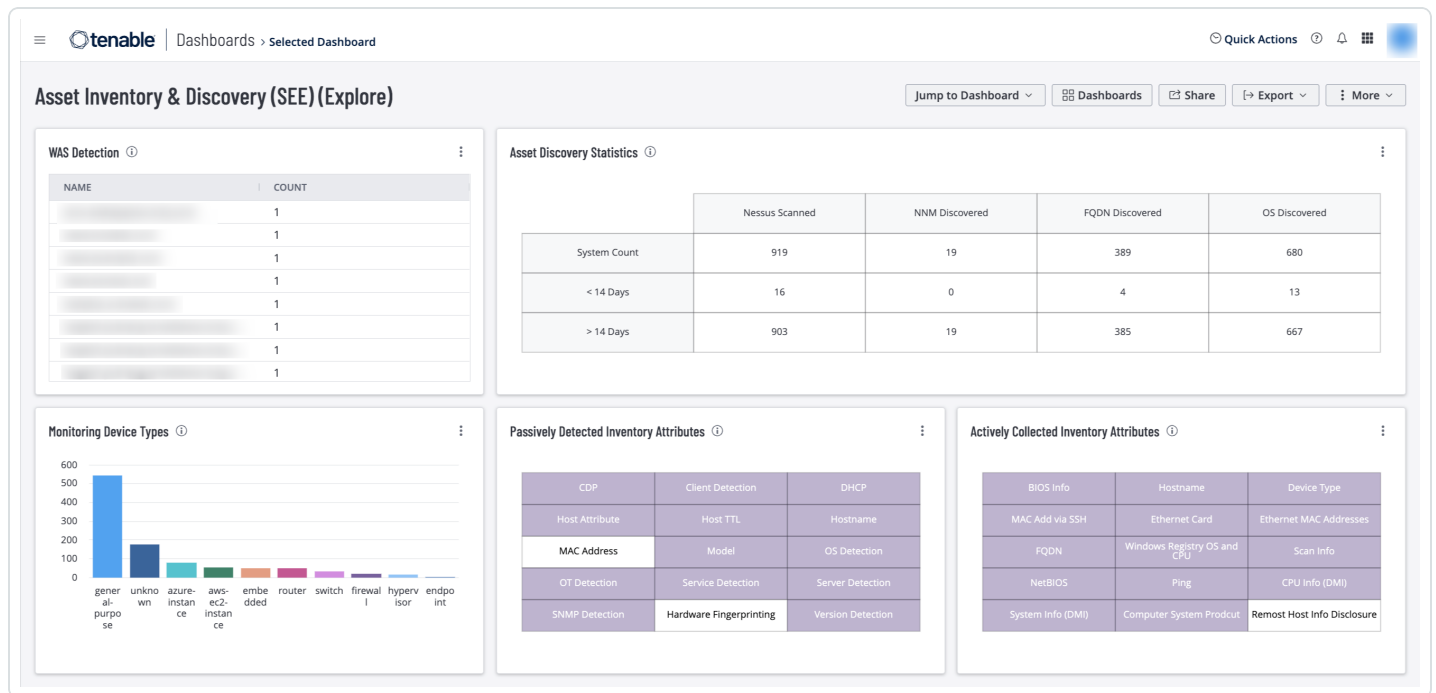
- Actively and passively detected assets
- Asset discovery statistics
- Detected web applications
- Indications for device types (printers, cameras, routers, firewalls, WAPs)

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.

Tenable OT Security | 12:02 PM • Tuesday, May 21, 2024

All Assets Search...

| Name | Type | Risk Score | Criticality | IP | Category | Vendor | Family | Firm |
|--|-------------------|------------|-------------|---------------|----------------|----------------|------------------|---------|
| HR 4 - Comm. Adapter | Communicati... | 67 | High | 192.168.1.100 | Controllers | Rockwell | ControlLogix | 5.001 |
| Packaging 2 - Comm. Adapter | Communicati... | 67 | High | 192.168.1.101 | Controllers | Rockwell | CompactLogix | 2.005 |
| Infusion Mold 3 | PLC | 66 | High | 192.168.1.102 | Controllers | Rockwell | ControlLogix | 31.01 |
| WaterPump1 | PLC | 59 | High | 192.168.1.103 | Controllers | Rockwell | CompactLogix | 20.01 |
| Heat Rollers 4 | PLC | 48 | Low | 192.168.1.104 | Controllers | Rockwell | ControlLogix | 30.01 |
| Packaging 2 | PLC | 47 | Low | 192.168.1.105 | Controllers | Rockwell | CompactLogix | 20.01 |
| PLC 1511C-1 | PLC | 45 | High | 192.168.1.106 | Controllers | Siemens | 57-1500 | 2.0.1 |
| WIN-KL90A8CBO08 | Domain Cont... | 42 | High | 192.168.1.107 | Network Assets | VMware | | |
| ZTCedge1 - HA Appliance | OT Server | 41 | Medium | 192.168.1.108 | Network Assets | Axiom Techn... | Yokogawa | |
| Medical Device #33 | Medical Device | 41 | High | 192.168.1.109 | IoT | VMware | | |
| BAC0 | Controller | 41 | High | 192.168.1.110 | Controllers | Servisys | BAC0 Scriptin... | 3.12... |
| PLC #54 | PLC | 40 | High | 192.168.1.111 | Controllers | Schneider | Modicon M221 | 1.5 |
| col-lab-esx-001.corp.tenablesecurity.com | PLC | 39 | High | 192.168.1.112 | Controllers | Dell | | |
| WaterPump1 - I/O #2 | I/O Module | 39 | High | 192.168.1.113 | Controllers | Rockwell | | 1.001 |
| WaterPump1 - I/O #1 | I/O Module | 39 | High | 192.168.1.114 | Controllers | Rockwell | | 3.001 |
| DESKTOP-05CETH9 | Communicati... | 39 | High | 192.168.1.115 | Controllers | VMware | | |
| WIN-P3FNGET61DF | Security Appli... | 39 | Medium | 192.168.1.116 | Network Assets | VMware | | |
| ML1400 | PLC | 39 | High | 192.168.1.117 | Controllers | Rockwell | MicroLogix 1... | 21.0C |

Items: 84

Version 3.18.51 Expires Sep 17, 2024
Assets Limit 41%



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.

Compliance

[Security Framework Preferences](#)

General

| | |
|-----------------------|---|
| TOTAL ASSETS IN SCOPE | 548 |
| FRAMEWORKS IN SCOPE | ISO 27001 Controls, NIS2 Directive (Article 21) |

Incident Handling

Applies to:

ISO 27001 | Controls: 5.7, 5.25, 5.28, 6.8, 8.7, 8.15, 8.16

NIS2 Directive (Article 21) | measures: b, f, g

Abnormal unresolved events by asset criticality

| Event Category | Asset Criticality: High | Asset Criticality: Medium | Asset Criticality: Low |
|-----------------|-------------------------|---------------------------|------------------------|
| Network Events | 72 | 15 | 6 |
| Network Threats | 89 | 44 | 20 |

[Show Asset List](#)

Event Mean Time to Response (MTTR) - Last 30 Days

| Event Category | Asset Criticality: High | Asset Criticality: Medium | Asset Criticality: Low |
|-----------------|-------------------------|---------------------------|------------------------|
| Network Events | 3 | 1 | 2 |
| Network Threats | 6 | 8 | 0 |

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

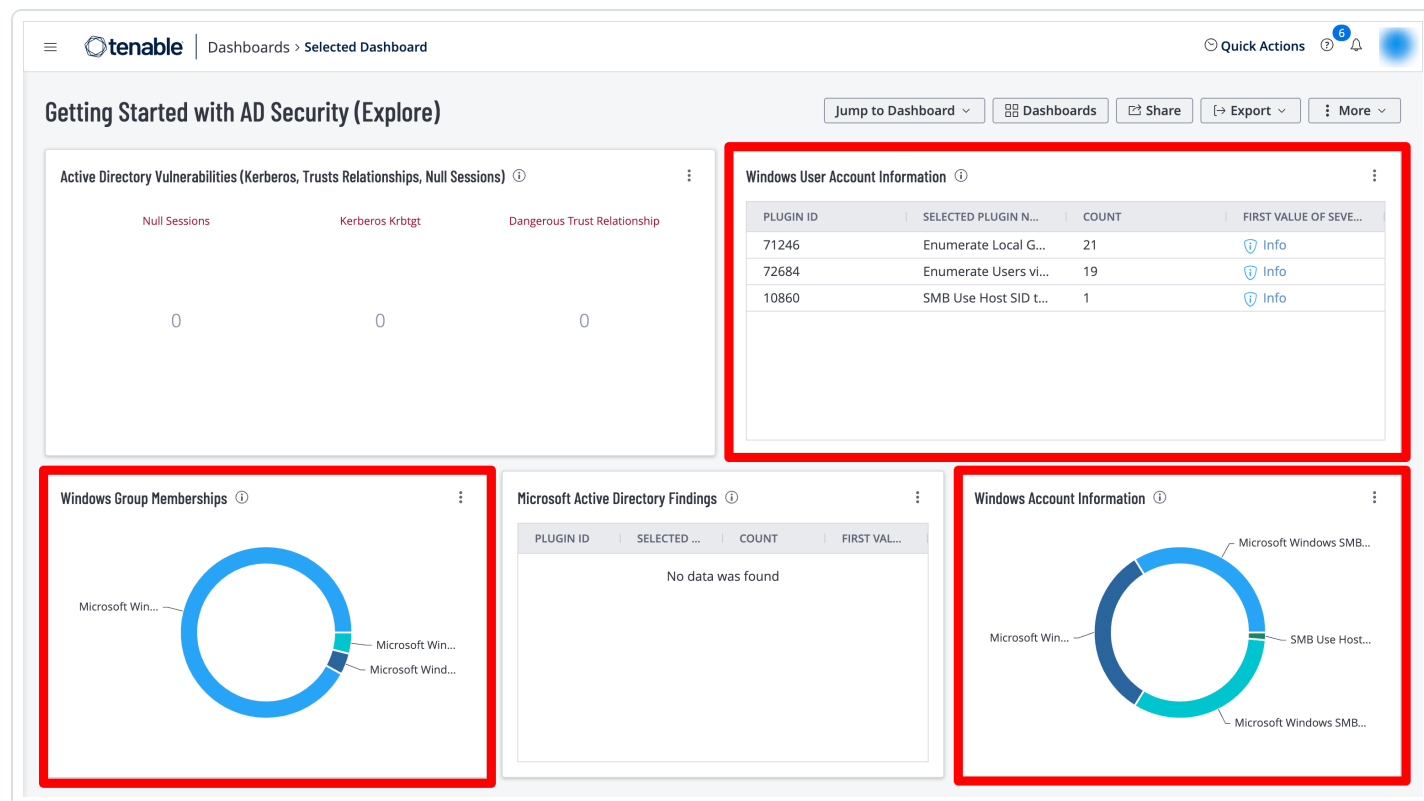
In this section the following Tenable products will be highlighted:

- 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.

CIS Control 4/5: Secure Configurations & Group Memberships

Account Status Indicators - Windows SMB Account Information

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

Last Updated: Less than a minute ago

Account Status Indicators - Local Users Information

- Automatically Disabled Accounts: Can't Change Password
- Disabled Accounts: Never Changed Password
- User has Never Logged in: Passwords Never Expires

Last Updated: Less than a minute ago

CSC - Compliance Checks

| | Systems | Scans (Last 7 Days) | Passed | Manual | Failed |
|-------------|---------|---------------------|--------|--------|--------|
| All CIS CSC | 44 | ✓ | 38% | 5% | 57% |
| All Checks | 67 | ✓ | 36% | 7% | 57% |

Last Updated: Less than a minute ago

CSC - Compliance Checks By Keyword

| | Systems | Scans (Last 7 Days) | Passed | Manual | Failed |
|------------|---------|---------------------|--------|--------|--------|
| All | 67 | ✓ | 36% | 7% | 57% |
| Account | 43 | ✓ | 31% | 2% | 57% |
| Audit | 39 | ✓ | 15% | 16% | 69% |
| Disable | 38 | ✓ | 40% | 1% | 59% |
| Enable | 40 | ✓ | 51% | 1% | 48% |
| Log | 42 | ✓ | 29% | 4% | 68% |
| Password | 37 | ✓ | 20% | 2% | 78% |
| Permission | 35 | ✓ | 48% | 1% | 50% |
| User | 45 | ✓ | 38% | 3% | 59% |

Last Updated: Less than a minute ago

Prioritize Hosts - Top Hosts with Compliance Concerns

| IP Address | DNS | Total | Vulnerabilities |
|-------------|---|-------|-----------------|
| 10.10.10.10 | ubuntu1904-desktop.target.tenablesecurity.com | 283 | 258 (25) |
| 10.10.10.11 | debian9.target.tenablesecurity.com | 282 | 257 (25) |
| 10.10.10.12 | ubuntu1810-desktop.target.tenablesecurity.com | 277 | 251 (26) |
| 10.10.10.13 | ubuntu1904server.target.tenablesecurity.com | 276 | 251 (25) |
| 10.10.10.14 | ubuntu1810-server.target.tenablesecurity.com | 274 | 249 (25) |

Last Updated: Less than a minute ago

Account Status Indicators - Users and SID Information

- Use Host SID to Enumerate Local U: Local User Information
- Automatically disabled accounts: Can't change password
- Disabled accounts: Never changed passwords
- User has never logged on: Passwords never expire
- Guest Account Local User Access: Use Host SID to Enumerate Local U
- Enumerate Local Group Memberships: Enumerate Local Users

Last Updated: Less than a minute ago

Account Status Indicators - Group Memberships

- User Aliases List: User Groups List
- Account Operators Group User List: Administrators Group User List
- Server Operators Group User List: Backup Operators Group User List
- Print Operators Group User List: Replicator Group User List
- Guest Account Belongs to a Group: Domain Administrators Group User List

Last Updated: Less than a minute ago

CIS - Configuration Info Collected during Active Scanning

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

Last Updated: Less than a minute ago

CSC - Account and Group Information

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

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.

Plugins

Settings

Plugins Pipeline

Newest

Updated

Search

Nessus Families

WAS Families

NNM Families

LCE Families

Tenable OT Security Families

About Plugin Families

Nessus Release Notes

Audits

Tenable Cloud Security

Plugins / Search

Plugins Search

Start typing or add a filter...

Filters (1)

Relevance

Plugin Name (Active)

Clear All

Search by Plugin Name

User Enumeration

Page 1 of 15 • 726 Total

Next

| ID | Name | Product | Family | Published | Updated | Severity |
|-------|--|---------|------------|-----------|-----------|----------|
| 45478 | LDAP User Enumeration | Nessus | Misc. | 4/9/2010 | 4/25/2023 | INFO |
| 90067 | WordPress User Enumeration | Nessus | CGI abuses | 3/21/2016 | 4/11/2022 | MEDIUM |
| 29187 | Plumtree Portal User Object User Enumeration | Nessus | CGI abuses | 12/4/2007 | 4/11/2022 | MEDIUM |
| 59358 | Plumtree Portal R10 User Enumeration | Nessus | CGI abuses | 6/6/2012 | 4/11/2022 | MEDIUM |

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.ad

Active Directory

Indicators of Exposure

Indicator details

Search

default

Critical

No indicators

High

No indicators

Medium

Recent

Built-in

Low

No indicators

Recent Use of the Default Administrator Account

Severity: Medium

Status: Not compliant

Information

Vulnerability details

Deviant objects

Recommendations

EXECUTIVE SUMMARY

Built-in administrative accounts should almost never be used (except in very specific cases that rarely happen).

DOCUMENTS

Securing Active Directory Administrative Groups and Accounts

Appendix D: Securing Built-In Administrator Accounts in Active Directory

ATTACKER KNOWN TOOLS

No tools listed for this indicator

IMPACTED DOMAINS

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.

- 29 -



Missing MFA for Privileged Account

MFA provides strong protection for accounts against weak or breached passwords. Security best practices and standards recommend that you enable MFA, especially with privileged accounts. Accounts without an MFA method registered cannot benefit from it...

Tenable Cloud Security Cu... Complexity

Missing MFA for Non-Privileged Account

MFA provides strong protection for accounts against weak or breached passwords. Security best practices and standards recommend that you enable MFA, even for non-privileged accounts. Accounts without an MFA method registered cannot benefit from it.

Tenable Cloud Security Cu... Complexity

- [MITRE ATT&CK] T1098 (Account Manipulation)
- [MITRE ATT&CK] T1110 (Brute Force)
- [MITRE ATT&CK] T1566.006 (Modify Authentication Process: Multi-Factor Authentication)
- [MITRE ATT&CK] T1078.004 (Valid Accounts: Cloud Accounts)

| Type | Object | Provider | Tenant | Description | Date (HH:MM:SS, YYYY-MM-DD) |
|---------|-----------------------------------|--------------------|-----------------------------------|---|-----------------------------|
| ACCOUNT | Scott | Microsoft Entra ID | Tenable Cloud Security Customer 2 | Scott (object ID=...-1ee1a9e2ad87) does not show any registered MFA method, which means that this privileged account with the Global Administrator role (role ID=62e1...-f-9e72-1ee1a9e2ad87) does not benefit from MFA protection. | 16:33:40, 2024-04-23 |
| ACCOUNT | Super Admin | Microsoft Entra ID | Tenable Cloud Security Customer 2 | Super Admin (object ID=841...-f3e1...) | 16:33:40, 2024-04-23 |
| ACCOUNT | Super Admin | Microsoft Entra ID | Tenable Cloud Security Customer 2 | Super Admin (object ID=b1b...-6228...) | 16:33:40, 2024-04-23 |
| ACCOUNT | Alex | Microsoft Entra ID | Tenable Cloud Security Customer 2 | Alex Feigenson (object ID=...-f72fe...) | 16:33:40, 2024-04-23 |
| ACCOUNT | On-Premises Directory Synchron... | Microsoft Entra ID | Tenable Cloud Security Customer 2 | On-Premises Directory Synchronization Service Account (objec... | 16:33:40, 2024-04-23 |

| Type | Object | Provider | Tenant | Description | Date (HH:MM:SS, YYYY-MM-DD) |
|---------|--------|--------------------|-----------------------------------|--|-----------------------------|
| ACCOUNT | Kristi | Microsoft Entra ID | Tenable Cloud Security Customer 2 | Kristi (object ID=29c8b962-dfcd-...-ID=a441755d-8723-4...) | 16:33:40, 2024-04-23 |
| ACCOUNT | Danico | Microsoft Entra ID | Tenable Cloud Security Customer 2 | Danico (object ID=...-ID=e817ed39-4f2d-49...) | 16:33:40, 2024-04-23 |
| ACCOUNT | Melba | Microsoft Entra ID | Tenable Cloud Security Customer 2 | Melba (object ID=734b9dc1-4e56...) | 16:33:40, 2024-04-23 |
| ACCOUNT | Miles | Microsoft Entra ID | Tenable Cloud Security Customer 2 | Miles (object ID=8f7f78ce-ae78...) | 16:33:40, 2024-04-23 |
| ACCOUNT | Maria | Microsoft Entra ID | Tenable Cloud Security Customer 2 | Maria (object ID=01e2143a-a4...) | 16:33:40, 2024-04-23 |
| ACCOUNT | Arthu | Microsoft Entra ID | Tenable Cloud Security Customer 2 | Arthu (object ID=a9a4c3dc-d88f-...) | 16:33:40, 2024-04-23 |
| ACCOUNT | Eilee | Microsoft Entra ID | Tenable Cloud Security Customer 2 | Eilee (object ID=d1a32d57-6b8e-...) | 16:33:40, 2024-04-23 |
| ACCOUNT | Corrie | Microsoft Entra ID | Tenable Cloud Security Customer 2 | Corrie (object ID=01e2143a-a4...) | 16:33:40, 2024-04-23 |
| ACCOUNT | Skyli | Microsoft Entra ID | Tenable Cloud Security Customer 2 | Skyli (object ID=da5585...) | 16:33:40, 2024-04-23 |
| ACCOUNT | Milton | Microsoft Entra ID | Tenable Cloud Security Customer 2 | Milton (object ID=458f7145-54a5...) | 16:33:40, 2024-04-23 |
| ACCOUNT | Elton | Microsoft Entra ID | Tenable Cloud Security Customer 2 | Elton (object ID=83124597-1e7a-4c...) | 16:33:40, 2024-04-23 |
| ACCOUNT | Kenne | Microsoft Entra ID | Tenable Cloud Security Customer 2 | Kenne (object ID=8f2995b7-261...) | 16:33:40, 2024-04-23 |
| ACCOUNT | Hugo | Microsoft Entra ID | Tenable Cloud Security Customer 2 | Hugo (object ID=31a3cf49-bc08...) | 16:33:40, 2024-04-23 |
| ACCOUNT | Nikol | Microsoft Entra ID | Tenable Cloud Security Customer 2 | Nikol (object ID=82d1284f-...) | 16:33:40, 2024-04-23 |
| ACCOUNT | Nathe | Microsoft Entra ID | Tenable Cloud Security Customer 2 | Nathe (object ID=6f4a6e49-8...) | 16:33:40, 2024-04-23 |

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.

tenable Identity Exposure

Indicators of Exposure

Search for an indicator

Show all indicators Yes 4/4 domains >

Critical

Unsecured Configuration of Netlogon Protocol

CVE-2020-1472 ("Zerologon") affects Netlogon protocol and allows elevation of privilege

▲ 4 domains Complexity

Mapped Certificates on Accounts

Ensures that privileged objects do not have any mapped certificate assigned to them.

▲ demo Complexity

Domain Controllers Managed by Illegitimate Users

Some domain controllers can be managed by non-administrative users due to dangerous access rights.

▲ 3 domains Complexity

Verify Sensitive GPO Objects and Files Permissions

Ensures that the permissions assigned to GPO objects and files linked to sensitive containers, such as the domain controllers or OU, are appropriate and secure.

▲ 3 domains Complexity

User Primary Group

Verify users' Primary Group has not been changed

▲ No domain Complexity

WSUS Dangerous Misconfigurations

Lists the misconfigured parameters related to Windows Server Update Services (WSUS).

▲ No domain Complexity

ADCS Dangerous Misconfigurations

List dangerous permissions and misconfigured parameters related to the Windows Public Key Infrastructure (PKI).

▲ demo Complexity

Verify Permissions Related to Microsoft Entra Connect Accounts

Ensure the permissions set on Microsoft Entra Connect accounts are sane

▲ 2 domains Complexity

Application of Weak Password Policies on Users

Some password policies applied on specific user accounts are not strong enough and can lead to credentials theft.

▲ 4 domains Complexity

Root Objects Permissions Allowing DCSync-Like Attacks

Checks for unsafe permissions on root objects that may enable unauthorized users to steal authentication credentials.

▲ demo Complexity

Dangerous Kerberos Delegation

Checks for unauthorized Kerberos delegation, and ensures protection for privileged users against it.

▲ demo Complexity

Ensure SDProp Consistency

Control that the adminSDHolder object is in a clean state.

▲ demo Complexity

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.



tenable Cloud Security MISCONFIGURATIONS REPORT

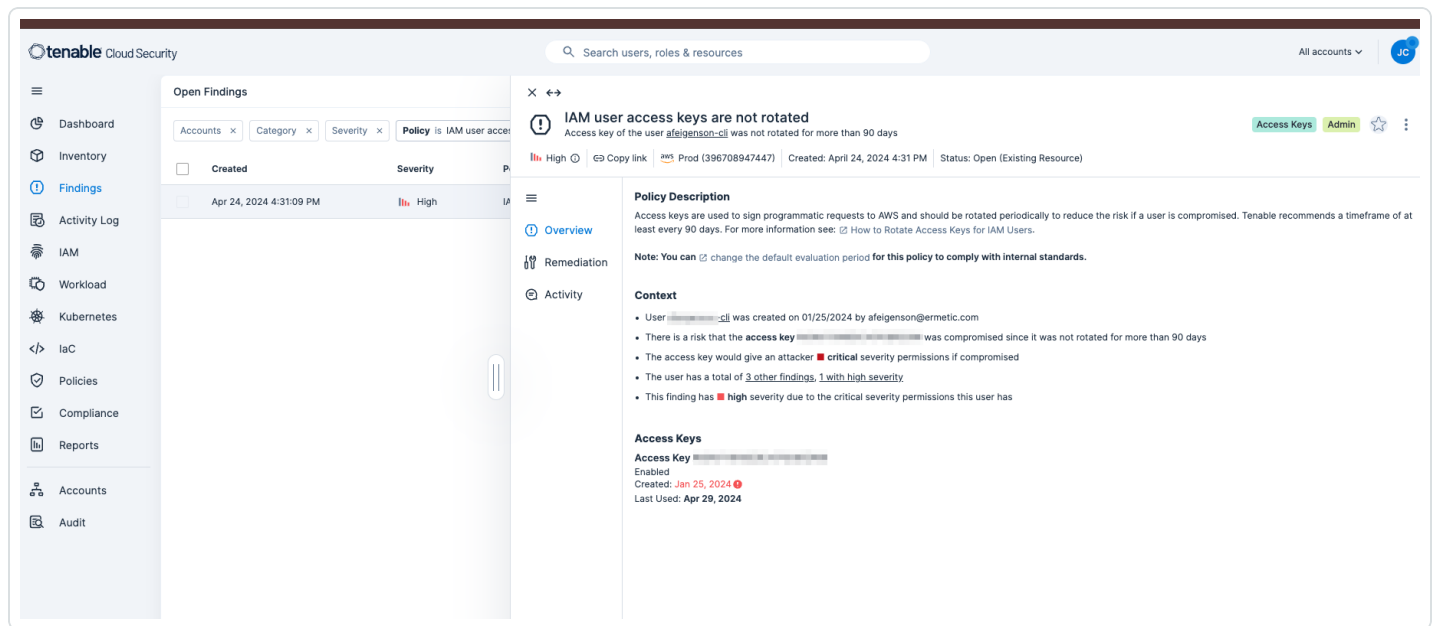


IAM

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 | | 2 Accounts | 0 | 2 |
| aws | IAM access analyzer is not enabled for all regions | | 2 Accounts | 0 | 2 |
| aws | IAM server certificate is expired | | 0 IAM Server Certificates | 0 | - |
| aws | IAM user access keys are not rotated | | 1 IAM User | 0 | 1 |
| aws | IAM user has multiple active access keys | | 24 IAM Users | 22 | 2 |
| aws | IAM user has policies attached | | 24 IAM Users | 19 | 5 |
| aws | IAM user MFA is not enabled | | 15 IAM Users | 0 | 14 1 |
| aws | IAM user unused access keys | | 22 IAM Users | 0 | 19 3 |

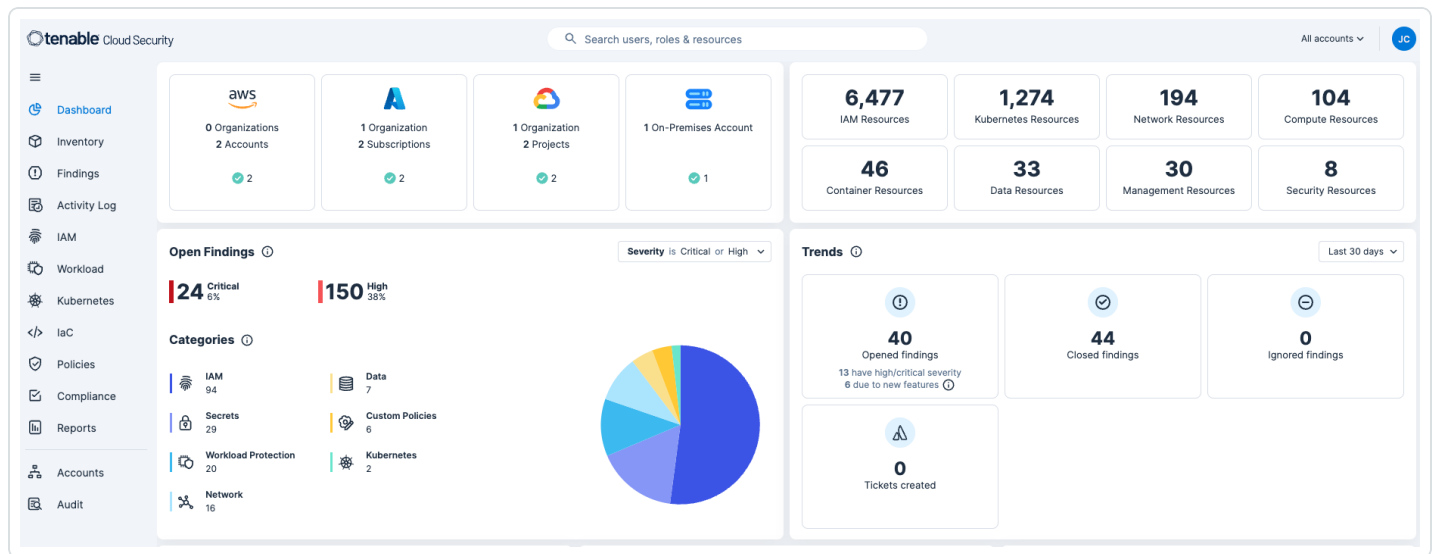
Details within each policy violation contain an overview, policy violation details, and policy remediation strategies, as well as defining any impacted resources. Policies are used to identify misconfigurations and vulnerabilities present on cloud resources. Tenable Cloud Security has built-in policies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

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 attack 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). 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).

The screenshot displays the Tenable One Asset Inventory interface. At the top, there's a navigation bar with the Tenable One logo and 'Inventory' text. Below this, a sidebar on the left contains a dropdown menu labeled 'Assets' with options for 'Assets', 'Tags', and 'Weaknesses'. The main area shows a summary of asset counts: 3.4k total assets, 4 new assets in the last 7 days, and 972 updated assets in the last 7 days. Below the summary, there are five buttons for different security views: Vulnerability Management (100%), Identity Exposure (<1%), Web Application Security (0%), Cloud Security (0%), and OT Security (<1%). The main table lists assets with columns for Asset, AES, Class, Weaknesses, Number of tags, Last Updated, and Sources. The table contains 15 rows of asset data, including details like 'svr-sharepoint', 'qa-webapp', 'tenable-pbrf54bz.dc.demo.io', etc.

| Asset | AES | Class | Weaknesses | Number of tags | Last Updated | Sources |
|-------------------------------|-----|--------|------------|----------------|--------------|-----------------------------|
| svr-sharepoint | 751 | Device | 317 | 5 | June 3, 2024 | See Details |
| qa-webapp | 700 | Device | 683 | 5 | June 3, 2024 | See Details |
| tenable-pbrf54bz.dc.demo.io | 700 | Device | 1,124 | 6 | June 1, 2024 | See Details |
| prod-ssh-command.labnet.local | 696 | Device | 1,104 | 5 | June 3, 2024 | See Details |
| rhell.dc.demo.io | 684 | Device | 338 | 6 | June 3, 2024 | See Details |
| win-8bgf8bnvk6 | 673 | Device | 35 | 5 | May 18, 2024 | See Details |
| dwva-ubuntu.labnet.local | 673 | Device | 60 | 5 | June 3, 2024 | See Details |
| deblan0-demo.labnet.local | 654 | Device | 210 | 5 | May 25, 2024 | See Details |
| kms.labnet.local | 635 | Device | 66 | 5 | May 25, 2024 | See Details |
| water-plant-01 | 632 | Device | 3,285 | 5 | June 3, 2024 | See Details |
| dev-sc-team-expansion-child-1 | 631 | Device | 2,383 | 5 | June 2, 2024 | See Details |
| al-win10-rg1 | 631 | Device | 1,598 | 5 | June 3, 2024 | See Details |
| al-win10-tp | 631 | Device | 1,598 | 5 | June 3, 2024 | See Details |
| al-win10-co | 631 | Device | 1,597 | 5 | June 3, 2024 | See Details |

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](#).

The screenshot shows the Tenable One interface for an asset named 'Sql2019'. The top navigation bar includes the Tenable One logo and 'Inventory'. A breadcrumb trail shows 'Back to Asset Inventory'. The asset details section includes a summary of the asset's role as a domain controller and DNS server, its criticality score of 9, and a list of weaknesses including CVE-2021-28471, CVE-2021-40444, and CVE-2019-1405. Below this, four key metrics are displayed: Asset Exposure Score (947/1000), Asset Criticality Rating (9/10), Weaknesses Identified (3,450), and Key Properties (Asset Class: Profile Drivers, Last Observed At: Jun 4, 2024 at 11:55 am). A horizontal tab bar allows switching between Properties, Liveboard, Attack Paths, Weaknesses, Tags, Exposure Cards, Relationships, and Accounts. The 'Key Properties (5)' section is currently active, showing a table with columns for Asset Class, Device, Created Date, and Host System Type.

| Asset Class | Device | Created Date | Host System Type |
|--------------------------|-------------|--------------------------|------------------|
| Host Fully Qualified DNS | sql2019-001 | Sep 26, 2022 at 05:36 pm | general-purpose |

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.

Sensor updates are available [View Sensors](#)

10:36 AM • Friday, May 24, 2024 • Joe

Dashboards

Risk

Inventory

Events and Policies

Events

Policies

Inventory

All Assets

Controllers and Modules

Network Assets

IoT

Network Map

Vulnerabilities

Active Queries

Network

Groups

Local Settings

WaterPump1

PLC

IP: 172.17.0.101 MAC: 98:96:1B:16:00:00 Vendor: Rockwell Model: 1769-L24ER-QB1B/A LOGIX5324ER Last Seen: May 24, 2024 10:34:28 AM State: Fault Family: CompactLogix 5370 Firmware: 20.012

Details

Code Revision

IP Trail

Attack Vectors

Open Ports

Vulnerabilities

Events

Network Map

Overview

NAME: WaterPump1

DESCRIPTION: Rockwell Automation 1769-L24ER-QB1B

PURDUE LEVEL: Level 1

STATE: Fault

EXTENDED STATE: MajorFault

LAST STATE UPDATE: 05:48:38 PM • May 23, 2024

DIRECT IP: 172.17.0.101

DIRECT MAC: 98:96:1B:16:00:00

FAMILY: CompactLogix 5370

VENDOR: Rockwell

MODEL NAME: 1769-L24ER-QB1B/A LOGIX5324ER

LAST SEEN: 10:34:28 AM • May 24, 2024

FIRST SEEN: 03:22:58 PM • Oct 29, 2021

LAST UPDATE: 05:48:38 PM • May 23, 2024

NETWORK SEGMENTS: 172.17.0.101

Backplane View

Backplane #2

0 1 2 3 4 5 6 7 8

WaterPump1 - I/O #1

WaterPump1 - I/O #2

WaterPump1

PLC Details

NAME: WaterPump1

RISK SCORE: 59

TYPE: PLC

DESCRIPTION: Rockwell Automation 1769-L24ER-QB1B

MODEL: 1769-L24ER-QB1B/A LOGIX5324ER

VENDOR: Rockwell

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

- 37 -

The screenshot shows the Tenable OT Security web interface. The top navigation bar includes the Tenable logo, 'OT Security', and user information. A sidebar on the left contains a menu with options like Dashboards, Risk, Inventory, Events and Policies, Events, Policies, Inventory (with sub-options like All Assets, Controllers and Modules, Network Assets, IoT, Network Map, Vulnerabilities, Active Queries, Network, Groups, and Local Settings), and Vulnerabilities. The main content area displays a network map for 'WaterPump1' (PLC). The map shows a central node 'WaterPump1' connected to four other nodes: 'Tenable.ot - FT/HA', 'WIN-18OFIPB12HM', 'OT11 - PowerEdge R340', and 'OT8 - SE350'. A search bar and a 'Go to network map' button are visible. The bottom left corner indicates 'Version 3.18.51 Expires Sep 17, 2024'.

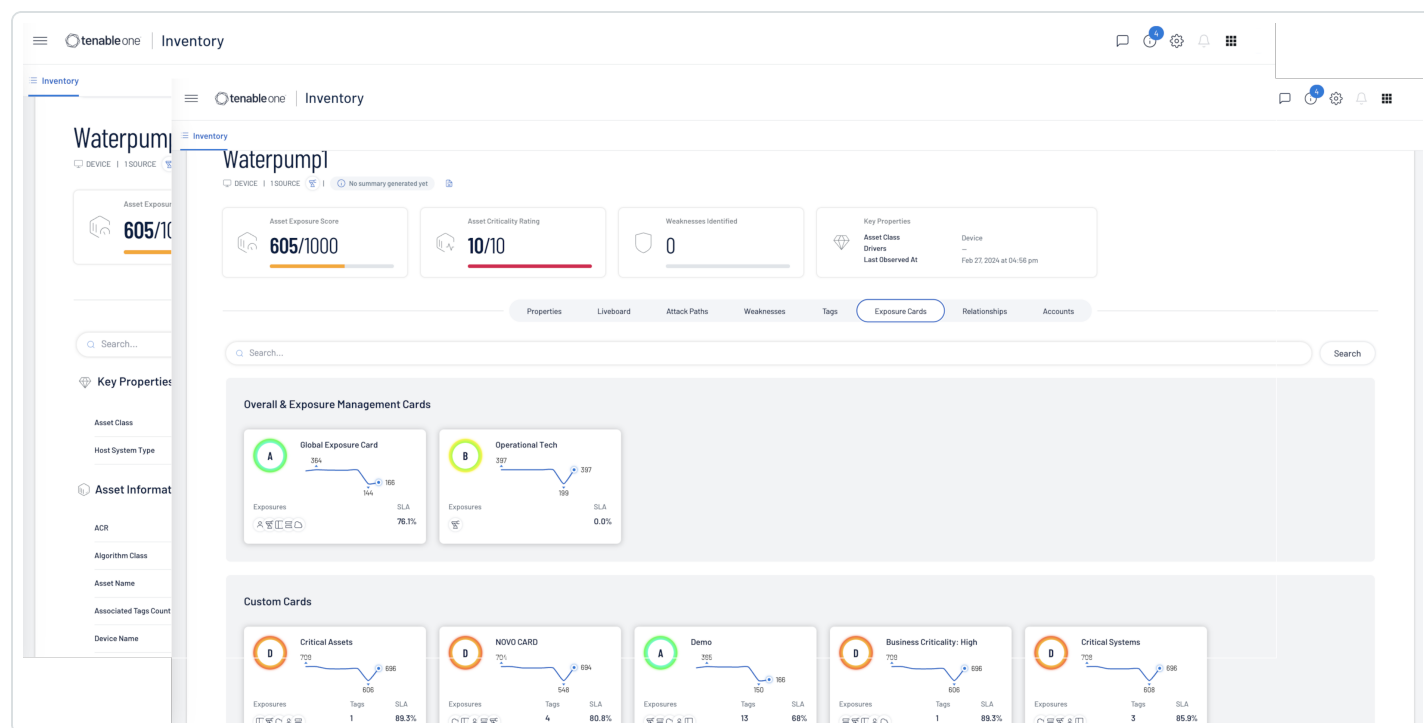
Utilising Tenable One, OT Assets can be displayed by selecting the OT Security icon.

The screenshot shows the Tenable One 'Inventory' page. At the top, there's a navigation bar with the Tenable logo and 'Inventory'. Below it, a sub-header 'Assets' is followed by several security status indicators: Vulnerability Management (12%), Identity Exposure (0%), Web Application Security (0%), Cloud Security (0%), and OT Security (100%). A red arrow points to the 'OT Security' icon. To the right of these indicators, summary statistics are shown: 'Number Of Assets' (138), 'New Assets in Last 7 Days' (0), and 'Updated Assets in last 7 days' (33). Below this is a search bar with the text 'FIND > Assets' and a placeholder 'Search by typing a valid query'. The main part of the page is a table listing various assets.

| Name | AES | Class | Weaknesses | Number of tags | Last Updated | Sources |
|------------------------|-----|--------|------------|----------------|-------------------|-----------------------------|
| rouge | 738 | Device | | 0 3 | June 5, 2024 | See Details |
| devicenet_181 | 723 | Device | | 0 3 | June 5, 2024 | See Details |
| infusion_mold_3 | 695 | Device | | 0 3 | June 5, 2024 | See Details |
| packaging_2 | 694 | Device | | 0 3 | June 5, 2024 | See Details |
| comm. adapter #1 | 689 | Device | | 0 3 | June 5, 2024 | See Details |
| perseverance | 689 | Device | | 0 3 | June 5, 2024 | See Details |
| comm. adapter #3 | 681 | Device | | 0 3 | June 5, 2024 | See Details |
| eng control station 01 | 666 | Device | | 0 3 | February 27, 2024 | See Details |
| win-ueupf5dga0h | 664 | Device | | 0 3 | February 27, 2024 | See Details |
| heat_rollers_4 | 661 | Device | | 0 3 | June 5, 2024 | See Details |
| waterpump1 | 605 | Device | | 0 3 | June 5, 2024 | See Details |
| naoh_pump | 605 | Device | | 0 3 | June 5, 2024 | See Details |
| comm. adapter #65 | 598 | Device | | 0 3 | June 5, 2024 | See Details |
| comm. adapter #41 | 597 | Device | | 0 3 | June 5, 2024 | See Details |



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.

Sql2019

DEVICE | 1 SOURCE | Last Updated: May 13, 2024 | Hide Summary

About this asset
The asset 'sql2019' is a virtual machine with a high asset criticality score of 9 and a relatively high asset exposure score of 947. It plays a crucial role as a domain controller and DNS server in the network. However, it is concerning that this asset has 77 critical and 389 high-risk vulnerabilities, making it highly susceptible to cyber threats. Immediate attention and remediation are required to mitigate these risks and protect the organization's sensitive data and overall security posture.

Weaknesses
This asset is exposed to several critical vulnerabilities, including CVE-2021-2641l, CVE-2021-40444, CVE-2019-1405, CVE-2021-1675, CVE-2020-0674, CVE-2021-34627, CVE-2019-1053, CVE-2019-0555, and CVE-2022-30180. These vulnerabilities allow for remote code execution, elevation of privileges, and unauthorized access, posing significant risks to the organization's data and systems. Prompt patching and security measures are essential to address these vulnerabilities and minimize the attack surface.

Asset Exposure Score: 947/1000
Asset Criticality Rating: 9/10
Weaknesses Identified: 3,450

Key Properties
Asset Class: Profile Drivers
Last Observed At: Jun 4, 2024 at 11:55 am

Properties | Liveboard | Attack Paths | Weaknesses | Tags | Exposure Cards | Relationships | Accounts

Key Properties (5)

| Asset Class | Device | Created Date | Host System Type |
|--------------------------|---------|--------------------------|------------------|
| Host Fully Qualified DNS | sql2019 | Sep 26, 2022 at 05:36 pm | general-purpose |

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

Weaknesses

This asset is exposed to several critical vulnerabilities, including CVE-2021-2641l, CVE-2021-40444, CVE-2019-1405, CVE-2021-1675, CVE-2020-0674, CVE-2021-34627, CVE-2019-1053, CVE-2019-0555, and CVE-2022-30180. These vulnerabilities allow for remote code execution, elevation of privileges, and unauthorized access, posing significant risks to the organization's data and systems. Prompt patching and security measures are essential to address these vulnerabilities and minimize the attack surface.

Asset Exposure Score: 947/1000
Asset Criticality Rating: 9/10
Weaknesses Identified: 3,450

Key Properties
Asset Class: Profile Drivers
Last Observed At: Jun 6, 2024 at 11:55 am

Properties | Liveboard | Attack Paths | **Weaknesses** | Tags | Exposure Cards | Relationships | Accounts

| Weakness Name | Type | Description | Severity | VPR | Impacted Assets | Sources | Last Seen |
|----------------|---------------|-------------------------------------|----------|-----|-----------------|---------|--------------|
| CVE-2023-20569 | Vulnerability | A side channel vulnerability o... | Medium | 8.1 | 192 | ... | June 6, 2024 |
| CVE-2022-43562 | Vulnerability | A use after free vulnerability e... | Medium | 4.4 | 187 | ... | June 6, 2024 |
| CVE-2019-11135 | Vulnerability | TSX Asynchronous Abort cond... | Medium | 5.2 | 174 | ... | June 6, 2024 |
| CVE-2022-38023 | Vulnerability | Netlogon RPC Elevation of Pri... | High | 7.4 | 144 | ... | June 6, 2024 |
| CVE-2018-12207 | Vulnerability | Improper invalidation for pag... | High | 7.1 | 139 | ... | June 6, 2024 |
| CVE-2019-9506 | Vulnerability | The Bluetooth BR/EDR specifi... | Medium | 6 | 133 | ... | June 6, 2024 |
| CVE-2023-44487 | Vulnerability | The HTTP/2 protocol allows a ... | Medium | 6.7 | 132 | ... | June 6, 2024 |
| CVE-2013-3800 | Vulnerability | The WinVerifyTrust function L... | High | 8.9 | 122 | ... | June 6, 2024 |

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.



tenable.sc

Dashboard

Solutions

Analysis

Scans

Reporting

Assets

Workflow

Users

3

Establishing a Software Inventory (SEE)

Refresh All

Switch Dashboard

Options

Unsupported Product Summary - Operating Systems

| Fedora | Ubuntu | Slackware |
|--------|----------|-----------|
| Debian | Mandrake | Mac OS X |
| CentOS | openSUSE | Microsoft |

Last Updated: 10 minutes ago

Configuration Management - Detected Software

| Windows OS | Linux OS | macOS | Other OS | OS ID Failed |
|-----------------|-------------|-------------------|----------------|--------------|
| Chrome | Firefox | Internet Explorer | Microsoft Edge | Safari |
| Software per IP | Common Apps | Open Source Apps | Apps w/NVR >7 | Unsupported |

Last Updated: 10 minutes ago

CIS - Installed Software

| Linux | Mac OS X Software | Microsoft | Solaris |
|-------|-------------------|-----------|---------|
|-------|-------------------|-----------|---------|

Last Updated: 10 minutes ago

Software Inventory - Active Processes and Startup Programs

6 Items | 1 to 6 of 6 << < Page 1 of 1 > >

| PLUGIN ID | NAME | TOTAL |
|-----------|--|-------|
| 10456 | Microsoft Windows SMB Service Enumeration | 2001 |
| 58452 | Microsoft Windows Startup Software Enumeration | 1393 |
| 24269 | WMI Available | 1345 |
| 70331 | Microsoft Windows Process Module Information | 1343 |
| 70329 | Microsoft Windows Process Information | 1342 |
| 110483 | Unix / Linux Running Processes Information | 34 |

Last Updated: 22 hours ago

Unsupported Product Summary - Applications

33 Items | 1 to 5 of 33 << < Page 1 of 7 > >

| PLUGIN ID | NAME | SEVERITY | TOTAL |
|-----------|----------------------------|----------|-------|
| 62758 | Microsoft XML Parser (...) | Critical | 492 |
| 90544 | Apple QuickTime Unsup... | Critical | 367 |
| 40362 | Mozilla Foundation Uns... | Critical | 347 |
| 64784 | Microsoft SQL Server U... | Critical | 226 |
| 56212 | Adobe Acrobat Unsupp... | Critical | 96 |

Last Updated: May 11, 2022 13:31

InfoSec Team - Roadblocks Currently Gating Remediation

| Windows Host Missing Rollup KBs | Hosts Requiring Additional Patch/Config Act... |
|--|--|
| Windows Hosts with Unsupported/Missing Serv... | 0 |
| Windows Reboot Required to Apply Patch | 302 |
| Vendor Requires Registry Key Change to Reme... | 1407 |
| Remote Host Missing Patches - Includes Step... | 1883 |
| Remediation Requires Disabling Something on... | 1412 |
| Red Hat/CentOS Hosts Where Service Restart ... | 1 |

Last Updated: 22 hours ago

CSC - Inventory of Authorized and Unauthorized Software

| | Last 24 Hrs | Last 7 Days | > 7 Days |
|------------------|-------------|-------------|----------|
| Unsupported Apps | 0 | 0 | 393 |
| Missing Patches | 3 | 8 | 1342 |

Last Updated: 9 minutes ago

Software Summary - Top Installed Software

100 Items | 1 to 6 of 100 << < Page 1 of 17 > >

| NAME | COUNT | DETECTION METHOD |
|---|-------|------------------|
| Local Administrator Password Solution ... | 1357 | Active |
| Microsoft Silverlight [version 5.1.50918.0] | 1192 | Active |
| Google Update Helper [version 1.3.35.4... | 1133 | Active |
| Adobe Refresh Manager [version 1.8.0] | 1011 | Active |
| Microsoft Visual C++ 2010 x86 Redistrib... | 973 | Active |
| Microsoft Visual C++ 2010 x64 Redistrib... | 941 | Active |

Last Updated: 1 hour ago

Network Services Summary - Service Detection Summary

95 Items | 1 to 7 of 95 << < Page 1 of 14 > >

| PLUGIN ID | NAME | SEVERITY | TOTAL |
|-----------|-----------------------------|----------|-------|
| 20007 | SSL Version 2 and 3 Prot... | Critical | 344 |
| 10205 | rlogin Service Detection | High | 3 |
| 104743 | TLS Version 1.0 Protocol... | Medium | 2490 |
| 121010 | TLS Version 1.1 Protocol... | Medium | 2293 |
| 12218 | mDNS Detection (Remot... | Medium | 40 |
| 10061 | Echo Service Detection | Medium | 33 |
| 10198 | Quote of the Day (QOTD... | Medium | 30 |

Last Updated: 4 hours ago

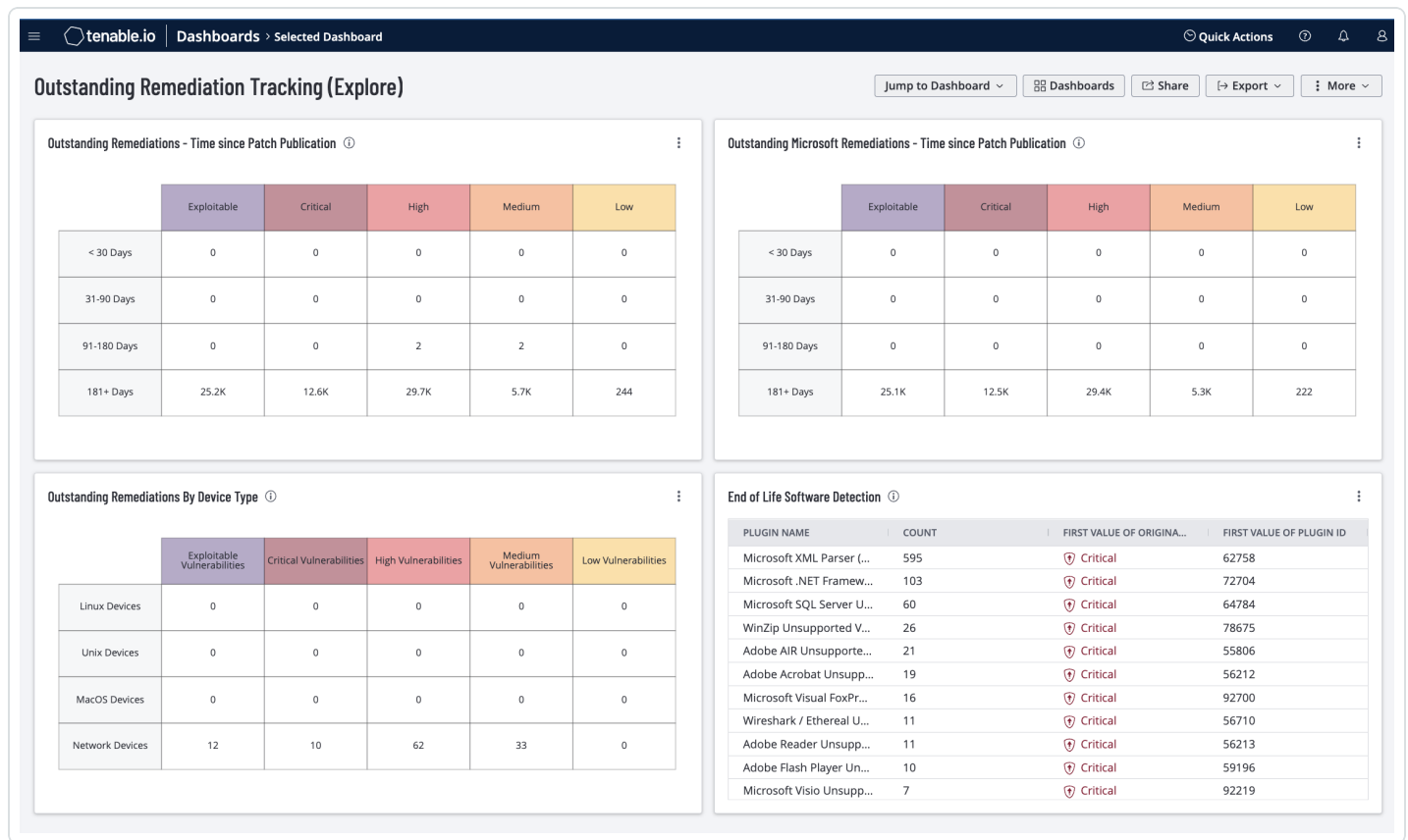
Unsupported Product Summary - Applications by Type and Percentage

| General | 0% |
|-------------------------|-----|
| Windows | 38% |
| *nix | 0% |
| Databases | 25% |
| Webservers | 1% |
| Other Operating Systems | 0% |
| Other Families | 0% |

Last Updated: 9 minutes ago

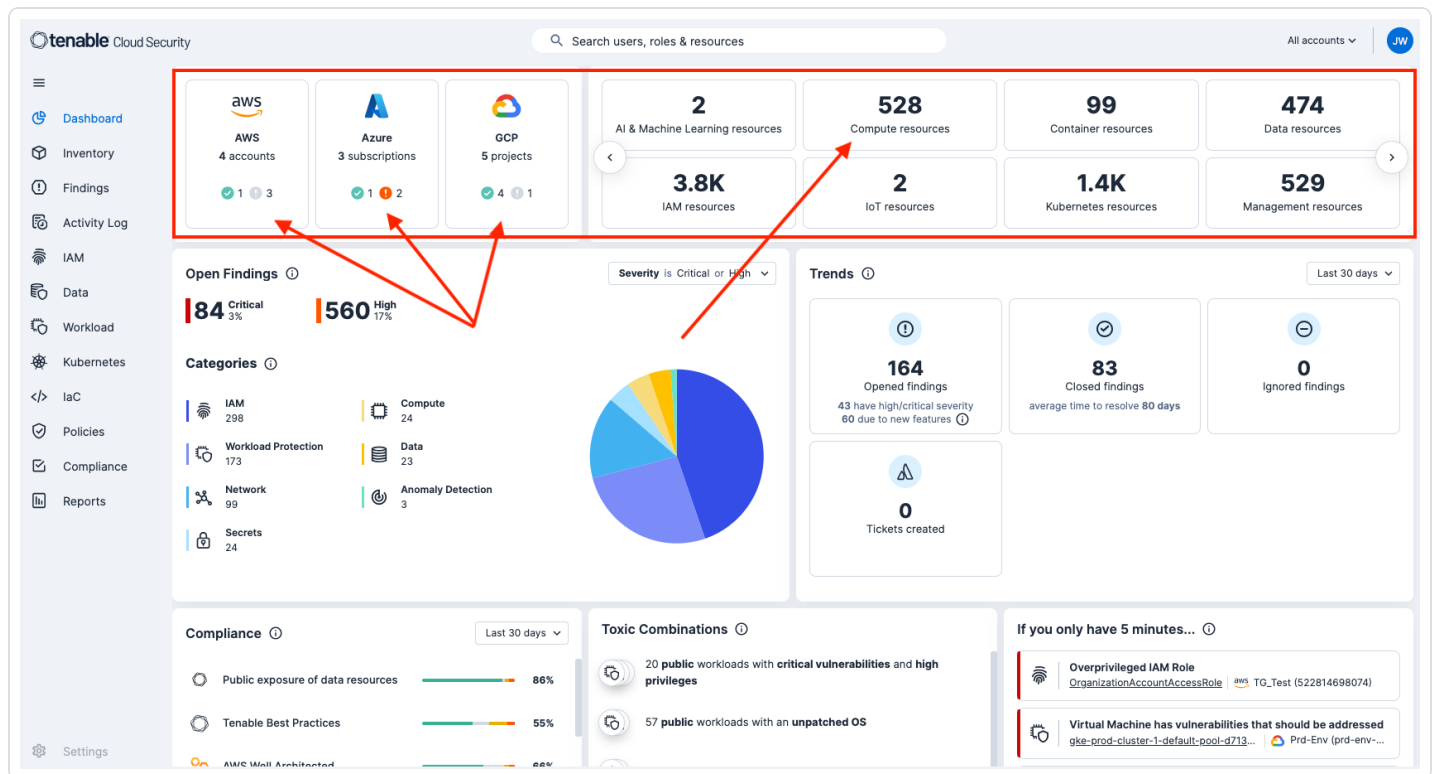
For more information on Software Inventory see the Establishing a Software Inventory Cyber Exposure Study [here](#).

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.

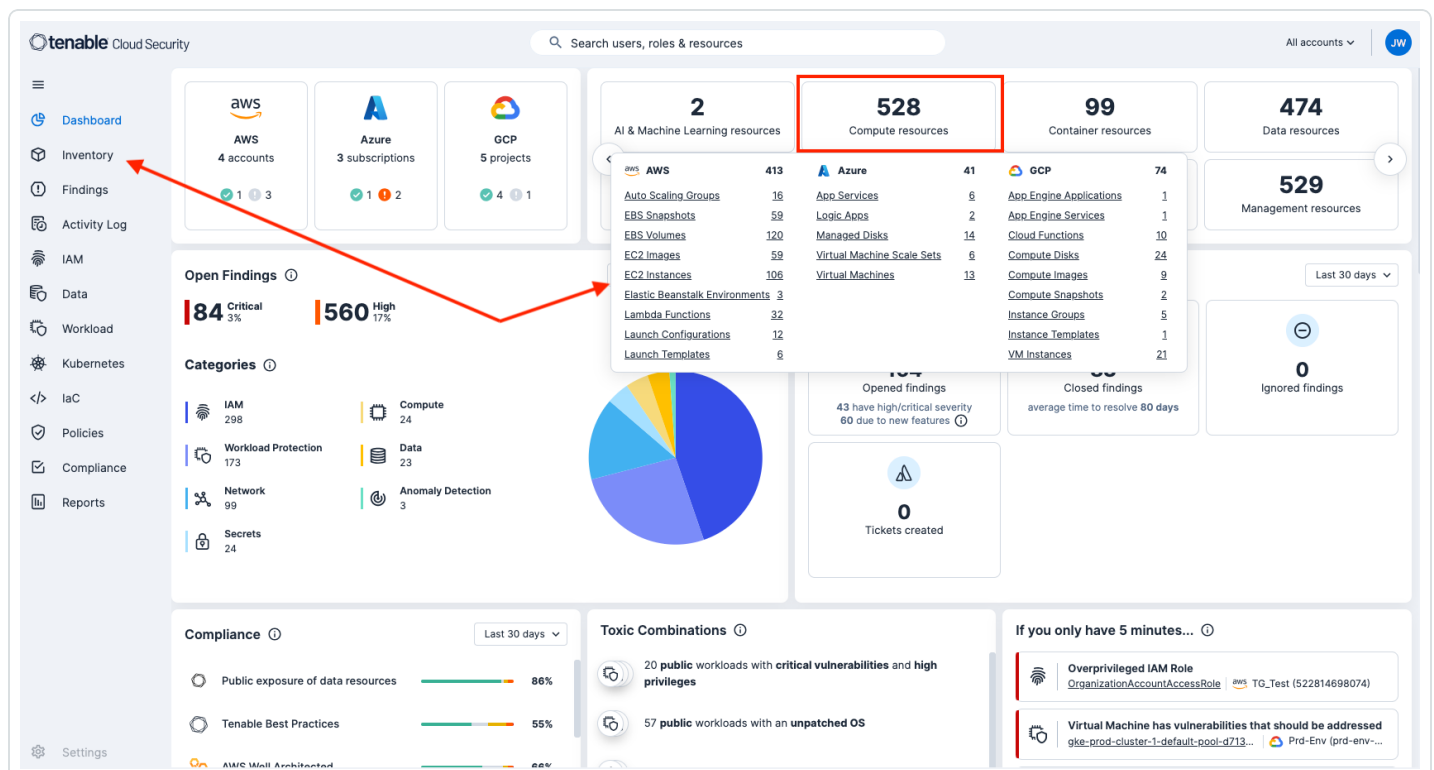


Tenable Cloud Security not only automates threat detection and remediation to eliminate noise, but also identifies cloud services and prioritises risk by continuously monitoring the cloud environment. Tenable analyses cloud provider logs to reveal the identity behind each activity and affected accounts,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