Tenable Cyber Exposure Study - The Essential Eight Strategies

Last Revised: February 06, 2025

Table of Contents

Executive Overview

The Australian Cyber Security Centre (ACSC) under the Australian Signals Directorate (ASD) provides helpful information when relating to cybersecurity within the Australian landscape. The ASD provides this guidance to address targeted cybersecurity intrusion. This guidance is called the Strategies to Mitigate Cyber Security Incidents. These strategies are given a Relative Security Effectiveness Rating: Essential, Excellent, Very Good, Good, or Limited. The Essential Eight describes only a minimum set of preventative cyber security measures and therefore organisations should use the Essential Eight in conjunction with the ASD's Information Security Manual (ISM) controls. This Cyber Exposure study will focus on what the ASD calls the Essential Eight and their associated ISM controls. The ISM is a cybersecurity framework that all organisations should apply to ensure the confidentiality, integrity, and availability of their information technology and operational technology systems.

The Essential Eight

The Essential Eight are considered by the ACSC to be the most effective security risk mitigation strategies within the Strategies to Mitigate Cyber Security Incidents. While the Essential Eight are focused on Microsoft Windows networks, the strategies can be equally applied to Linux, Cloud and other networks or infrastructure that supports them.

The Essential Eight is comprised of:

1. Patch Applications
2. Patch Operating Systems
3. Multi-factor Authentication
4. Restrict Administrative Privileges
5. Application Control
6. Restrict Microsoft Office Macros
7. User Application Hardening
8. Regular Backups

The Essential Eight strategies are designed to be self-assessed and/or externally assessed against a maturity model (E8MM). The model consists of four maturity levels, Maturity Level 0 to Maturity Level 3, that are clearly articulated for each of the Essential Eight Strategies. As you progress through the Maturity Levels (Excluding Maturity Level 0) the strategies adjust to cover increasing levels of adversary threats.

- Maturity Level 0 signifies when there are overall flaws within the organisation's cyber security posture.
- Maturity Level One describes an instance where a threat actor utilises publicly available exploits or vulnerabilities to gain access to a system. In Maturity Level One, the target tends to also be less selective and the threat actor may just target any system or user that is vulnerable.
- Maturity Level Two further increases the level of effort as well as more specific targeting. With Maturity Level Two, a Threat Actor will invest more time and effort in a specific target; the threat actor may employ more sophisticated tradecraft to bypass security measures. Maturity Level Two also acts as the baseline for what organisations should strive for.
- Maturity Level Three describes instances when the Threat Actor will employ lesser known tools and techniques when attempting to breach security measures. Within Maturity Level Three the threat actor will target specific users and attempt to bypass Multi-factor authentication by stealing tokens values to impersonate the user. Once the user is compromised the threat actor will attempt to pivot to other parts of the network and actively try to cover their tracks to avoid detection.

When trying to establish an efficient Cyber Security posture an organisation may have several goals that the ACSC suggests; Reducing the impact of malware by preventing the delivery and execution of malware; Limiting the extent of cyber security incidents; and time to recovery and other disaster recovery planning. The ACSC suggests applying the Essential Eight strategies in this specific order.

Reducing the impact of malware by preventing delivery and execution of malware involves ensuring patches go out in a timely manner. The targets of these patches should be both operating systems and applications. Additional to patching operating systems and applications, the security team is also able to implement Application Control and Hardening strategies. Application control and hardening strategies include having a blacklist of applications that should not be installed or used on any asset. The Essential Eight strategies related to reducing the impact of malware by preventing delivery and execution of malware are:

- Application Control
- Patch Applications
- Restrict Microsoft Office Macro Settings
- User Application Hardening

After reducing the impact of malware a security team is going to want to implement strategies that will limit security incidents. Limiting security incidents can involve ensuring the organisation practises principles like Least Privilege, ensuring Multi-Factor Authentication (MFA) is enabled, and operating systems are patched. Using Tenable's Asset Criticality Rating (ACR) in tandem with Tenable's Vulnerability Priority Rating (VPR) enables an organisation to effectively prioritise which assets require attention first. The Essential Strategies related to limiting security incidents are:

- Restrict Administrative Privileges
- Patch Operating Systems
- Multi-Factor Authentication

Having a sense of Time to recovery and other disaster recovery planning involves being able to recover data and establish good system availability. Having an adequate system in place where assets' data is backed up is imperative to ensure not only data recovery is possible but that downtime is minimised. The Essential Strategy related to Recover Data and System Availability is:

- Regular Backups

There are two additional Mitigation goals that the ACSC suggests, Mitigation Strategy specific to preventing malicious insiders and Mitigation Strategy to Detect Cyber Security Incidents and Respond, but they do not include essential strategies and this cyber exposure study will only focus on the Essential Eight.

Tenable and the Essential Eight

Tenable provides risk measurement and communication tools that are suited to consistently measuring an organisation's maturity and risk posture. While Tenable can assist with measuring risk in many of the Essential Eight strategies, there are two strategies that Tenable cannot directly assist an organisation's Essential Eight maturity level; Regular backups and Restrict Microsoft Office Macros. Tenable does conduct a check-and-verify process across the Essential Eight controls, but does not implement, modify, or remove any existing control artifacts. Tenable's role is limited to reporting on the status of these artifacts in relation to the Essential Eight controls. Later in this cyber exposure study, we will explore how Tenable Host Audit scanning can be utilised to assist in verifying and assessing certain aspects of Regular Backups and the Restriction of Microsoft Office Macros, as part of the Essential Eight Strategies.

The Tenable One Platform incorporates a comprehensive suite of sensors designed to facilitate efficient vulnerability scanning, regardless of network complexity or infrastructure type. By leveraging these capabilities, organizations can effectively discover and assess their attack surface, gaining a clearer and more complete understanding of potential exposure points. Combined with Exposure Response, Tenable enables organizations to not only scan for vulnerabilities but also prioritize remediation efforts based on contextual risk. Tenable provides thorough vulnerability scanning and exposure insights for:

- On-Prem and remote IT (Tenable Security Center and Tenable Vulnerability Management)
- Internet Facing assets (Tenable Attack Surface Management)
- Web Applications and APIs (Web App Scanning)
- Cloud Resources (Cloud Security)
- Industrial Infrastructure (OT Security)
- Identity systems (Identity Exposure)

Implementing an Essential Eight mitigation strategy is likely to directly improve the security posture of an organisation. Auditing the implementation does not improve the maturity level of the mitigation, but rather, confirms the quality, consistency and expected state of that implementation.

Tenable's risk-based vulnerability management capabilities include extensive auditing capabilities. The auditing capabilities empower you to confirm the state of just about any such implementation such as:

- Essential Eight Application control (The application control agent is installed, its version, if log file exists, the application allow-list ›file exists)
- Configure Microsoft Office macro settings (GPOs are in place to control Microsoft Office functions)
- User application hardening (policies are in place as expected to control application function)
- Restrict administrative privileges (Numbers of admins, admin lists, policies for controlling access, expiry of passwords, GPOs controlling passwords, complexities and MFA)
- Multi-factor authentication (policies are in place to control authentication processes)
- Regular backups (software installed, processes running, logs being written, policy in place)

This Cyber Exposure Study will detail how an organisation can verify the implementation of the Essential Eight Strategies. With the setup of Credentialed Scanning, Agent Scanning, Compliance Policy Scans, Dashboards and Reports, this guide will detail how Tenable can assist the organisation in confirming their overall security posture.

This study provides guidance through the subjects matching the Essential Eight Strategies:

- Reducing the Impact of Malware
    - Patch Applications
    - Application Control
    - User Application Hardening
    - Restrict Microsoft Office Macros
- Limiting the Impact of Security Incidents
    - Patch Operating Systems
    - Multi-factor Authentication
    - Restrict Administrative Privileges

Tagging and Dynamic Asset Lists

Before getting started an important first step is to understand tagging (Tenable Vulnerability Management) and Dynamic Asset Lists (Security Center). By an organisation classifying assets, Tenable can assist the organisation better focus their dashboards, reports and queries. When dealing with operating systems, risk managers need to understand which assets are internet facing and which are non-internet facing. Then, when dealing with applications the risk managers need to determine if the application is an online service, a high risk application or a low risk application. The organisation can make use of Asset Tagging in Tenable Vulnerability Management or Dynamic Lists in Tenable Security Center to ensure assets data can be grouped appropriately and be better prioritised.

An asset tag (Tenable Vulnerability Management) is primarily composed of a Category:Value pair. For example, if you want to group your assets by their connection to the internet, create a new category with the value internet facing. You can then manually apply the tag to individual assets, or you can add rules to the tag that enable Tenable Vulnerability Management to apply the tag automatically to matching assets. For more information on creating a tag visit Tenable's Tagging documentation.

In all queries used in Tenable Vulnerability Management and/or Tenable Security Center, using tags or asset lists will enable the user to focus their scan data and results to give them more relevance to the Essential Eight. The ACSC wants organizations to differentiate between Internet-facing and non internet-facing assets to determine different Service Level Agreement (SLA) timelines. For example, internet facing applications should be patched within 48 hours as opposed to non internet-facing applications should be patched within two weeks. These SLA differences are useful to identify and group together the detected assets based on whether they're internet facing or not. To identify internet-facing assets in Tenable Vulnerability Management and/or Tenable Security Center, you can create tags that focus on key characteristics of these assets. These tags can be applied manually or automatically using filtering rules, such as identifying assets with public IP ranges, open ports (e.g., 80 or 443), externally accessible vulnerabilities, or cloud metadata indicating public accessibility. Grouping assets by their roles, such as application servers or customer-facing portals, can further enhance visibility. Setting up dynamic tagging ensures that these tags are applied automatically to new assets meeting the criteria, making monitoring and managing internet-facing systems effectively easier. One filter that can also be considered when creating rule based asset tags is "Public." The Public filter specifies whether the asset is available on a public network. A public asset is within the public IP space and identified by the `is_public` attribute in the Tenable

Vulnerability Management query namespace. An exhaustive list of possible Asset filters can be found here.

Host Audit Scanning

Host audit scanning within Tenable Vulnerability Management, plays a vital role in supporting the implementation and enforcement of the Essential Eight. This scanning capability provides a detailed assessment of system configurations, software versions, and vulnerabilities across hosts, helping organizations identify and remediate gaps that could undermine the security objectives of the Essential Eight. By leveraging Tenable's robust scanning capabilities, organizations can automate compliance checks, detect misconfigurations, and prioritize remediation efforts based on risk.

The ability to scan and audit hosts for compliance with Essential Eight controls ensures a proactive security posture. Host audit scanning is particularly valuable in identifying unpatched vulnerabilities, misaligned configurations, and unmanaged assets, all of which can be exploited in targeted cyberattacks. Moreover, Tenable Vulnerability Management's reporting and dashboard features enable security teams to track their progress toward achieving full compliance with the Essential Eight framework. This capability is further enhanced by understanding the Key Audit File Data Fields, which provide the foundational structure for evaluating system compliance and identifying critical vulnerabilities during host audits.

Key Audit Data Fields

The audit file is an XML like file, which consists of several configuration checks. When the Tenable Research team examines the various benchmarks, for example Center for Internet Security (CIS), each CIS benchmark is broken into profiles (Level 1 and Level 2) and each profile is an item. The Tenable Audit files convert the "items" into XML like elements `<item>` or `<custom_item>` which then becomes an Audit Name in Tenable Vulnerability Management or Tenable Security Center. From this point forward, `<item>` or `<custom_item>` in audit files are referred to as an **Audit Name**, and the presence of an Audit Name on an asset is called a finding.

More information on audit files can be found here:

- Audits
- Nessus Compliance Checks Reference

```
    <custom_item>
      system      : "Linux"
      type        : FILE_CONTENT_CHECK
      description : "5.3.3 Ensure password reuse is limited - system-auth"
      info        : "The /etc/security/opasswd ---TEXT OMITTED---"
      reference   : "800-171|3.5.2,800-53|IA-5(1),800-53r5|IA-5(1),CSCv7|4.4,CSF|PR.AC-1,GDPR|
32.1.b,HIPAA|164.306(a)(1),HIPAA|164.312(a)(2)(i),HIPAA|164.312(d),ITSG-33|IA-5(1),LEVEL|
1S,NESA|T5.2.3,QCSC-v1|5.2.2,QCSC-v1|13.2,SWIFT-CSCv1|4.1"
      see_also    : "https://workbench.cisecurity.org/files/2449"
      file        : "/etc/pam.d/system-auth"
      regex       : "^[\\s]*password[\\s]+(sufficient[\\s]+pam_unix\\.so|required[\\s]
+pam_pwhistory\\.so).*remember"
      expect      : "remember[\\s]*=[\\s]*([5-9]|[1-9][0-9]+)"
    </custom_item>
```

The description line becomes the Audit Name, the other key field is the **reference** line, also known as the Cross Reference or XREF. The XREF is a mapping of this respective check to several compliance standards and benchmarks. Customers are able to search using the XREF in different methods based on the product, see below:

Product	Search Term	Example
t.vm	Your Tenable Vulnerability Management linking key.	Compliance Framework= 800*53 Compliance Family= ACCESS CONTROL
t.sc	800-53 ACCESS CONTROL	Cross Reference = 800-53|AC*

To help customers verify the audit checks authority in the benchmark, the **see_also** field provides the location a customer can download the benchmark from the provider. This benchmark is used to consolidate audit checks by the correct benchmark and version.

https://workbench.cisecurity.org/files/2449

When an asset is scanned using an audit file, and a check becomes a finding, the finding is returned in one of the following states: PASSED, FAILED, ERROR, WARNING. The state is converted into a severity level for use with Tenable Security Center, and for Tenable Vulnerability Management the state is retained. The colour coding for the state coincides with the colour for the severity levels as displayed in the following table.

State	Tenable Security Center Severity	Tenable Vulnerability	Description

		Management State	
PASSED	Informational	Passed	The audit check was within the tested parameters.
FAILED	High	Failed	The audit check was not within the tested parameters.
ERROR	Medium	Error	The audit check is not supported on the asset.
WARNING	Medium	Warning	The audit check was successful, however compliance cannot be determined and needs to be reviewed manually.

Data Fields Explained

Now that we understand the key fields used for analysis there are a few other fields used to enhance search behaviours and are commonly used in the compliance dashboards and reports. In this section a detailed review of all the fields and how they work together are provided.

- Tenable Vulnerability Management
- Tenable Security Center (6.3)

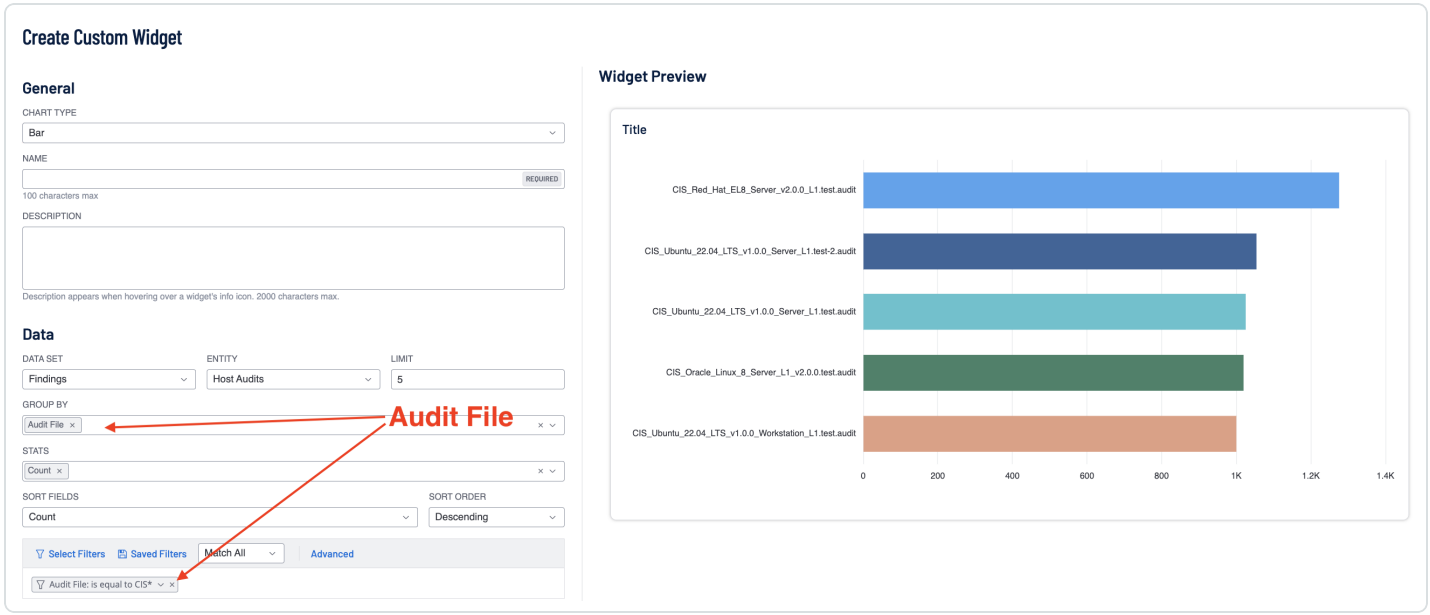
Audit File

The name of the Audit file the scanner used to perform the audit. Audit files are XML-based text files that contain the specific configuration, file permission, and access control tests to be performed. The audit file can be customised and should be changed if the customer edits the audit file. For example, if the audit file provided by Tenable is named “CIS_AlmaLinux_OS_8_Server_v3.0.0_L1.audit” and the customer edits the parameters of the audit file, then the customer might change the name to be “ACME-Mar24-CIS_AlmaLinux_OS_8_Server_v3.0.0_L1.audit." This name suggests that the ACME corp added this audit file in March of 2024. In doing this, analysts are able to easily find the audit files edited by the organisation and apply the filters correctly.

While changing the name of an audit file is not required, here is helpful information to consider if choosing to do so. Note that the names of the audit file are not to be confused with benchmark. Tenable names the audit files to coincide with the benchmark, but the name is just a name. When choosing the name for the audit files, consider the operating system the audit file is intended for, the benchmark (including the version) used to create the audit file, and the date the audit file is added. Note that audit files that are custom, meaning imported by the customer, are not updated and therefore need to be maintained.

Tenable Vulnerability Management:

- Using the audit file name is supported in both the group-by options in the widget and in the filters.
- In the bar chart example, the bars represent the count of findings by the respective audit file. Other factors, such as state, date, etc., are not included.



Tenable Security Center:

- Analysis using an Audit Files is only available in a filter.
- In the bar chart example, the bars represent the count of findings by the respective audit file. Other factors for example state, date, or etc. are not included.
- Dashboard component documentation is found here.

Audit Name

The name Tenable assigned to the audit, as previously mentioned, is the value in the **description** field in the audit file. In some cases, the compliance control may be listed as the prefix within the name. This is often combined with a nomenclature from the benchmark. In CIS benchmark, the name is prefixed with a number and DISA uses the STIG-ID. Just note that regardless of the benchmark used to create the audit file, review the descriptions that are provided in the audit file for a list of possible Audit Names.

Using grep or similar tool, the user can search audit files and return all the descriptions which are converted into the Audit Name: `grep -E '\s+description(\s):' *.audit`

- CIS Example: "**4.5.3.3** Ensure default user umask is configured"
- DISA Example : "**WG050 W22** - The web server service password(s) must be entrusted to the SA or Web Manager."

Tenable Vulnerability Management:

- The Audit Name is available using group by and filtering similar to the audit file above.
- Use the “*” or wild card and the end of the string to search for all the Audit Names that match the pre-fixed pattern. All the patterns below find Audit Names with the relative pattern. Note, when using the * as the first character in the search you will match any pattern. The samples below match each of the examples shown above.

Pattern	Result
4.5.*	Strings that begin with 4 <period> 5 <period> and followed by any character.
WG*	Strings that begin with WG (case insensitive).

W22	String that begins with any character but contain W22 within the string, followed by any other characters.
W*W22*	Strings that begin with “W” and contain W22.

Tenable Security Center:

- Audit Names become the plugin name. When an audit file is imported and used in a scan or filter, Tenable Security Center creates plugins for each of the `<items>` or `<custom_items>` in the audit file. The plugins have an ID > 1,000,000 and the plugin ID will be unique to the installation. Also note, if an audit file is updated and re-added, new plugins are created, this is another reason why it's often a good idea to name the audit file during import.
- The plugin name field supports regex patterns allowing for very complex and flexible pattern matching, here are some examples:

Pattern	Result
^4\.5.*	Strings that begin with 4 <period> 5 <period> and followed by any character.
^[Ww][Gg].*	Strings that begin with WG (case sensitive, but account for both upper and lower case).
^.*[Ww]22.*	String that begin with any character but contain W22 within the string, followed by any other characters.
^[Ww].*[Ww]22.*	Strings that begin with “W” and contain W22.

Benchmark

Benchmarks are published best practices released from source authorities, such as Center for Internet Security (CIS), United States Defense Information Systems Agency (DISA), and Microsoft. This filter provides a list of the supported benchmarks and the version of the benchmark. Tenable used the URL of the Benchmark to distinguish to which benchmark the audit file is mapped. The URL is stored in the SEE_ALSO element found in the audit file.

- CIS: https://workbench.cisecurity.org/benchmarks/12695
- DISA: https://iasecontent.disa.mil/stigs/zip/U_Apache_2-2_WIN_V1R13_STIG.zip

- Microsoft: https://blogs.technet.microsoft.com/secguide/2018/04/30/security-baseline-for-windows-10-april-2018-update-v1803-final

CIS Benchmarks are linked directly with See Also URL, in this example CIS Windows Server 2016 version 2.0.0 can be accessed via https://workbench.cisecurity.org/benchmarks/12695. Each of the audit files that support the benchmark are focused on the different role or functions of the asset. In this example the DC is the domain controller, and MS is a member server. The L1 and L2 describing the level 1 or level 2 checks depicted in the benchmark. To obtain full coverage with a benchmark all audit files from the specific role needs to be added to the targeted scan. Be careful not to scan a domain controller with a member server audit file, and there are different checks and some coverage could be mis-represented. This benchmark is covered by six audit files:

- CIS_Microsoft_Windows_Server_2016_Benchmark_v2.0.0_DC_NG.audit
- CIS_Microsoft_Windows_Server_2016_Benchmark_v2.0.0_L1_DC.audit
- CIS_Microsoft_Windows_Server_2016_Benchmark_v2.0.0_L1_MS.audit
- CIS_Microsoft_Windows_Server_2016_Benchmark_v2.0.0_L2_DC.audit
- CIS_Microsoft_Windows_Server_2016_Benchmark_v2.0.0_L2_MS.audit
- CIS_Microsoft_Windows_Server_2016_Benchmark_v2.0.0_MS_NG.audit

For a DISA STIG, there can be situations where there are more that one version of an Audit file that makes the STIG. For example, DISA STIG Apache Server 2.4 Unix in the URL https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_Apache_Server_2-4_Unix_Y23M07_STIG.zip, contains several version files in version 2.4.0 and 2.6.0. Listed below are the audit files that comprise the STIG, much like the aforementioned CIS benchmark there can be different roles and the appropriate audit files should be deployed to targeted assets.

- DISA_STIG_Apache_Server-2.4_Unix_v2r6.audit
- DISA_STIG_Apache_Server-2.4_Unix_v2r6_Middleware.audit
- DISA_STIG_Apache_Site-2.4_Unix_v2r4.audit
- DISA_STIG_Apache_Site-2.4_Unix_v2r4_Middleware.audit"

After scanning with appropriate audit files here are examples on how to find the relevant data.

Tenable Vulnerability Management:

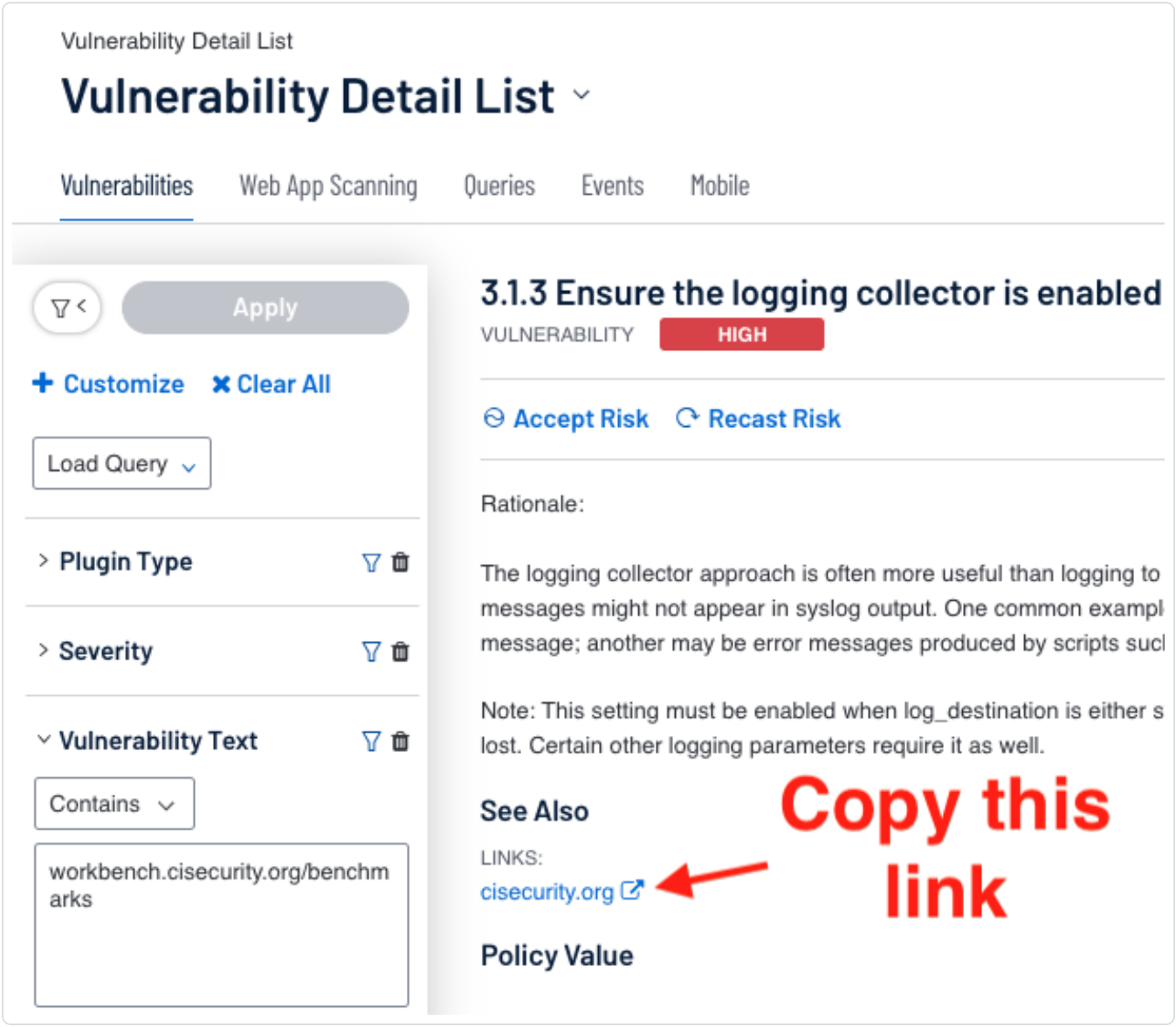
- In this field the benchmark name and version are combined into one string. Using regular search terms, the search can be limited to only the desired content.

Pattern	Result
CIS *	Strings that begin with CIS<space> followed by any other character.
CIS P*9*	Strings that begin with CIS<space>P followed by any other character but must contain a 9 in the string. (Ex: CIS Palo Alto Firewall 9 v1.1.0.)
v1.0.0	Strings that begin with any character but contain v1.0.0 within the string, followed by any other characters.

- For benchmarks that are no longer supported by Tenable, the “Deprecated <prefix> Benchmark” is available
    - Example: Deprecated CIS Benchmark
- DISA_STIG_Apache_Site-2.4_Unix_v2r4.audit
    - CIS, DISA, MSCT, NetApp, TNS
- Custom audit files are also supported however the benchmark name will be “Custom”

Tenable Security Center:

- For notes on how to search for specific elements in Security Center, review this section Tenable Security Center Compliance Elements.
- To locate the benchmark using the Vulnerability text for contains “cisecurity” or other relevant string, and then copy the link shown under the **See Also**, as shown below.



- When the “cisecurity.org” link is copied, this would be the string that is collected.
    - https://workbench.cisecurity.org/benchmarks/12695
- The Vulnerability Test filter example: <cm:compliance-see-also>https://workbench.cisecurity.org/benchmarks/12695</cm:compliance-see-also>
    - https://workbench.cisecurity.org/benchmarks/12695
- Add the string with `<cm:compliance-see-also>URL-HERE</cm:compliance-see-also>` to the Vulnerability Text field.

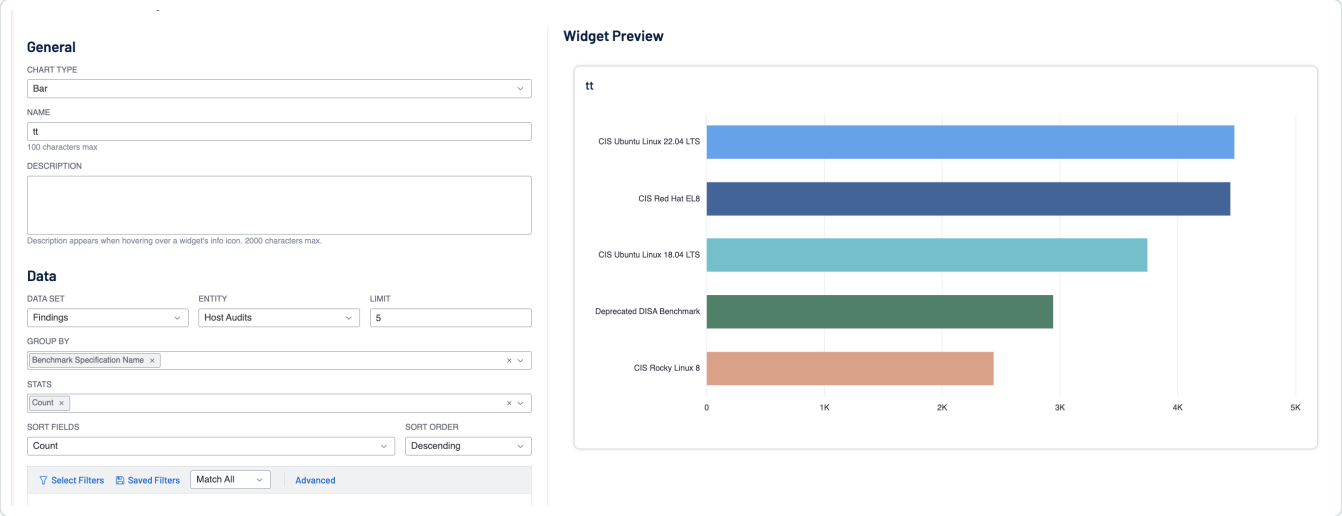
Benchmark Specification Name

The benchmark name is the same as previously described but does not contain the version. Using only the benchmark name in the search merges the data collected using all versions of the respective benchmark.

After scanning with appropriate audit files here are examples on how to find the relevant data.

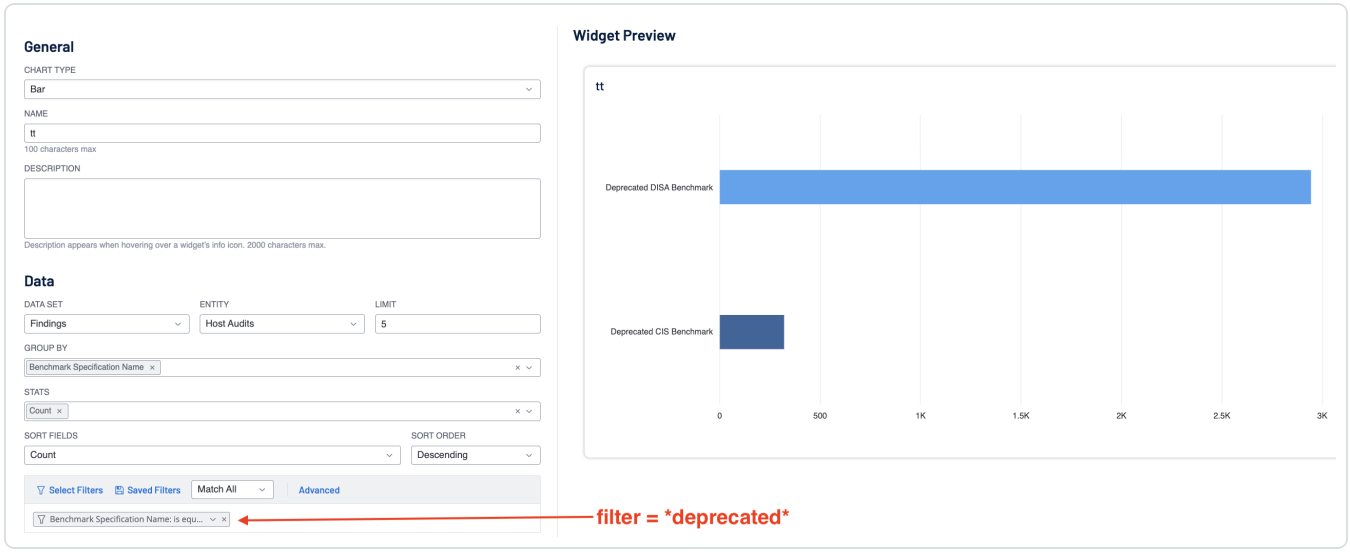
Tenable Vulnerability Management:

- Tenable Vulnerability management supports widgets using a “Group By” using the Benchmark Name, as shown below, the chart quickly shows the benchmarks in use, allowing for more filtering options.



- Note that when a benchmark becomes deprecated and is no longer supported by the benchmark name is changed to Depreciated <TYPE> Tenable. By adding the filter Benchmark Specification Name = “*deprecated*”, you can see the use check found with deprecated audit

files.



Tenable Security Center:

- Use the same approach as before with Tenable Security Center, use the Vulnerability Text field and add the Benchmark Name.
- `<cm:compliance-benchmark-name>some text here</cm:compliance-benchmark-name>`

Benchmark Version

The benchmark version should only be used with the Benchmark Specification Name filters, and the version is unique to each benchmark and provider. For example, version 2.0.0 on a CIS Benchmark could be the latest version on one benchmark and a deprecated version on another.

Tenable Vulnerability Management:

- Use a string with or without wildcards just as other text-based search patterns

Tenable Security Center:

- Use the same approach as before with Tenable Security Center, use the Vulnerability Text field and add the Benchmark Version.
- Note that if you search using a regex to combine the benchmark name and version, the regex pattern must include the match for the version to come before the name and after the name. The order of the CM elements in the Vulnerability text is not consistent, so both possible

patterns should be searched.

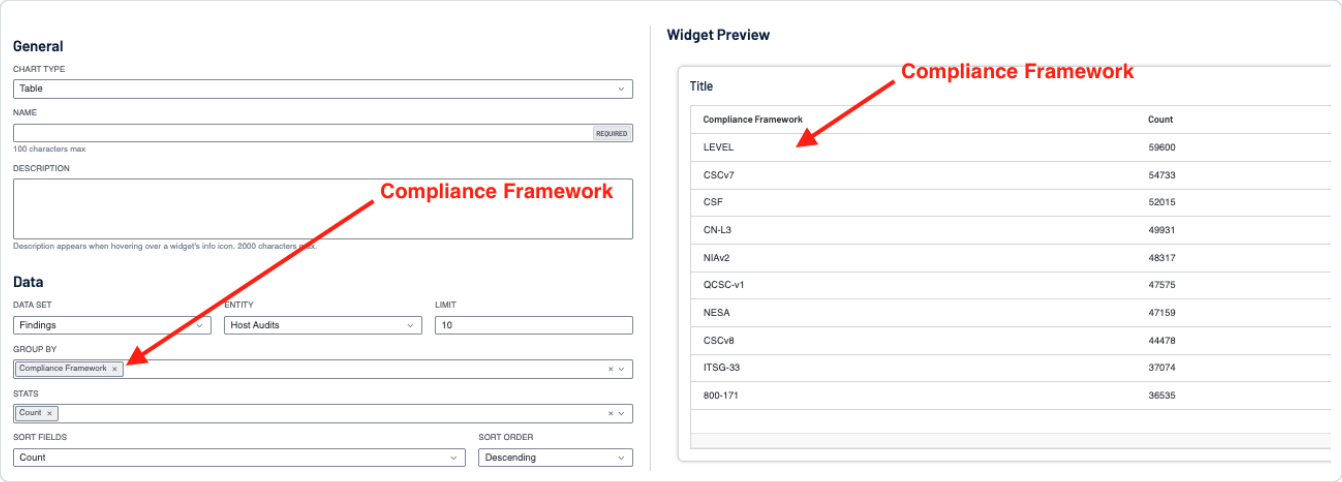
- `<cm:compliance-benchmark-version>some text here</cm:compliance-benchmark-version>`

Compliance Framework

Tenable audits configuration compliance with a variety of standards including GDPR, ISO 27000, HIPAA, NIST 800-53, PCI DSS, and so on. This filter allows searching based on the respective framework.

Tenable Vulnerability Management:

- Creating a custom widget using a table or bar chart, you can quickly see the number of compliance frameworks identified by the audit files used in the scans.
- By adding other fields as filters, such as audit file, result, or benchmark, you are able to focus on the data returned.



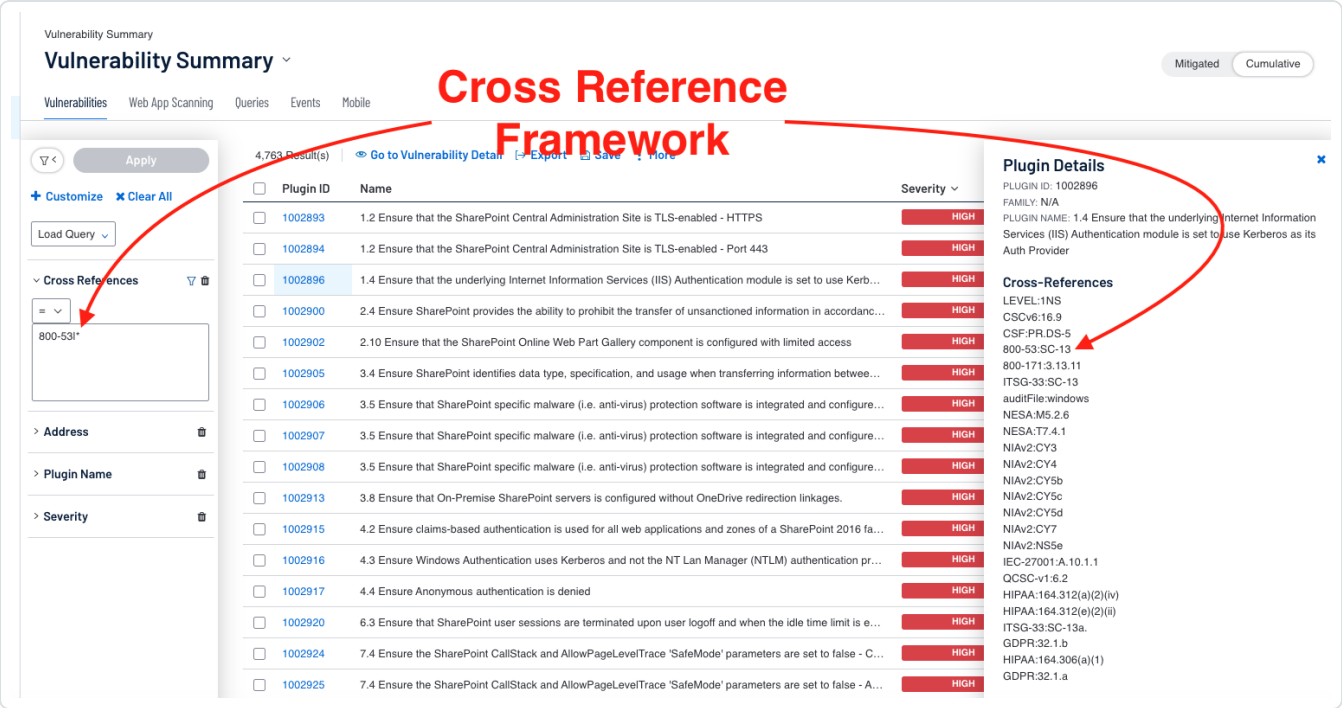
Tenable Security Center:

- The “Maintaining Data Protection Controls” Cyber Exposure Study has a good section that describes how to use the Cross Reference field.
    - /cyber-exposure-studies/data-protection/Content/VerifyingDataProtectionControls.htm
- Tenable audit checks contain a reference field that points to specific controls in a standard (ISO 27001), framework (NIST Cybersecurity Framework), or regulation (HIPAA) and is used

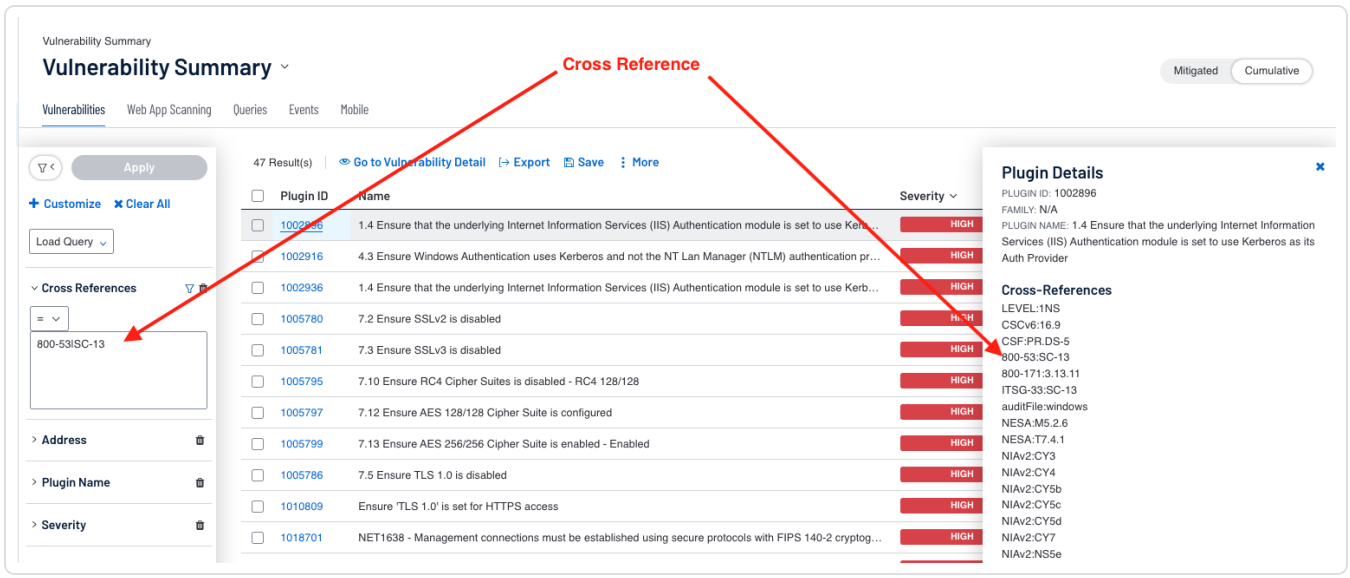
by nearly all plugins. Any external reference can be identified using the Cross References field. References can be used to search or filter in Tenable Security Center. For example, the following References define requirements for the encryption of data at rest:

  - 800-171 - 3.13.16
  - 800-53 - SC-28

- Searching with the Cross Reference Field as described in the study allows for mapping controls to the respective benchmarks. In the example below, the search pattern is 800-53|* for all audit checks for the framework NIST 800-53r4. By clicking on the Plugin ID, a window on the right is displayed showing plugin details, including the cross references.



- As mentioned in the Key Data Fields section and “Maintaining Data Protection Controls” Cyber Exposure Study, the search needs to be the full cross reference, as shown below.

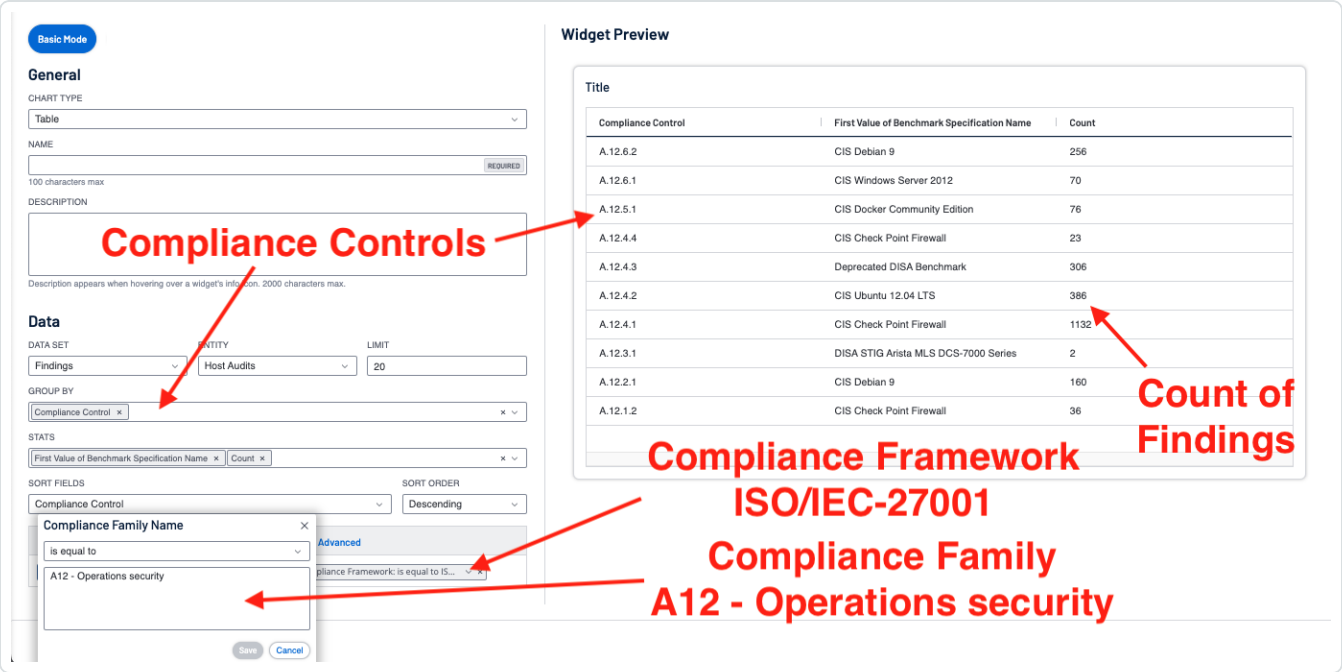


Compliance Framework

There are a series of designations within compliance frameworks that Tenable calls control. For example: ISO/IEC-27001:A.12.4.1, or CSF:DE.CM-1. This filter groups the controls into families for easier and more efficient queries. For example: A12 - Operations security or CSF:Detect. Use this filter in conjunction with the Compliance Framework filter.

Tenable Vulnerability Management:

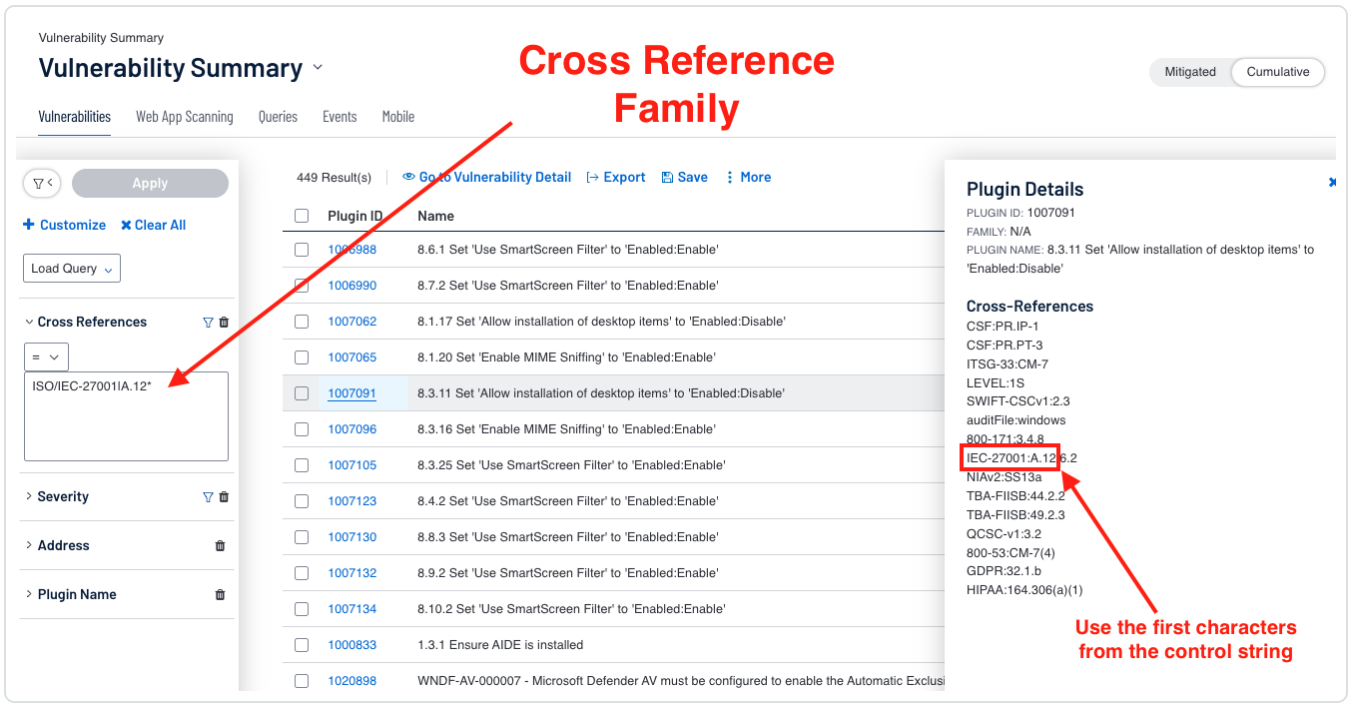
- Listed in this section is a list of the supported frameworks and the corresponding families. Much like the Compliance Control filters, the Compliance Family Name should be used with framework filters.



- This example shows the benefit of combining the various aspects of the compliance filtering, and illustrates how Tenable Vulnerability Management is able to track the compliance with several frameworks and benchmarks at the same time.

Tenable Security Center:

- As mentioned in the Key Data Fields section and “Maintaining Data Protection Controls” Cyber Exposure Study, searching for families is accomplished by using wildcard patterns in the Cross Reference search.



- In this search example we are using “ISO/IEC-27001|A.12*” to search for the family ISO/IEC-27001: A12 - Operations security.

Reducing the Impact of Malware

Within today's environment, many new vulnerabilities surface that, in most cases, have patches developed and implemented quickly. Installing application and operating systems patches is an imperative action needed to ensure these vulnerabilities don't affect the integrity or availability of the organisation. Two of the Essential Eight strategies involve ensuring that patches have been applied across operating systems and applications within the organisation. Tenable can assist an organisation in tracking patching efforts and ensure applications or operating systems that are out of date are identified.

Another Essential Strategy is Application Control. Application Control is a security approach where only an approved list of applications are used on a system. Application Control defines and can ensure only trusted applications are executed and reduces the risk of malware affecting the system. Tenable is able to detect blacklisted applications that are on an asset to assist the organisation in complying with this strategy. Although at certain maturity levels the Application Control strategy does require the use of built in solutions like Microsoft's AppLocker or Windows Defender Application Control. Some other third-party solutions are available.

This section will support the following Essential Eight Strategies:

- Patch Applications
- Application Control
- User Application Hardening
- Restrict Microsoft Office Macros

The end goal of this section is reducing the Impact of malware through the previously mentioned Essential Eight Strategies and their related ASD ISM controls. For convenience the Essential Eight to ISM Control mapping is at the end of this guide.

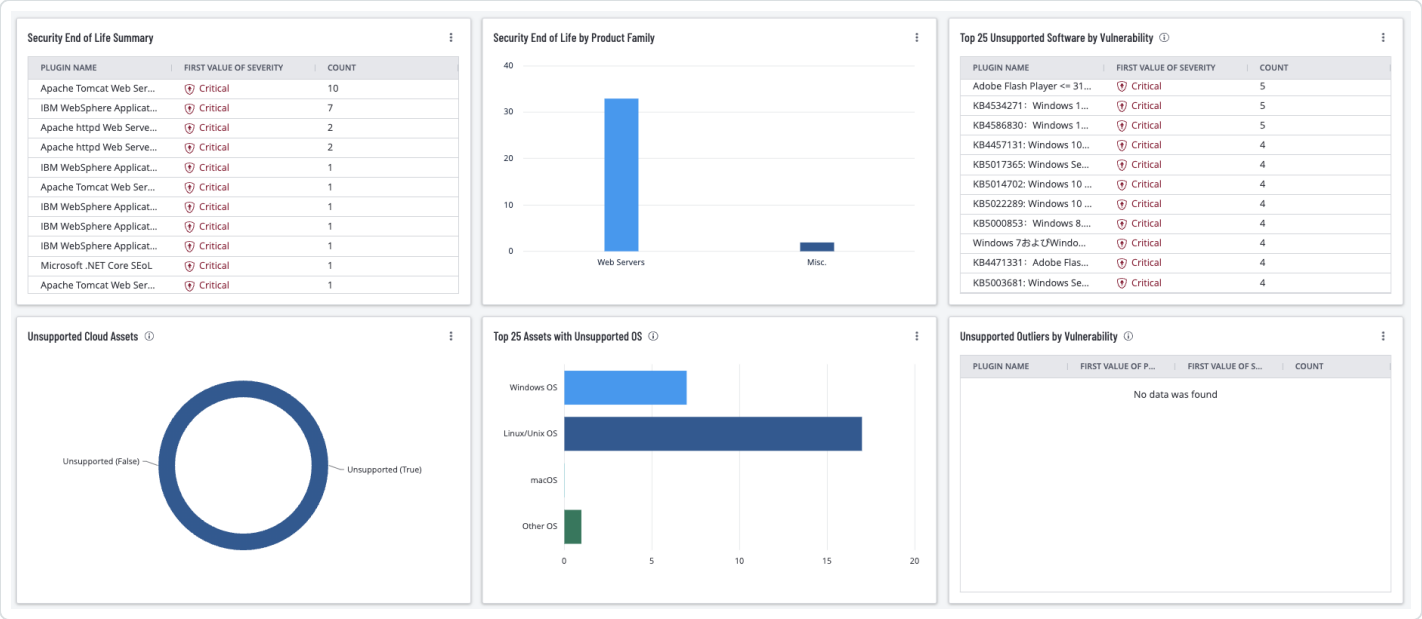
Tenable and Application Patch Management

Tenable Vulnerability Management enables organisations to continuously assess the health and security posture of the network, including identification and monitoring of unsupported software. Quick identification of unsupported applications enables risk managers to see risks associated with End of Life (EoL) software. Identifying exposures provides the operations teams direction to implement, act, and prioritise remediation efforts to mitigate cyber risk. Risk managers and

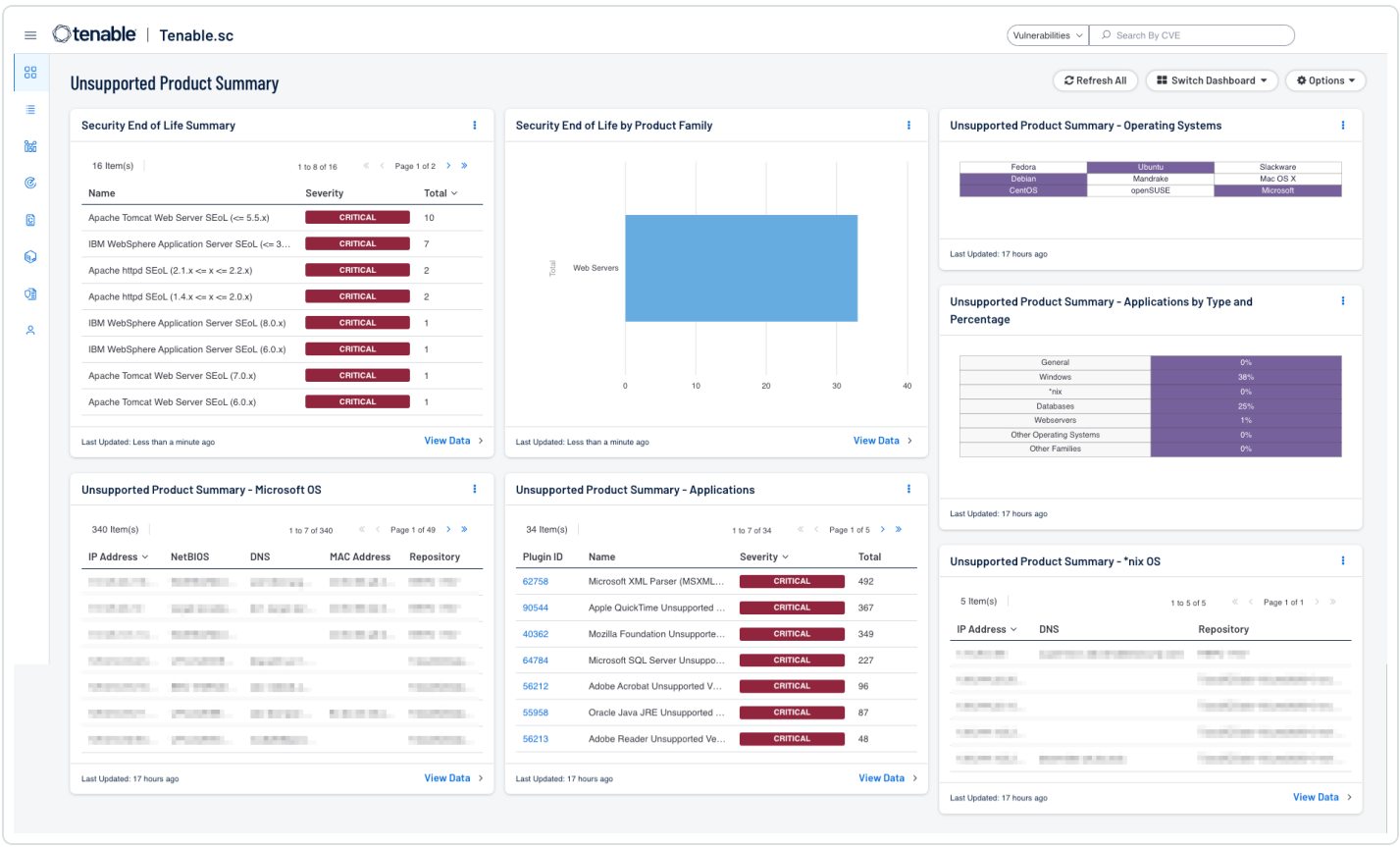
operations teams can communicate to the leadership team how upgrading unsupported applications reduces their network risk.

Tenable Vulnerability Management uses active methods to identify EOL products found in the environment by examining the Microsoft registry, common software installation locations, or using applications utilities such as YUM or APT in Linux systems. Risk managers are able to verify the operation team's activities and identify areas for risk mitigation.

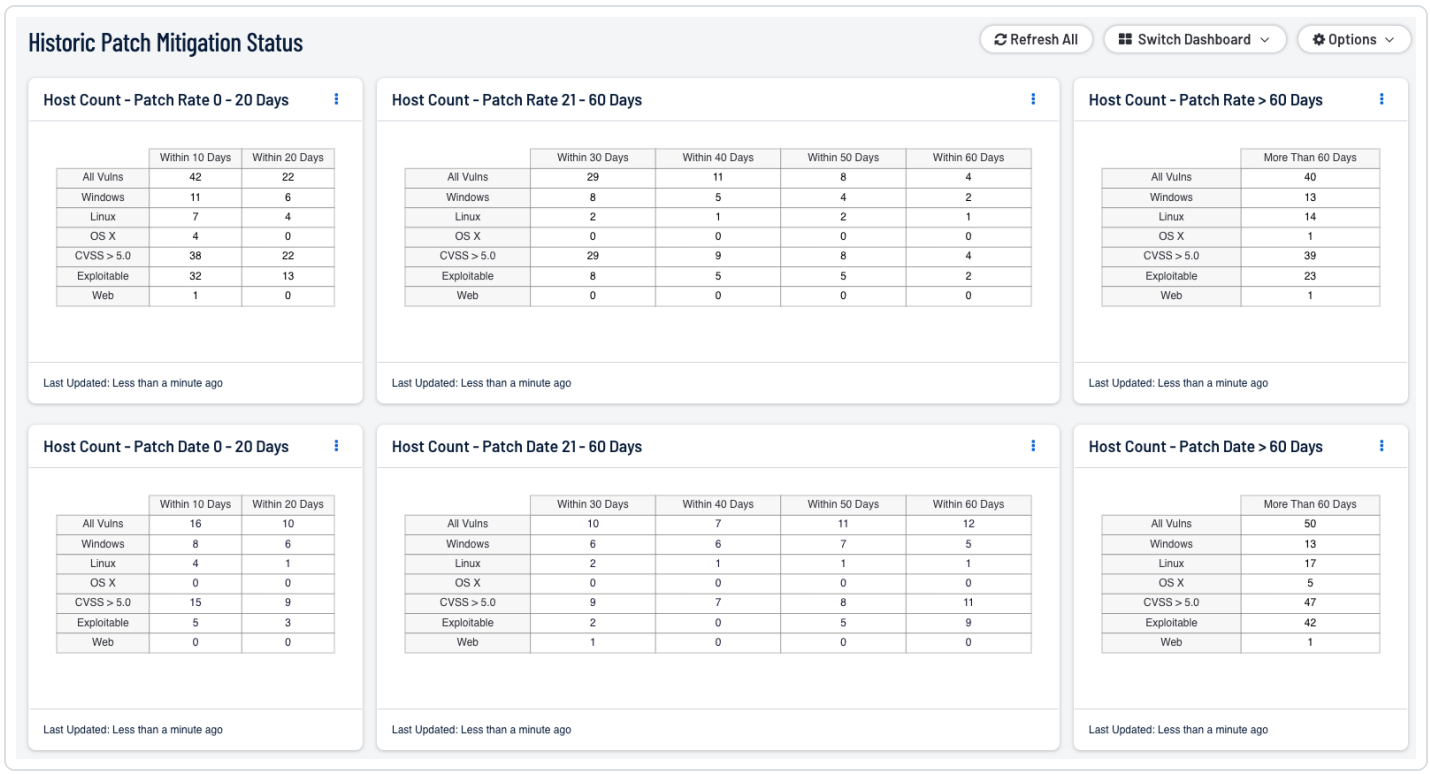
The Unsupported Software dashboard for Tenable Vulnerability Management provides the organisation with a clear and simplified method to identify EOL software and enables security managers to predict where risk will increase and develop a mitigation plan.



The Unsupported Product Summary dashboard for Tenable Security Center, shown in the following image, is similar to the Unsupported Software dashboard for Tenable Vulnerability Management and consists of seven components that report on unsupported (end-of-life) products found in the environment. Components include indicators, bar graphs, pie-charts, and tables to display, track, and report on unsupported applications.



The Historic Patch Mitigation Status dashboard for Tenable Security Center monitors vulnerability mitigation on an organisation's network in order to help security teams understand the effectiveness of their patch management efforts. Increased visibility into vulnerability mitigation can assist security teams in implementing improved patch application procedures as needed.

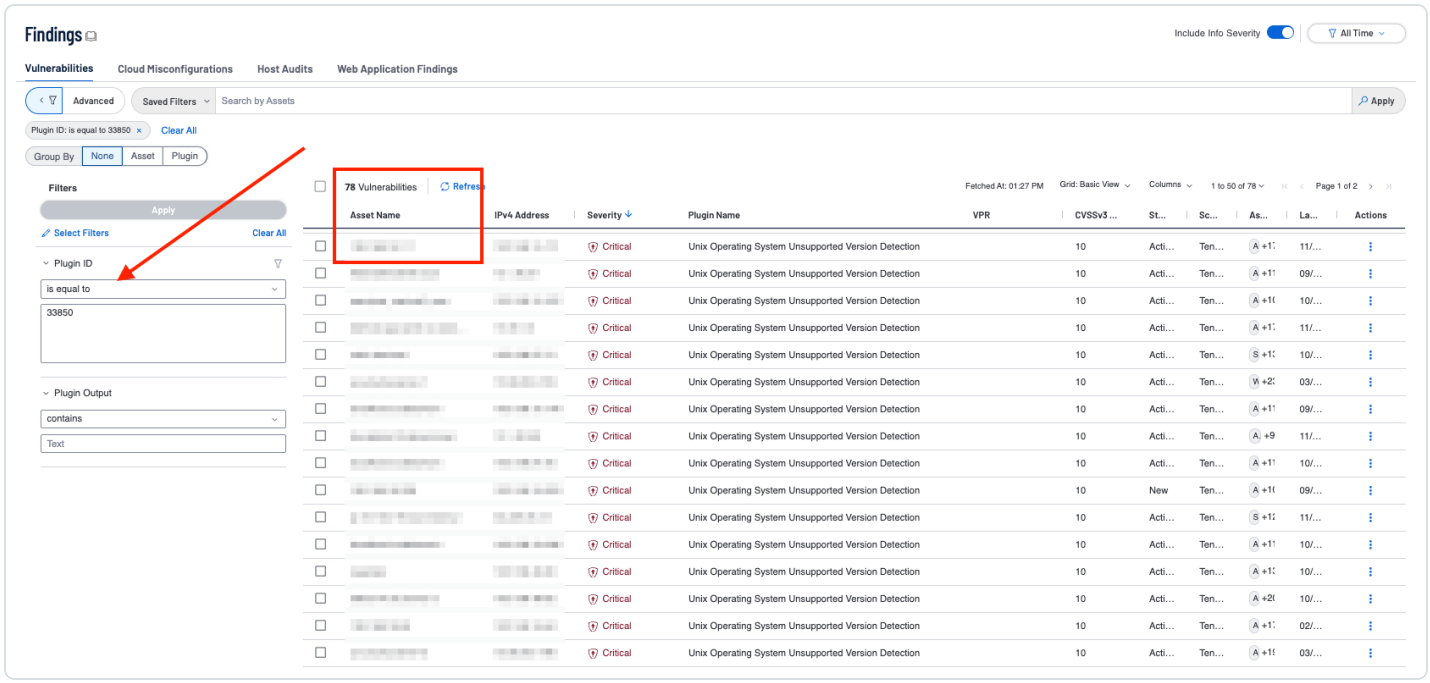


By monitoring the patterns of patch application and vulnerability mitigation, security teams can better understand the effectiveness of their efforts and make adjustments as necessary in order to effectively secure their network. ISM-1876 and ISM-1901 involve patches being applied within 48 hours and two weeks, respectively.

The components in this dashboard display data about the mitigation dates of detected vulnerabilities. Two filters are leveraged: “Days to Mitigate” and “Days Since Mitigation.” The components depicting patch rates use the “Days to Mitigate” filter to count vulnerabilities that were mitigated within the specified number of days of initial discovery. The count is based on the difference between the “First Discovered” date and the “Mitigated On” date. The components that depict patch dates use the “Days Since Mitigation” filter to count vulnerabilities that were mitigated within the specified timeframe. The count is based on the number of days between the current date and the “Mitigated On” date. Together, the components in this dashboard can assist security teams with understanding the effectiveness of their patch application and vulnerability remediation efforts.

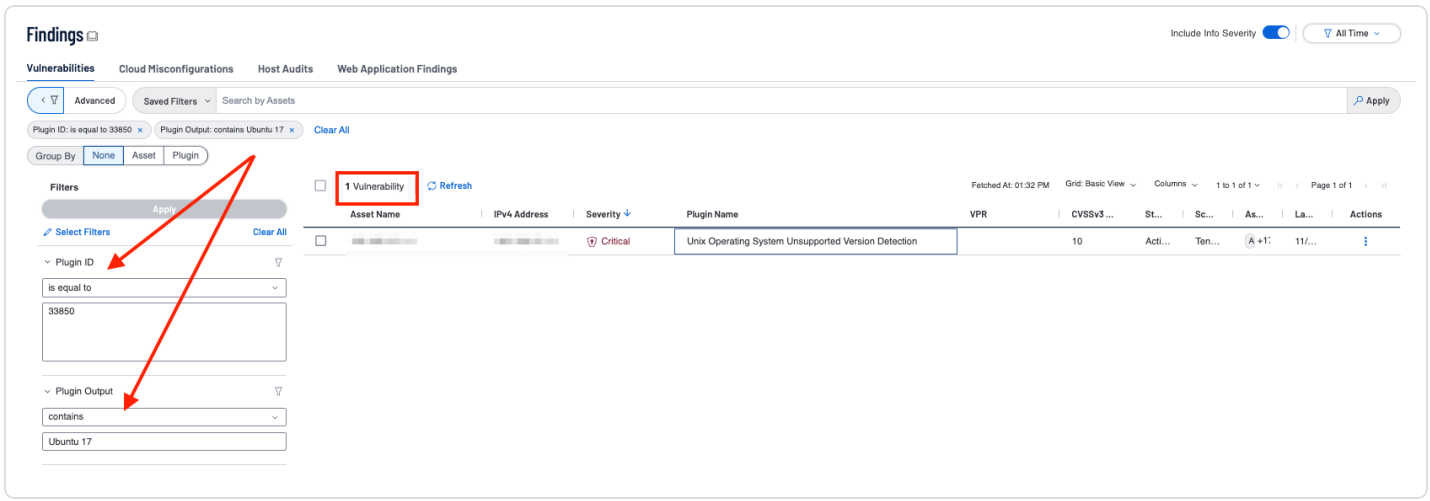
The manual vulnerability search process works like this. Specific vulnerability data can be found by searching the vulnerability text for keywords, plugin family, severity, or OS CPE strings. For example, perhaps an update was performed on all of the organisation's Ubuntu devices to version 21.04. You want to know if any unsupported devices remain in the inventory. From the **Findings** tab in Tenable Vulnerability Management (or the Analysis tab in Tenable Security Center), and using a

filter based on PluginID = 33850, Unsupported Unix Operating Systems, the number of results returned in this example is 78.

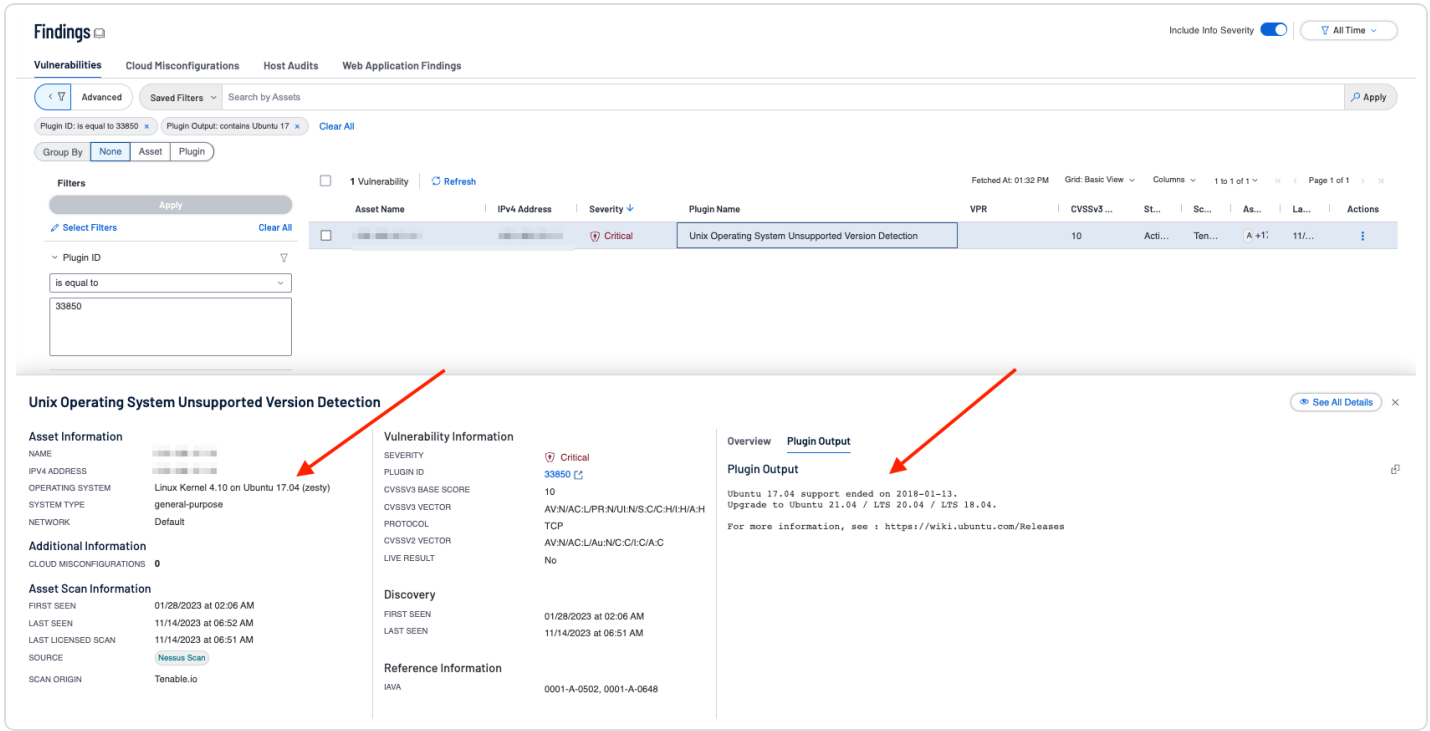


A quick review of the details of these assets reveals several different Unix-based Operating systems. Say for instance, we want to focus solely on Ubuntu, by adding a Plugin Output filter of “Ubuntu” we reduce the number of assets seen in this example to seven. The user should have ‘Plugin Output Search’ Enabled from within the Settings in Tenable Vulnerability Management.

Another quick review of the details of these assets reveals several different Ubuntu OS versions. However, some of the versions, while unsupported, are still covered by extended security maintenance. As of the time of this writing, Ubuntu version 16.04 support ended on 2021-04-30 (end of maintenance), but had extended security maintenance releases available until 2026-04-30. So if we want to focus on patching more vulnerable versions of Ubuntu, by changing the Plugin Output filter to “Ubuntu 17” we are returned with one asset.



Looking at the details of this asset we can verify no support for this version has been available since 2018, effectively rendering this asset unpatched for the last five years. In a matter of minutes, using this type of search methodology we have reduced the immediate patching requirement in this example from 78 assets to just a single asset. While the others are also a priority, this one single asset has floated to the top, and can be dealt with immediately, while a plan is developed to patch the remaining assets.



Using these queries can help an organisation confirm ISM controls similar to ISM-1690, ISM-1901, ISM-1694, ISM-1697, ISM-1902, ISM-1904. These controls involve scanning for updates and ensuring now exploitable or vulnerable assets are present.

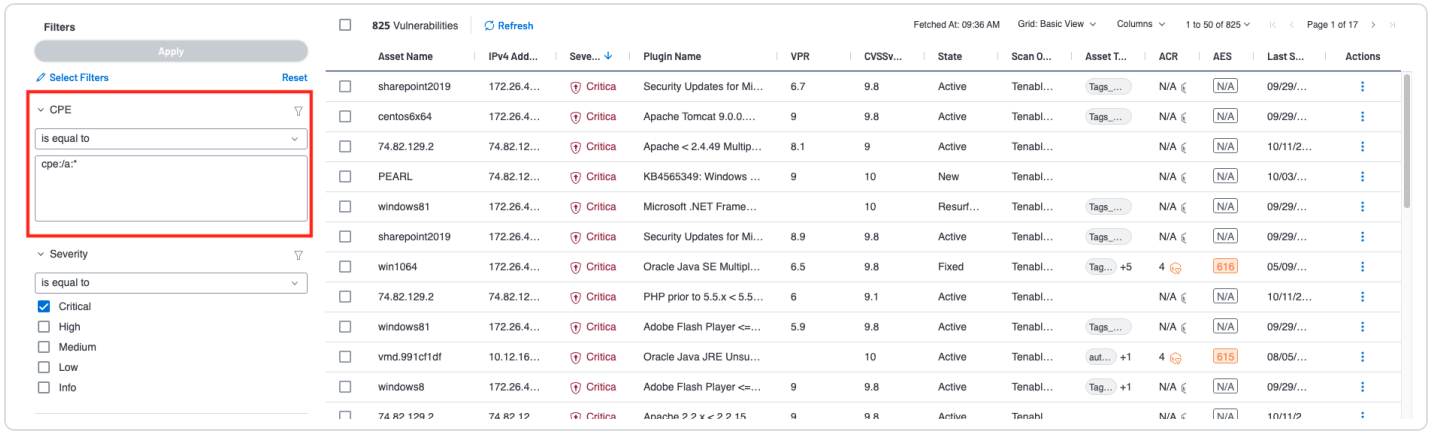
Tenable also publishes Security End of Life (SEoL) plugins to detect and assess products in the SEoL state. SEoL is the state in the Security Maintenance Life Cycle when a product no longer receives security updates. The plugins attempt to abstract various terminologies such as End of Life, Unsupported, End of Support, etc. and provide a clear definition that serves as the basis for SEoL detection plugins. There is a difference between plugins with "Unsupported" in the name and those that are SEoL. SEoL plugins are the evolution of the legacy "Unsupported" plugins. Over time, all legacy "Unsupported" plugins will be converted to the SEoL detection plugins or enter the deprecation cycle.

For more information on the SEoL plugins, reference this knowledge document.

Common Platform Enumeration (CPE) strings are also acquired when scanning an asset. The user is able to use these CPE strings to further refine their query to, for example, just focus on assets with application CPEs. CPE strings have the following format:

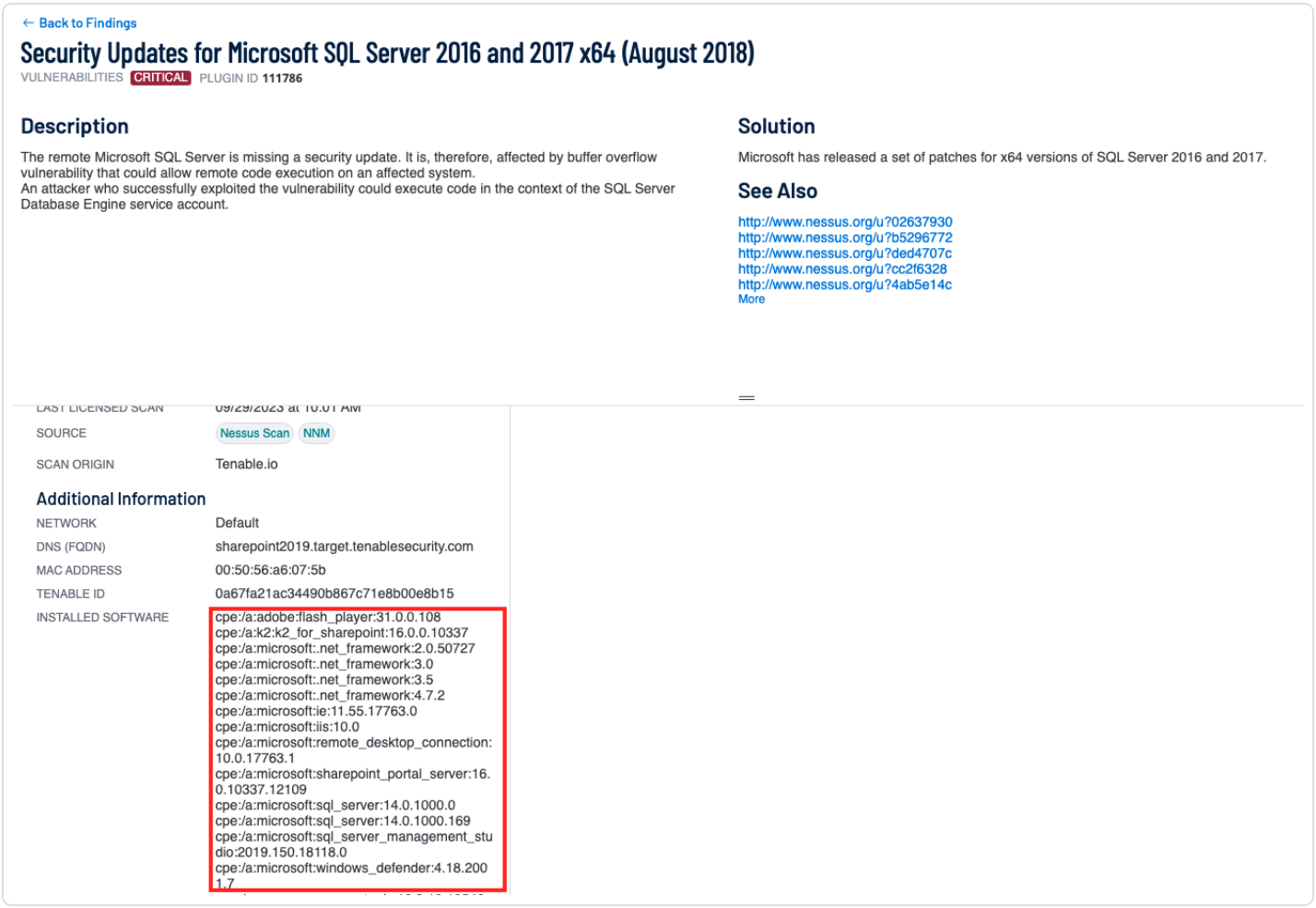
`cpe:<cpe_version>:<part>:<vendor>:<product>:<version>:<update>:<edition>:<language>:<sw_edition>:<target_sw>:<target_hw>:<other>`

Within the '`<part>`' portion of the string will be the target's type. There are three possible types; '`/a`' for Applications, '`/h`' for Hardware, and '`/o`' for Operating Systems. In relation to these essential strategies we will focus only on `/a` or `/o`. The user can further focus the query by using a query similar to `` `*cpe:/a:microsoft:` ``.



The user can refine their search of vulnerabilities by searching for only findings that have application CPE strings. The example query can be replicating by selecting ‘Advanced’ and typing “CPE is equal to cpe:/a:* AND Severity is equal to Critical." This query will return findings which have a critical severity value and have an application CPE string. The string can be confirmed by drilling into one of the findings.

When drilling into the findings and selecting **See All Details** the user is sent to the **Finding Details** page. The **Affect Asset** is displayed and the user can scroll through and see the CPE strings within the **Installed Software** section.



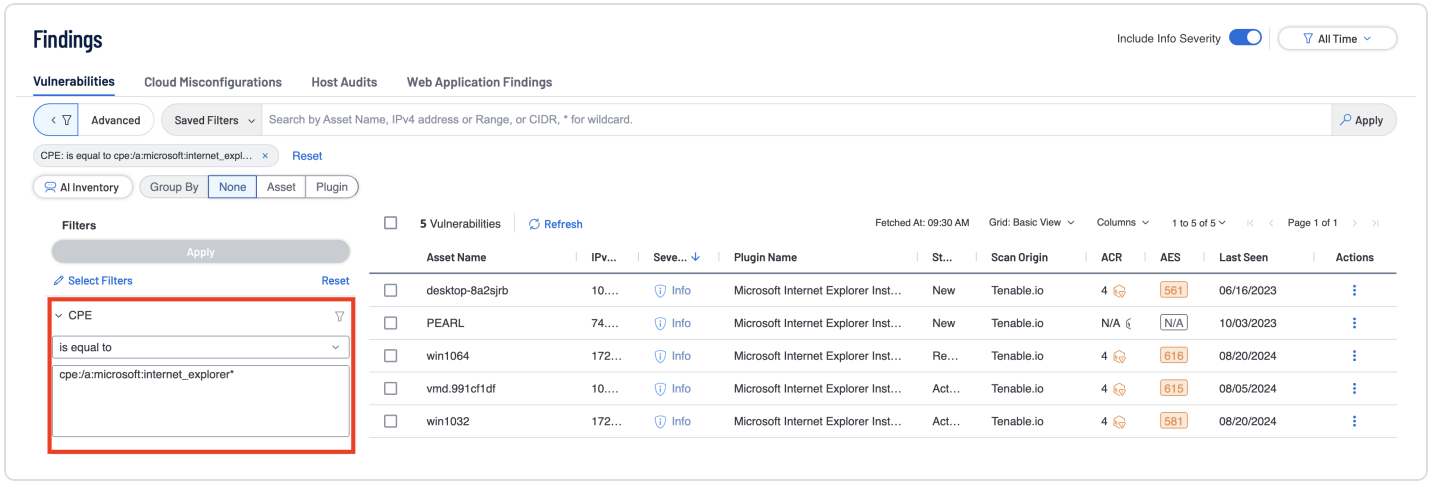
Using the CPE filter can further assist the user in searching for assets that have blacklisted software. This method will be further explained in the Application Controls section of this Cyber Exposure Study.

> **Note:** An important note to take into consideration when using the CPE filter is that a plugin can have both a **cpe:/a** and a **cpe:/o** assigned to them.

Application Control and User Application Hardening With Tenable

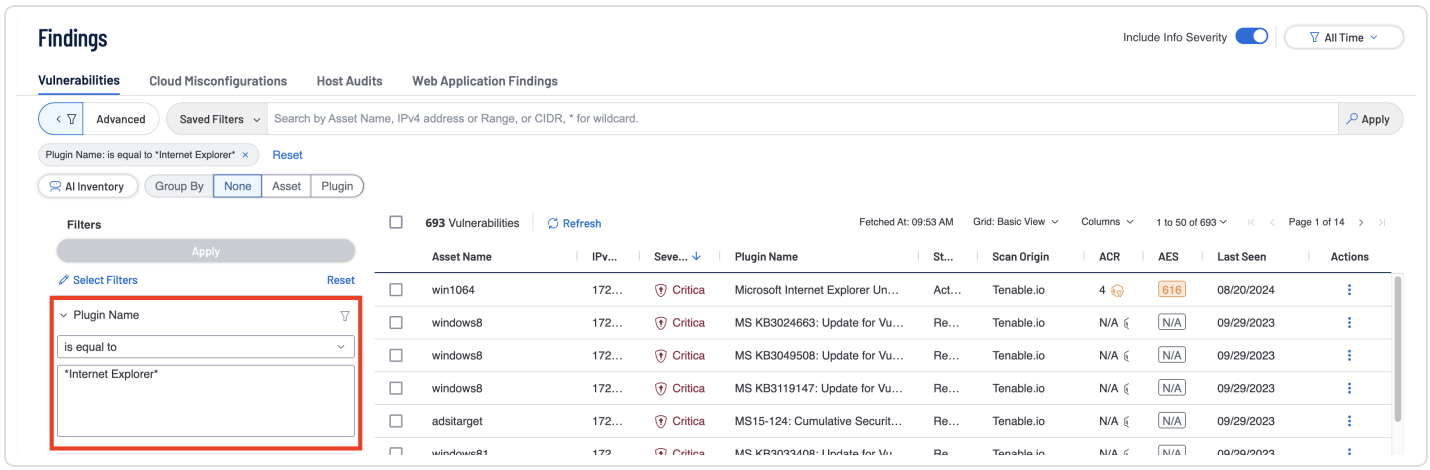
The Essential Eight strategies Application Control and User Application Hardening are closely related and some of the mapped ISM Controls that can be confirmed are ISM-1654, ISM-1621, ISM-1655, ISM-1486, ISM-1544, ISM-1659. These ISM controls are related to ensuring application blocklists are implemented and services and applications like Internet Explorer 11, Powershell 2.0, and .NET Framework 3.5 are disabled or removed altogether. In certain maturity levels the use of Application Control Solutions like Microsoft's AppLocker is required. Using Tenable Vulnerability Management to search for assets with blacklisted apps can be done using several methods. The first method can be using the CPE filter, and more specifically looking for assets with application CPE strings. For example, ASD recommends not using browsers that run Java, that means browsers like Internet Explorer or some older versions of Firefox.

Utilising the CPE filter, the user can use a string like "`cpe:/a:microsoft:internet_explorer:*`" to look for any asset that has been found to have Internet Explorer installed.



This query can be replicated by selecting **Advanced** in the **Findings** page and inputting the following query string "**CPE is equal to cpe:/a:microsoft:internet_explorer***"

Another method of looking for blacklisted applications is using the Plugin Name Filter. Many applications have detection plugins which will fire when Nessus scans the target. To search using the plugin name, and using the same example as above, the user could use the following string to search for assets with Internet Explorer; "**Plugin Name is equal to Internet Explorer**"



The operator in the query using that string should be “is equal to”; this ensures the asterisks used in the string make the query use regex. An alternative query can be made by using the “contains” operator instead and just inputting “internet explorer."

Implementing similar queries is also possible using Tenable Security Center by utilising the same filters.

As previously mentioned, an application control solution is required in certain maturity levels and for those Tenable can assist in identifying if an asset has one installed. Tenable has some detection plugins which could help identify some third party application control solutions.

Plugin ID	Plugin Name
73149	Windows AppLocker Installed
151129	VMware Carbon Black App Control Installed (Windows)
87923	McAfee Application Control / Change Control Installed
135408	Trend Micro Deep Security Agent Installed (Linux)
135409	Trend Micro Deep Security Agent Installed (Windows)

Using Tenable Host Audit Scanning will be the alternative way to identify the presence of some of these solutions and in some cases some of their configurations. Tenable Host Audit Scanning supports the use of Microsoft Security Compliance Toolkit (MSCT) benchmarks.

Using MSCT benchmarks, an organisation is able to determine more specialised information about setups within the solutions like Microsoft’s AppLocker. For example, within the MSCT Windows Server 2022 DC v1.0.0 audit file, there are checks like "AppLocker - Block Microsoft Internet

Explorer" and "AppLocker - Block Google Chrome." Using audit names like these can assist the organisation to verify certain configurations of AppLocker.

ISM control 0843 states that Application Control should be implemented on workstations, so using Host Audit Scanning can be used to verify this. ISM control 1490 states that all internet facing servers need to also have Application Control implemented and this can also be verified when run against a set of targets based on a tag or dynamic asset list consisting of the organisation's internet facing assets. Refer to Tagging and Dynamic Asset Lists for tips on Tagging and Dynamic Asset Lists.

ISM Control to Tenable Filters Mapping

Application Control:

The following mapping table lists the go-to filters an organisation can utilise to verify conformity to the related Essential Eight mapped ISM controls. The filters most used for ISM controls mapped to the Application Control Essential Eight Strategy are the Plugin Name Filter and Audit Name Filter (Plugin Name in Tenable Security Center). The Plugin Name Filter can assist any application control solution to detect any possible blacklisted application on an asset. Then the Audit Name, or Plugin Name in Security Center, can allow an organisation to target specific audit checks run during a host audit scan. These host audit scans can include, depending on the audit file used, configuration setups. For example, if an organisation utilises MSCT audit files which would be pertinent when relating to controls like ISM-1544, ISM-0843 and others, an organisation can look for the audit results for checks like "Configure detection for potentially unwanted applications." To enhance these filters utilise Asset Tagging in Tenable Vulnerability Management or Dynamic Asset Lists in Tenable Security Center.Tagging and lists will allow an organisation to separate findings and detected assets by categories like internet-facing, non-internet-facing, etc. Refer to Tagging and Dynamic Asset Lists for tips on Tagging and Dynamic Asset Lists.

Control ID	Description	Tenable VM Filter
ISM-0843	Application control is implemented on workstations.	Plugin Name, Audit Name
ISM-1490	Application control is implemented on internet-facing servers.	(Plugin Name OR Audit Name) +

		Asset Tagging
ISM-1544	Microsoft's recommended application blocklist is implemented.	Audit Name
ISM-1582	Application control rulesets are validated on an annual or more frequent basis.	(Plugin Name, Audit Name) + Last Seen
ISM-1656	Application control is implemented on non-internet-facing servers.	(Plugin Name) + Asset Tagging
ISM-1657	Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.	Audit Name
ISM-1658	Application control restricts the execution of drivers to an organisation-approved set.	Audit Name
ISM-1659	Microsoft's vulnerable driver blocklist is implemented.	Plugin Name, Audit Name

Patch Applications:

The following Mapping Table lists the go-to filters an organisation can utilise to verify conformity to the related Essential Eight mapped ISM controls. The filters most used for ISM controls mapped to the Patch Applications Essential Eight Strategy are the Plugin Name filter and Vulnerability Published filter, Patch Published filter, Exploitability Ease filter, Unsupported by Vendor filter, and Last Authenticated Scan asset filter. The Plugin Name filter can help the organisation look for any detected unsupported applications present on an asset. The Unsupported by Vendor filter can be used to quickly identify if an application is deemed to be unsupported by the vendor, this would support many controls related to Patch applications like: ISM-0304, ISM-1905, ISM-1704. Throughout the Patch Applications strategy, many of the mapped ISM controls include a timeframe when the requirements need to be done (for example,ISM-1691 states patches for office vulnerabilities need to be applied within two weeks). To meet the two week timeframes, Tenable

Vulnerability Management and Security Center support searching with the Patch Published filter. If a patch has not been released by the vendor, you can use the Vulnerability published filter. Exploitability Ease filter assists the organisation in determining if a vulnerability is exploitable or not, this exploitability is an explicit requirement in determining in ISM controls like: ISM-1690, ISM-1692, ISM-1876, and more. Lastly, the Last Authenticated Scan asset filter will satisfy the requirements where there are vulnerability scan frequency requirements and asset detection is required. Keeping the plugin set up to date is crucial to ensure the latest vulnerabilities are detected, enabling timely and accurate risk identification and remediation. These ISM controls are: ISM-1807, and ISM-1808.

Control ID	Description	Tenable VM Filter
ISM-0304	Applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors are removed.	(Unsupported by Vendor, Plugin Name)
ISM-1690	Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.	Vulnerability Published, Patch Published, Exploitability Ease
ISM-1691	Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release.	Vulnerability Published, Patch Published, plugin name
ISM-1692	Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.	Vulnerability Published, Patch Published, plugin name, Exploitability Ease
ISM-1693	Patches, updates or other vendor mitigations for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are	Vulnerability Published, Patch Published, plugin name, Exploitability

	applied within one month of release.	Ease
ISM-1698	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services.	Vulnerability Published, Patch Published, Last Seen, Online Services Tag or Asset List
ISM-1699	A vulnerability scanner is used at least weekly to identify missing patches or updates for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.	Vulnerability Published, Patch Published, plugin name
ISM-1700	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security	Vulnerability Published, Patch Published, plugin name
ISM-1704	Office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors are removed.	Plugin Name, Unsupported by Vendor
ISM-1807	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.	Last Authenticated Scan (Asset)
ISM-1808	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.	Last Authenticated Scan (Asset)
ISM-1876	Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.	Vulnerability Published, Patch Published, plugin name,Online Services Tag or

		Asset List
ISM-1901	Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.	Vulnerability Published, Patch Published, plugin name, Exploitability Ease
ISM-1905	Online services that are no longer supported by vendors are removed.	Plugin Name, Unsupported by Vendor, ,Online Services Tag or Asset List

Configure Microsoft Office Macro Settings:

The following **Mapping Table** lists the go-to filters an organisation can utilise to verify conformity to the related Essential Eight mapped ISM controls. The filters most used for ISM controls mapped to the Configure Microsoft Office Macro Essential Eight Strategy is the Audit Name filter in Tenable Vulnerability Management and Plugin Name filter in Tenable Security Center. Tenable solutions allow organisations to evaluate conformity with this Essential Strategy the most useful filter will be the Audit Name filter in Tenable Vulnerability Management or the Plugin Name filter in Tenable Security Center. These filters should be chosen for this Strategy because many MSCT audit files that can be run during a Policy Compliance Scan will include audit names related to Microsoft office macro configurations. Some related Audit Names include: "Block macros from running in Office files from the Internet - blockcontentexecutionfrominternet - access", "Security setting for macros", "Prevent Excel from running XLM macros", and many more.

Control ID	Description	Tenable VM Filter
ISM-1488	Microsoft Office macros in files originating from the internet are blocked	Audit Name
ISM-1489	Microsoft Office macro security settings cannot be changed by users.	Audit Name

ISM-1671	Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.	Audit Name
ISM-1672	Microsoft Office macro antivirus scanning is enabled.	Audit Name
ISM-1673	Microsoft Office macros are blocked from making Win32 API calls.	Audit Name
ISM-1674	Only Microsoft Office macros running from within a sandboxed environment, a Trusted Location or that are digitally signed by a trusted publisher are allowed to execute.	Audit Name
ISM-1675	Microsoft Office macros digitally signed by an untrusted publisher cannot be enabled via the Message Bar or Backstage View.	Audit Name
ISM-1676	Microsoft Office's list of trusted publishers is validated on an annual or more frequent basis.	Audit Name
ISM-1890	Microsoft Office macros are checked to ensure they are free of malicious code before being digitally signed or placed within Trusted Locations.	Audit Name

User Application Hardening:

The following mapping table lists the go-to filters an organisation can utilise to verify conformity to the related Essential Eight mapped ISM controls. The filters most used for ISM controls mapped to the User Application Hardening Essential Eight Strategy are the Plugin Name filter and the Audit Name filter in Tenable Vulnerability Management and just Plugin Name filter in Tenable Security Center. Using these filters an organisation can establish a level of compliance with the User Application Hardening strategy. The Plugin Name filter can enhance the implementation of application blocklists by detecting if any application on the list is present. Furthermore, the Host Audit scanning using any of the many supported audit files allows the organisation to get a bit more information on specific configurations.

Control ID	Description	Tenable VM Filter
ISM-1486	Web browsers do not process Java from the internet.	Plugin name,

		Audit Name
ISM-1542	Microsoft Office is configured to prevent activation of Object Linking and Embedding packages.	Audit Name
ISM-1585	Web browser security settings cannot be changed by users.	Audit Name
ISM-1621	Windows PowerShell 2.0 is disabled or removed.	Plugin Name, Host Audit Name
ISM-1654	Internet Explorer 11 is disabled or removed.	Plugin Name, Host Audit Name
ISM-1655	.NET Framework 3.5 (includes .NET 2.0 and 3.0) is disabled or removed.	Plugin Name, Host Audit Name

Limiting the Impact of Security Incidents

After reducing the impact of Malware the organisation is advised to limit the impact of any inevitable security incidents. This category of strategy is intended to minimise the impact of a security incident once the incident has occurred. The Essential Eight Strategies included in this category are:

- Patch Operating Systems
- Restrict Administrative Privileges
- Multi-Factor Authentication

When looking at which operating systems require any patches an organisation is able to follow the same steps as previously described in the previous section but here we will enhance on how an organisation will prioritise which assets should be patched first.

There are two main vulnerability categorisation methods Tenable provides which will assist in an organisation's prioritisation of patching efforts. An organisation can leverage the Tenable Asset Criticality Rating (ACR), which rates the criticality of an asset to the organisation. The ACR is expressed as an integer from 1 to 10, where higher values correspond to the asset being more critical to the business.

The **Vulnerabilities by ACR** widget enables organisations to view risks that are currently open, along with those that have been patched. The information is ranked by ACR score to demonstrate progress of risk remediation efforts, with the most critical assets at the top of the table along with a count of open and patched vulnerabilities. A large count of open vulnerabilities on critical assets indicates that the organisation presents a higher risk of a data breach. A high count of patched vulnerabilities demonstrates that the organisation is addressing cyber risk promptly, and has a mature vulnerability management program.

Vulnerabilities by ACR (Explore)

ACR / Vulnerability State	Open Vulnerability Count	Patched Vulnerability Count
ACR 10	0	0
ACR 9	0	0
ACR 8	895	69
ACR 7	327	154
ACR 6	164	58
ACR 5	2.7K	112
ACR < 4	1.15K	355

To view the ACR key driver information for any asset, Navigate to the **Assets** page and select an asset to view the asset details. In the lower left corner of the assets details page reference the **Asset Criticality Rating** information and click **More**.

Assets

Advanced | Saved Filters | Search by Agent Name, NetBi

Last Seen: within last 30 days × | Licensed: is equal to Yes × | Clear All

Hosts 5 | Cloud Resources 0 | Web Applications 2

5 Hosts | Only Show Unmanaged Assets | Refresh

Name	AES	ACR
agent-name-sal	0	4
centos9	605	4
debian11	635	5
debian12	N/A	N/A

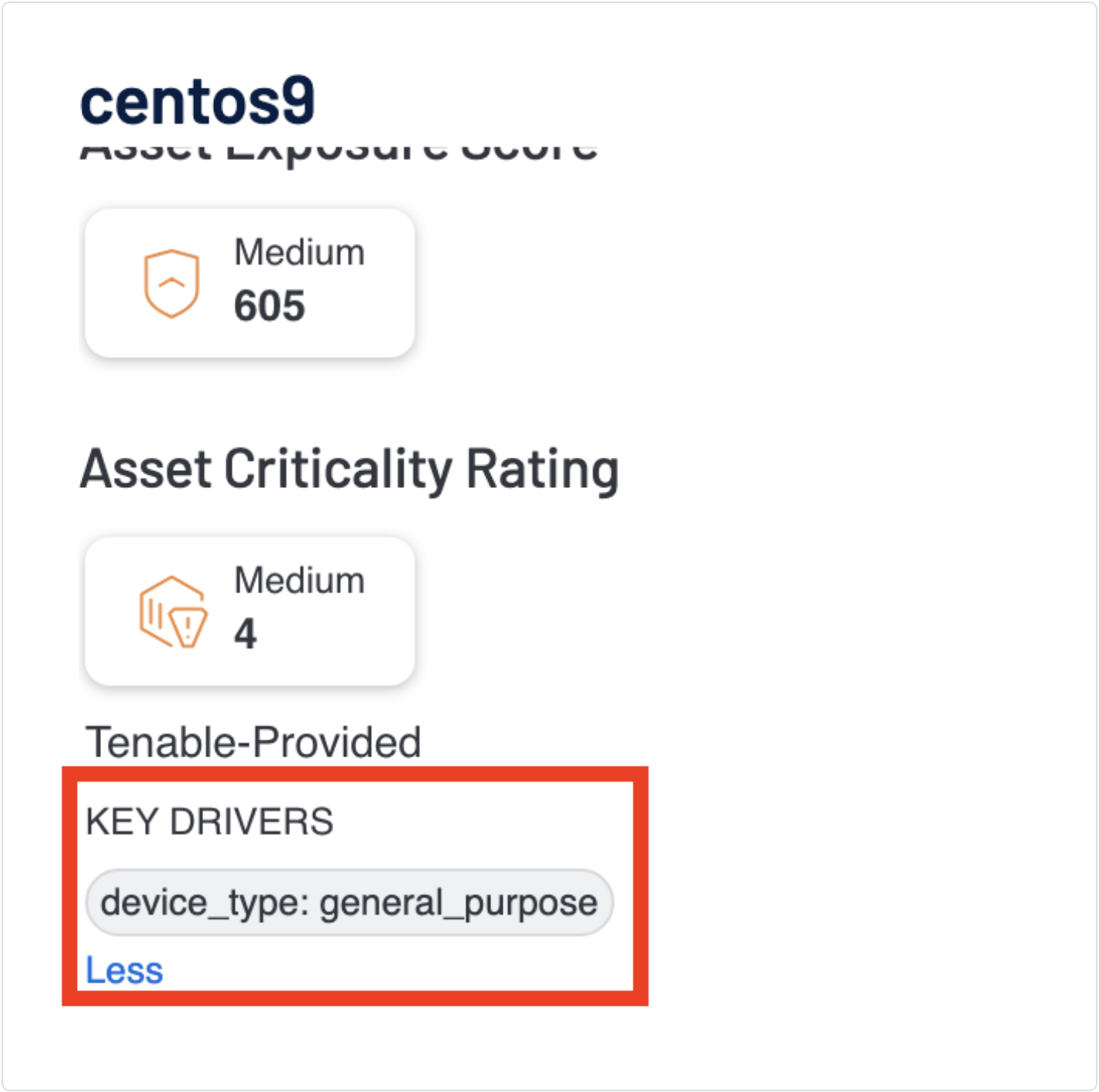
centos9

Asset Exposure Score

Medium
605

Asset Criticality Rating

Medium
4



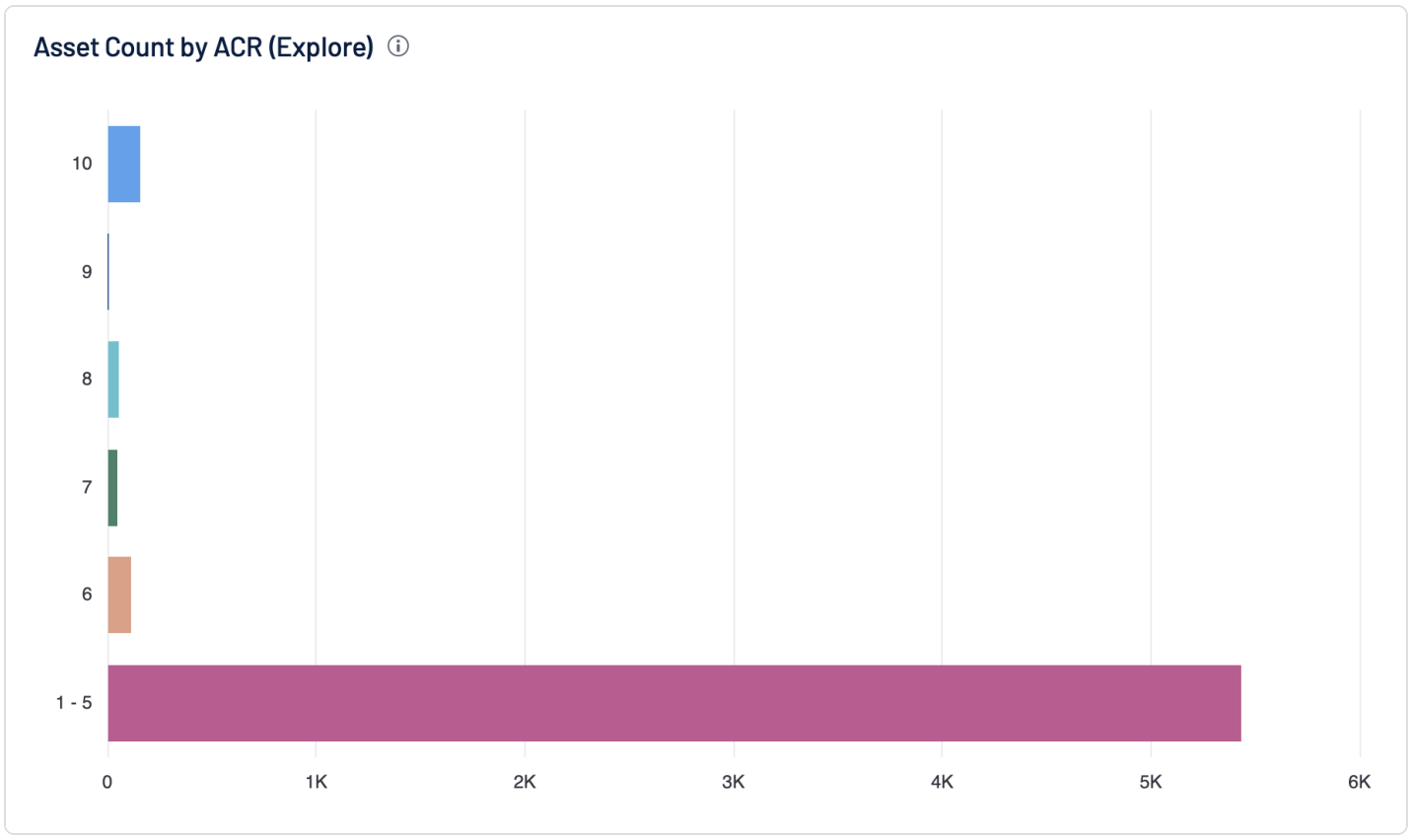
Tenable assigns an ACR to each asset on the network to represent the relative criticality of the asset as an integer from 1 to 10 . A higher ACR indicates higher criticality. Tenable One customers have the ability to adjust the default Tenable ACR to more accurately reflect organisational risk. Please refer to the Edit an ACR Manually page for more information.

The other categorisation method is the Vulnerability Priority Rating (VPR). VPR is a unique vulnerability severity rating in that the rating can change over time. Tenable updates a vulnerability's VPR score daily to reflect the current threat landscape. VPR ranges are values from 0.1-10, with the highest value representing a higher likelihood of exploitation.

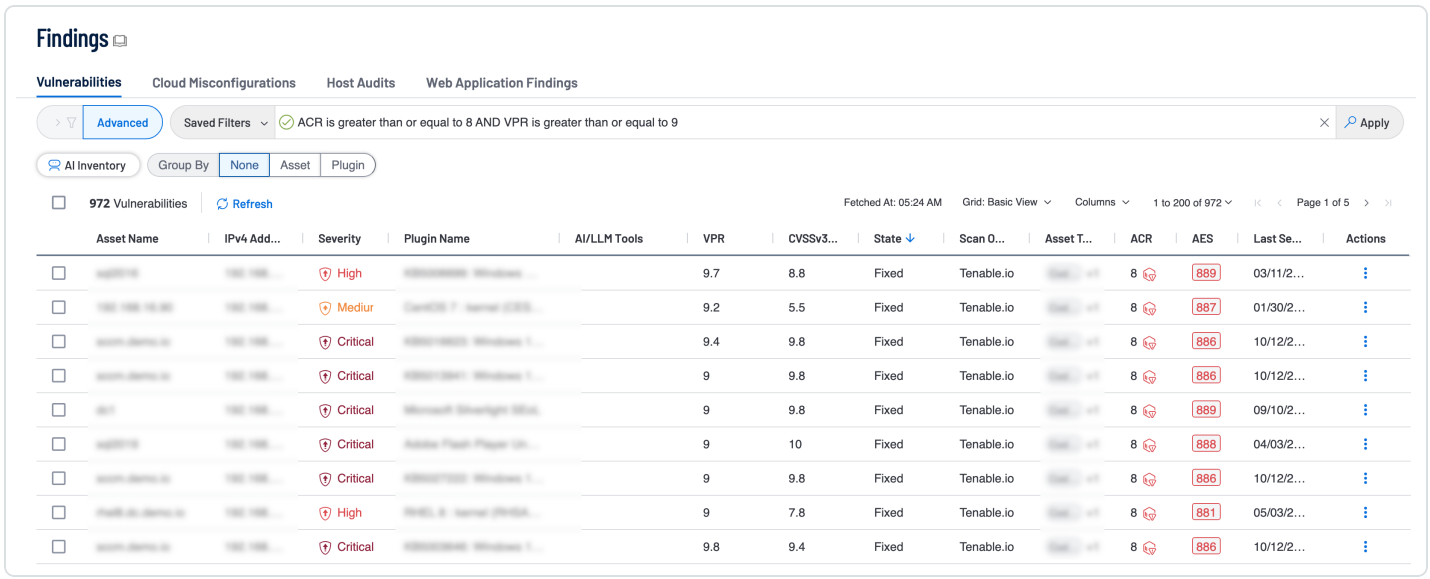
VPR severity ratings cannot be edited or customised. VPR scores are derived from seven key drivers:

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

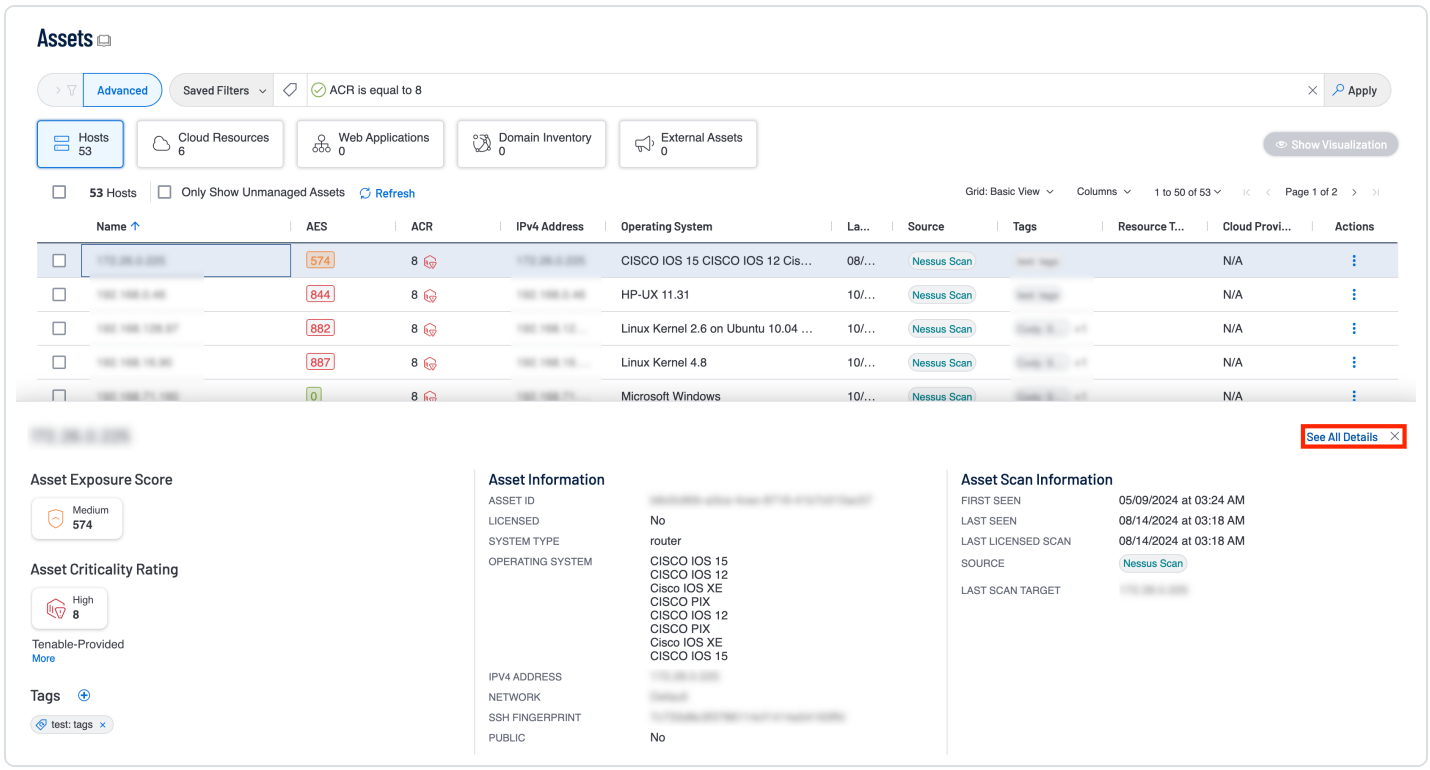
An organisation can use VPR in conjunction with ACR to establish a sense of priority when deciding what to patch first. An asset with a higher criticality rating should be prioritised over one with a lower rating as the asset is considered to be a lower business risk. Using the **Asset Count by ACR (Explore)** widget allows an analyst to quickly get a count of assets grouped by their ACR.



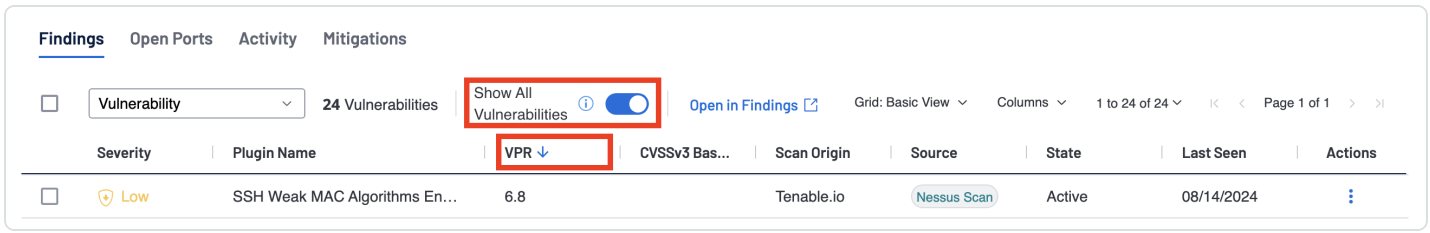
When drilling into any of the bars in this widget, the user is navigated to the **Assets** page with the query set to whichever ACR value bar was selected.



From this page, the user can drill into any asset that matches the query and look at their associated vulnerabilities by also selecting **See All Details**.



The user is then shown all vulnerabilities associated with the selected asset. The next step the user can do is sort the vulnerabilities by VPR in descending order to see the vulnerabilities with the highest VPRs.



For the organisation to satisfy specific maturity levels for the Patch Applications Strategy, the following ISM controls will be used. For example, if an organisation is trying to verify a control like ISM-1904, or ISM-1905 the queries could make use of filters like “Exploitability Ease” and/or “Patch Published”. The Exploitable Ease filter can be set to equal to “Exploit Exists” which will show any present exploitable vulnerabilities. Paired with the “Patch Published” filter, the organisation can verify some of the requirements for the date patches need to be installed by.

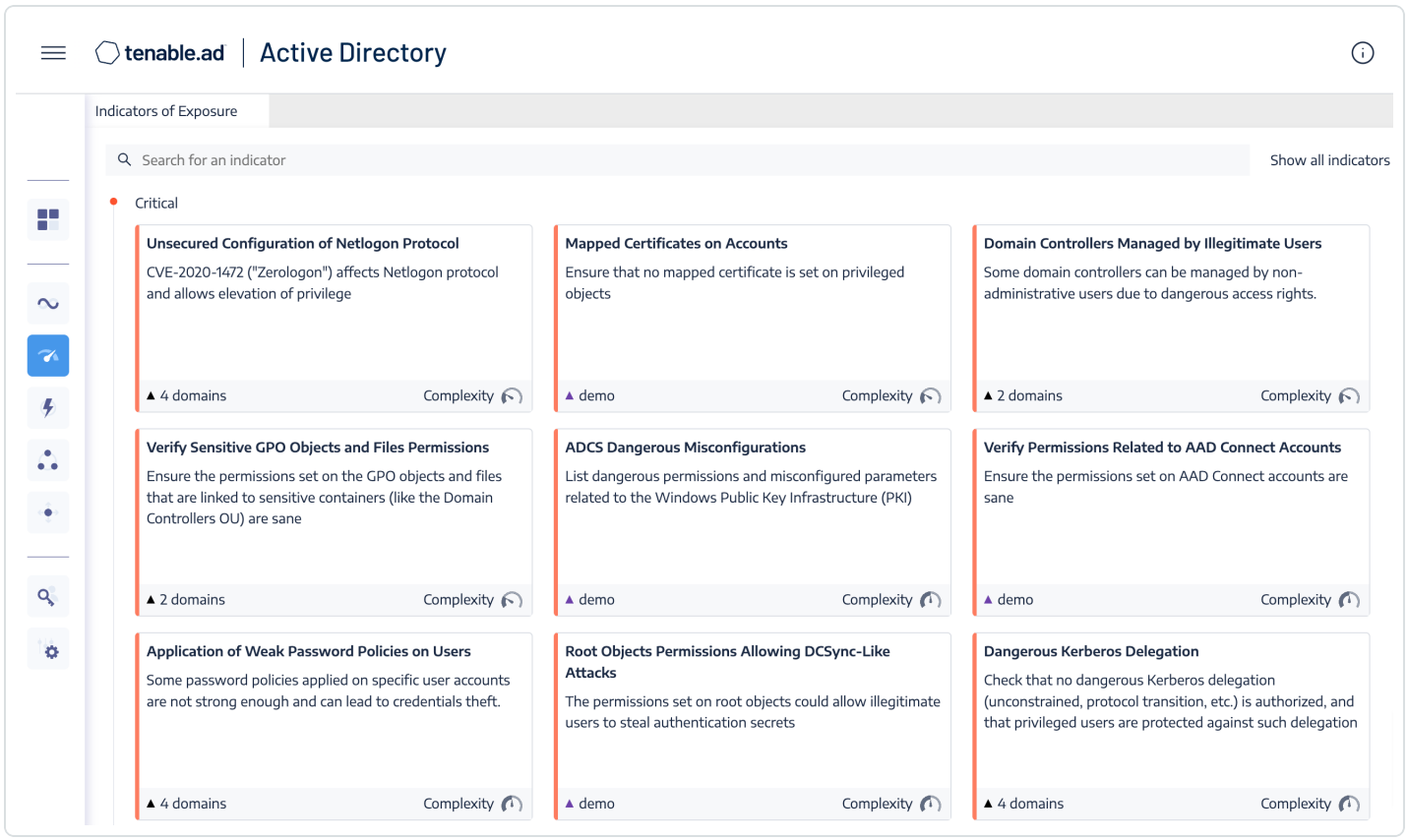
Another aspect that should be considered when limiting the impact of cyber security incidents is that the organisation is advised to Restrict Administrative Privileges. Leveraging Tenable Security Center, Tenable Vulnerability Management , and Tenable Identity Exposure solutions enables organisations to close attack paths, making the organisation a more difficult target to attack.

Tenable Identity Exposure

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

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

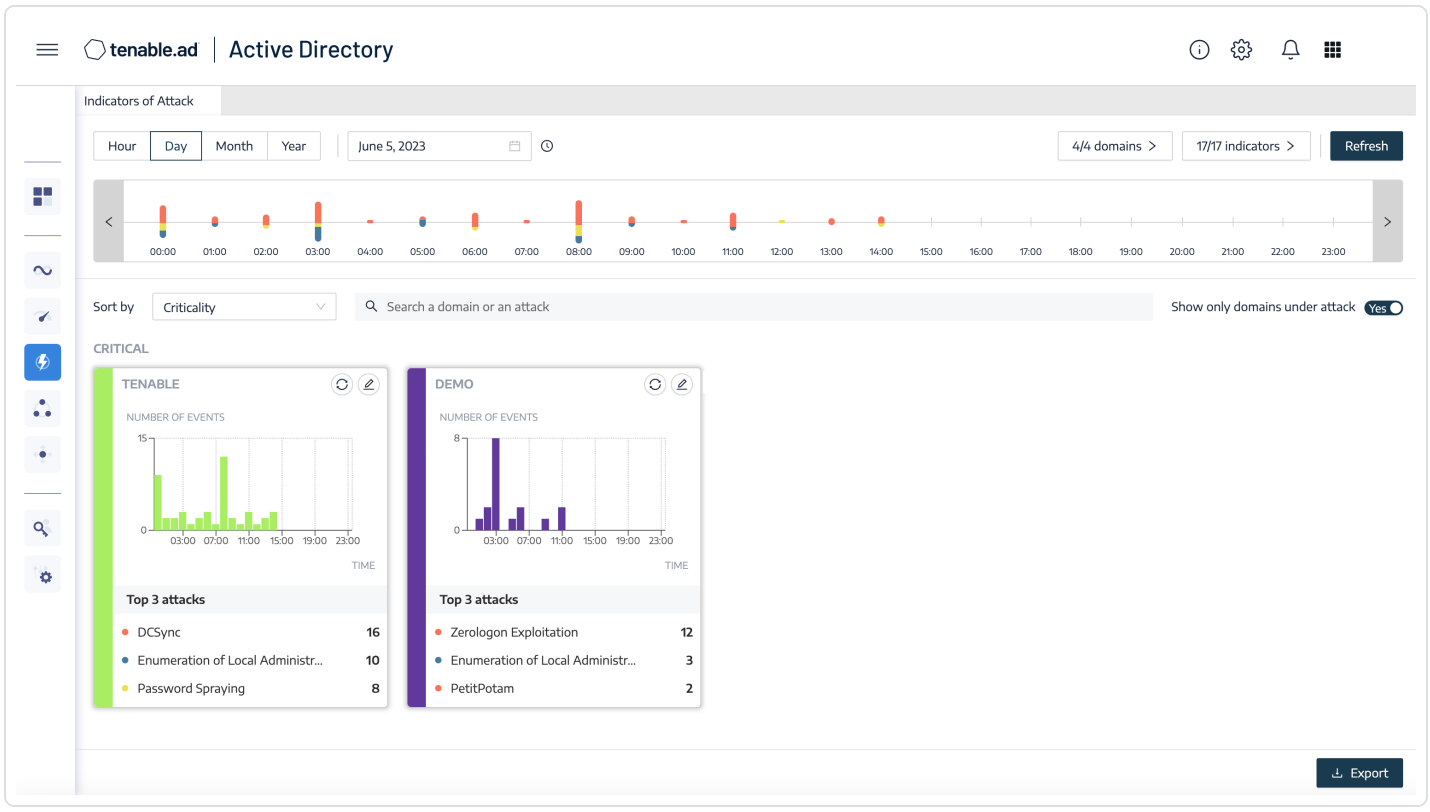
Indicators of Exposure provides an overview of critical, high, medium, and low risk exposures identified across the organisation’s domains. From the landing page, security analysts can drill down for more details about which assets are exposed.



The Indicators of Attack pane provides a consolidated view of exposures that impact the organisation's Active Directory environment. Displayed is an event timeline that shows when attacks occurred and identifies the severity level of the vulnerability targeted: Critical (red-orange), High (light orange), Medium (yellow), and Low (blue). The tiles below the timeline provide details on the top three attacks in the organisation's domains.

This view enables security teams to:

- Visualise Active Directory threats from an accurate attack timeline
- Analyse in-depth details about an Active Directory attack
- Explore MITRE ATT&CK descriptions directly from detected incidents


tenable.ad | Active Directory
Indicators of Attack
Hour
Day
Month
Year
June 5, 2023
4/4 domains
17/17 indicators
Refresh
00:00 01:00 02:00 03:00 04:00 05:00 06:00 07:00 08:00 09:00 10:00 11:00 12:00 13:00 14:00 15:00 16:00 17:00 18:00 19:00 20:00 21:00 22:00 23:00
Sort by
Criticality
Search a domain or an attack
Show only domains under attack
Yes
CRITICAL
TENABLE
NUMBER OF EVENTS
15
0
03:00 07:00 11:00 15:00 19:00 23:00
TIME
Top 3 attacks
DCSync 16
Enumeration of Local Administr... 10
Password Spraying 8
DEMO
NUMBER OF EVENTS
8
0
03:00 07:00 11:00 15:00 19:00 23:00
TIME
Top 3 attacks
Zerologon Exploitation 12
Enumeration of Local Administr... 3
PetitPotam 2
Export

Essential Eight Vulnerability Management Dashboard

The Essential Eight Vulnerability Management Dashboard is designed to support organizations in implementing and monitoring the Essential Eight Strategies for mitigating cybersecurity risks. This comprehensive dashboard provides actionable insights into asset discovery, patch management, compliance, and exploitability to ensure a robust security posture across operating systems and applications.

Essential 8: Patch Applications & Patch Operating Systems (Beta)

All | Jump to Dashboard | Dashboards | Share | Export | More

Asset Discovery Statistics

Licensed	First Observed	Discovered	Assessed	Scan Frequency	Last Scanned
1.6K	0 (<7 Days)	16.1K	10K (True)	4.8K	4.4K (<7 Days)
	1 (<30 Days)		7.1K (False)		700 (<30 Days)

Unsupported and SEoL Assets

	Unsupported	Security End of Life	Unsupported Detected
Operating System	103	12	91
Applications	321	143	178

Application Patch Risk Summary

	Most Targeted Apps	Other Apps
No Patch Available	147	4.3K
Patch Released < 7 Days Ago	0	0
Patch Released < 14 Days Ago	0	0
Patch Released < 21 Days Ago	0	0
Patch Released < 28 Days Ago	0	0
Patch Released > 28 Days Ago	4.9K	9.6K

Application Patch Published Summary

	Count
No Patch Available	718
Patch Released < 7 Days Ago	0
Patch Released < 14 Days Ago	0
Patch Released < 21 Days Ago	0
Patch Released < 28 Days Ago	0
Patch Released > 28 Days Ago	17K

Operating System Patch Published Summary

	Count
No Patch Available	708
Patch Released < 7 Days Ago	0
Patch Released < 14 Days Ago	0
Patch Released < 21 Days Ago	0
Patch Released < 28 Days Ago	0
Patch Released > 28 Days Ago	34.3K

2 Day Patch Mitigation Summary

Total (Fixed + Current)	Critical	High	Medium and Low
fixed within 2 days (within SLA)	1.44 %	1.48 %	1.42 %
not fixed within 2 days (within SLA)	0 %	0 %	0 %
fixed > 2 days (outside SLA)	0.04 %	0.02 %	0 %
not fixed > 2 days (outside SLA)	98.52 %	98.5 %	98.58 %

2 Week Patch Mitigation Summary

Total (Fixed + Current)	Critical	High	Medium and Low
fixed within 2 weeks (within SLA)	2.69 %	0.76 %	0.76 %
not fixed within 2 weeks (within SLA)	0 %	0 %	0 %
fixed > 2 weeks (outside SLA)	0 %	0 %	0 %
not fixed > 2 weeks (outside SLA)	97.31 %	99.24 %	99.24 %

1 Month Patch Mitigation Summary

Total (Fixed + Current)	Critical	High	Medium and Low
fixed within 30 Days (within SLA)	2.69 %	0.76 %	0.76 %
not fixed within 30 Days (within SLA)	0 %	0 %	0 %
fixed > 30 Days (outside SLA)	0 %	0 %	0 %
not fixed > 30 Days (outside SLA)	97.31 %	99.24 %	99.24 %

Online Services Detection Summary

Plugin Name	All Values of Severity	Count
Microsoft .NET Framework Dete…		138
Microsoft ODBC Driver for SQL …		38
Microsoft Internet Information Se…		27
Microsoft SQL Server TCP/IP Lis…		22
Microsoft SQL Server Detection (…		20
Microsoft SQL Server Managem…		10
Microsoft SQL Server Unsupport…		8
Microsoft SQL Server Unsupport…		4

Solutions Summary

Solution	All Values of Severity	Count
Update the affected packages.		12174
Update the affected firefox packa…		1030
Purchase or generate a proper S…		936
Microsoft has released security u…		876
Update the affected kernel packa…		671
Filter out the ICMP timestamp re…		467
Update the affected microcode_c…		290
Microsoft has released a set of p…		249

Exploitable Operating System Summary

	Not Exploitable	Hard to Exploit	Easy to Exploit
Low, Medium, High Severity	1.2K	6.5K	14.4K
Critical Severity	165	2.1K	3.9K

Exploitable Application Summary

	Not Exploitable	Hard to Exploit	Easy to Exploit
Low, Medium, High Severity	8K	2.7K	5.2K
Critical Severity	1.1K	744	1.9K

The Australian Cyber Security Centre (ACSC) under the Australian Signals Directorate (ASD) provides guidance to address targeted cybersecurity intrusions through its Strategies to Mitigate Cyber Security Incidents. Among these, the Essential Eight describes the minimum set of preventative cybersecurity measures organizations should implement. This guidance, complemented by the Information Security Manual (ISM) controls, forms a robust framework to ensure the confidentiality, integrity, and availability of information technology and operational technology systems. This dashboard aligns with these controls to provide critical insights into the implementation of the Essential Eight.

The Tenable One Platform combines a suite of sensors to facilitate efficient vulnerability scanning, regardless of network complexity. By leveraging Tenable's capabilities, organizations can effectively discover, assess, and understand their attack surface, gaining comprehensive insights into exposure points. This is coupled with Exposure Response features that prioritize remediation efforts based on contextual risk. The dashboard includes critical features to highlight asset discovery, identify unsupported systems, monitor patch management timelines, track compliance rates, and classify exploitable vulnerabilities, ensuring comprehensive coverage of the Essential Eight.

To maximize relevance, organizations should leverage Asset Tagging (Tenable Vulnerability Management) or Dynamic Asset Lists (Tenable Security Center). This ensures that the dashboard can be filtered to focus on data critical to implementing the Essential Eight. Tagging assets as Internet-facing or Non-Internet-facing enables differentiation for stricter service-level agreements (SLAs). For example, internet-facing systems require patching within 48 hours, while non-internet-facing systems have a longer patching window (e.g., two weeks).

Asset tags, composed of Category:Value pairs (e.g., Connectivity:Internet-Facing), can be applied manually or automatically using filtering rules such as public IP ranges, open ports (e.g., 80, 443). This categorization simplifies monitoring and prioritization for Essential Eight compliance, ensuring that organizations address vulnerabilities in their most critical assets. Tagging by application risk level (e.g., High Risk, Low Risk) or system role further enhances visibility. For more details, refer to Tenable's Tagging documentation.

This dashboard combines Tenable’s comprehensive vulnerability scanning, exposure insights, and asset prioritization with the ASD’s Essential Eight Strategies. By using the dashboard in conjunction with ISM controls and asset tagging, organizations can enhance their cybersecurity maturity, address vulnerabilities more effectively, and ensure compliance with Australia’s cybersecurity standards.

You can break down the dashboard into five main sections. The image above is annotated with colors to differentiate between the sections. The **red** widgets include The Asset Discovery Statistics and the Unsupported and EoL Assets widgets. These two widgets will provide the user with an overview of scan health in terms of assets discovered and Assets are broken down by products that are either unsupported, SEoL, or that have been detected as running an unsupported product.

The **blue** widgets include the Application Patch Risk Summary, Application Patch Published Summary and Operating System Patch Published Summary. These three widgets provide the user with an application based widget that focuses commonly targeted apps along with a row for different patch published date ranges to cover various SLA requirements within the ISM controls and, a pair of widgets (one application based and one operating system based) that will give more general counts of applications or operating systems along with patch published date ranges as well.

The **purple** widgets are a trio of widgets that all provide counts of critical, high, medium and low vulnerabilities split between specific SLA ranges. The three ranges are two day, two week, and one month. The **orange** widgets are both tables that can be easily replicated by a user for better customization if desired but should provide a good starting point for both an inventory list of possible online services (first widget) and a list of solutions for detected vulnerabilities.

The **green** widgets provide a couple of matrices that give the user counts of exploitable applications and operating systems. These widgets also utilize the CVSS Attack Complexity (AC) scores to split between hard to exploit and easier to exploit counts. Once again, the whole dashboard is greatly improved by leveraging asset tagging.