Tenable Cyber Exposure Study - Cyber Insurance Report

Last Revised: September 11, 2023

Table of Contents

Overview

A key driver for organizations that seek to obtain cyber insurance is to limit risk of financial loss in the event of a cyber breach. Cyber Insurance enables organizations to transfer some of the financial risk of a data breach by providing coverage to compensate for financial losses. As the costs associated with data breaches continue to rise, insurers are becoming more diligent with risk assessments both for cyber insurance applicants and those insured during the term of the policy. Underwriters want to ensure that organizations have a mature program to address risks posed by cyber exposure. Identifying and mapping the owners, stakeholders and processes, enables underwriters to quickly understand the extent of the exposure and risk to business operations if there is a breach to determine liability to the organization.

Cyber insurance underwriters need to have supporting evidence demonstrating the strength of the applicant's cybersecurity and risk management programs. This Cyber Exposure Study provides guidance through the following primary focus areas of the Cyber Insurance Report that are critical to any risk assessment program.

1. Asset Discovery and Assessment
2. Risk Prioritization
3. Vulnerability Management
4. SLAs and Remediation

The Tenable Cyber Insurance Report provides measurements for the foundation of a cyber risk program for organizations. This data helps facilitate risk analysis based on vulnerabilities discovered using the Tenable Vulnerability Management platform, which provides information about the organization's cyber risk exposure. Tenable Vulnerability Management provides organizations the ability to demonstrate risk management maturity with insurance companies.

Most organizations have some form of vulnerability management program, usually mandated by one of the myriad compliance standards or Service Level Agreements (SLAs) with third parties. Security frameworks and benchmarks such as the NIST SP 800-53, or the CIS Benchmarks provide consensus guidance that organizations can use to ensure their vulnerability management program is aligned with industry standards. Cyber Insurance underwriters do not impose any new or special requirements above what organizations are already required to follow.

Vulnerabilities are exposures that can be exploited. They can be in the form of a software defect, configuration error or basic human error. Vulnerability management programs provide some level of

assurance that assets are scanned, patched, and risk exposure is reduced to acceptable levels. The Tenable Cyber Insurance Report enables organizations to easily generate supporting evidence data required by cyber insurance underwriters that demonstrates the strength of their cybersecurity and risk management programs. Insurance companies that issue cyber insurance policies have varying questionnaires and rating services that may not provide a complete picture of the organization's cyber risk.

The Cyber Insurance Report provides measurements for the foundation of a cyber risk management program for organizations. This data helps facilitate risk analysis based on vulnerabilities discovered using the Tenable Vulnerability Management platform, which provides information about the organization's cyber risk exposure. Organizations must know the existence and location of critical assets to ensure that assets are monitored and protected based on the business risk rating of each asset. Identifying assets facilitates vulnerability scanning and remediation by ensuring that scans are configured to probe for common weaknesses in the platform or application

Risk Treatment is a strategy to appropriately manage threats to maximize profit and minimize financial loss. Cyber risk is associated with a level of severity of identified vulnerabilities that could potentially cause financial loss to the organization. Severity can be adjusted by accepting risk or adjusting vulnerability severity levels. This report has been configured to only report statistics on vulnerabilities and assets detected during the last 180 days. The report also takes a static approach by using the CVSSv3 Base Score to measure severity. The CVSS Base Score is divided into severity levels, 0 for Informational, 0.1-3.9 for Low, 4.0-6.9 for Medium, 7.0 to 9.9 for High, and 10 for Critical. These severity levels are used throughout this report.

> **Note:** This report does not take into account recast or accepted risk.

The Cyber Insurance Report leverages the Tenable Asset Criticality Rating (ACR), which rates the criticality of an asset to the organization. The ACR is expressed as an integer from 1 to 10, where higher values correspond to the asset being more critical to the business. For more information on editing an asset's ACR rating, please refer to the documentation page titled Edit an Explore Host Asset's ACR.

CVSS Base Score is the mainstay of most vulnerability management programs as the primary metric to compare and prioritize vulnerabilities. The base score does not change over time, and is not dependent on any other compensating factors. Tenable recommends combining the CVSS base score with temporal, environmental, and other factors for a more accurate view of business risk.

The Cyber Insurance Report has read-only widgets that cannot be modified by Tenable Vulnerability Management users that provide underwriters insight into an organization's cyber risk posture. This report benefits both insurers and applicants seeking to demonstrate proactive risk reduction actions. Tenable Vulnerability Management users are not able to modify the report by adding additional filters using Tags or Custom Assets. The report displays all assets discovered using the sources Nessus, Nessus Agent, Tenable Nessus Network Monitor or third parties.

Asset Discovery and Assessment

Organizations need to identify the existence and location of critical assets to ensure that said assets are monitored and protected based on each asset’s business risk rating. Discovering assets enables organizations to establish an inventory, which can be used to assess and mitigate associated risks to the organization. An asset inventory enables organizations to configure scans to probe for common weaknesses in the platform or application.

Asset Discovery

Tenable Vulnerability Management supports the discovery of assets without scanning the assets for vulnerabilities. Tenable Vulnerability Management provides scan templates for discovery scanning and passive detection using Tenable Nessus Network Monitor in discovery mode. Tenable Vulnerability Management also supports connectors from third parties such as ServiceNow or API calls to manually enter the assets. Assets that have not been scanned for vulnerabilities do not count towards the organization's asset license limit. After assets are discovered in this manner, a strategy can be developed to categorize and scan assets for vulnerabilities. Importing assets via the API or third party integration, such as ServiceNow, increases scanning capabilities by leveraging the extensive ServiceNow Configuration Management Database (CMDB) to accurately track assets. For more information on reconciling assets between ServiceNow and Tenable Vulnerability Management , please refer to the Tenable and ServiceNow Integration Guide.

For more information on Container Security Connectors please refer to the Configure Container Security Connectors to Import and Scan Images page.

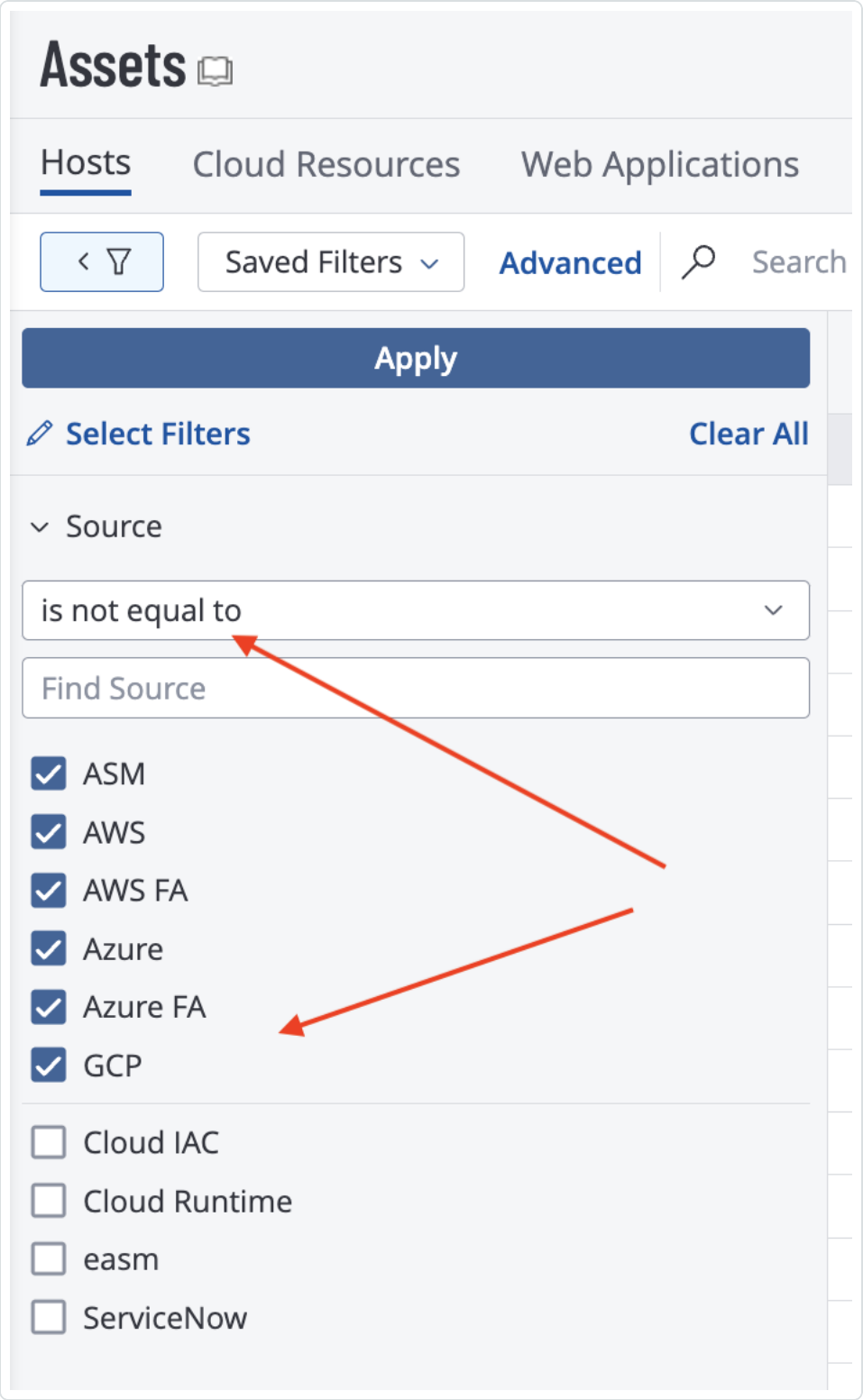
Assets by Source

The Asset by Source widget displays discovered third party assets that are not licensed, and have not been assessed for vulnerabilities. This query is accomplished by setting the source filter to ”is not equal to” and selecting the following values: GCP, AWS, SSM, AZURE, AZURE_FA, WAS, INDUSTRIAL_SECURITY, ASM, NNM, NESSUS_SCAN, or NESSUS_AGENT. The widget provides a count of assets by collection method. Assets listed have not been scanned for vulnerabilities or by other Tenable sensors. The ability to import assets from external sources into Tenable Vulnerability Management reduces the number of blind spots, and increases the likelihood of complete scan coverage.

Asset by Source

Source	Count
paloalto	25
servicenow	25
vmd team	25

To recreate the results from this widget,, navigate to the **Explore Overview → Assets** page in Tenable Vulnerability Management as shown below. Select **Source** as a filter option, choose “**is not equal to**” from the drop down menu, and check the boxes for the appropriate options. Click **Apply** to apply the filter to the results.


Assets
Hosts
Cloud Resources
Web Applications
Saved Filters
Advanced
Search
Apply
Select Filters
Clear All
Source
is not equal to
Find Source
ASM
AWS
AWS FA
Azure
Azure FA
GCP
Cloud IAC
Cloud Runtime
easm
ServiceNow

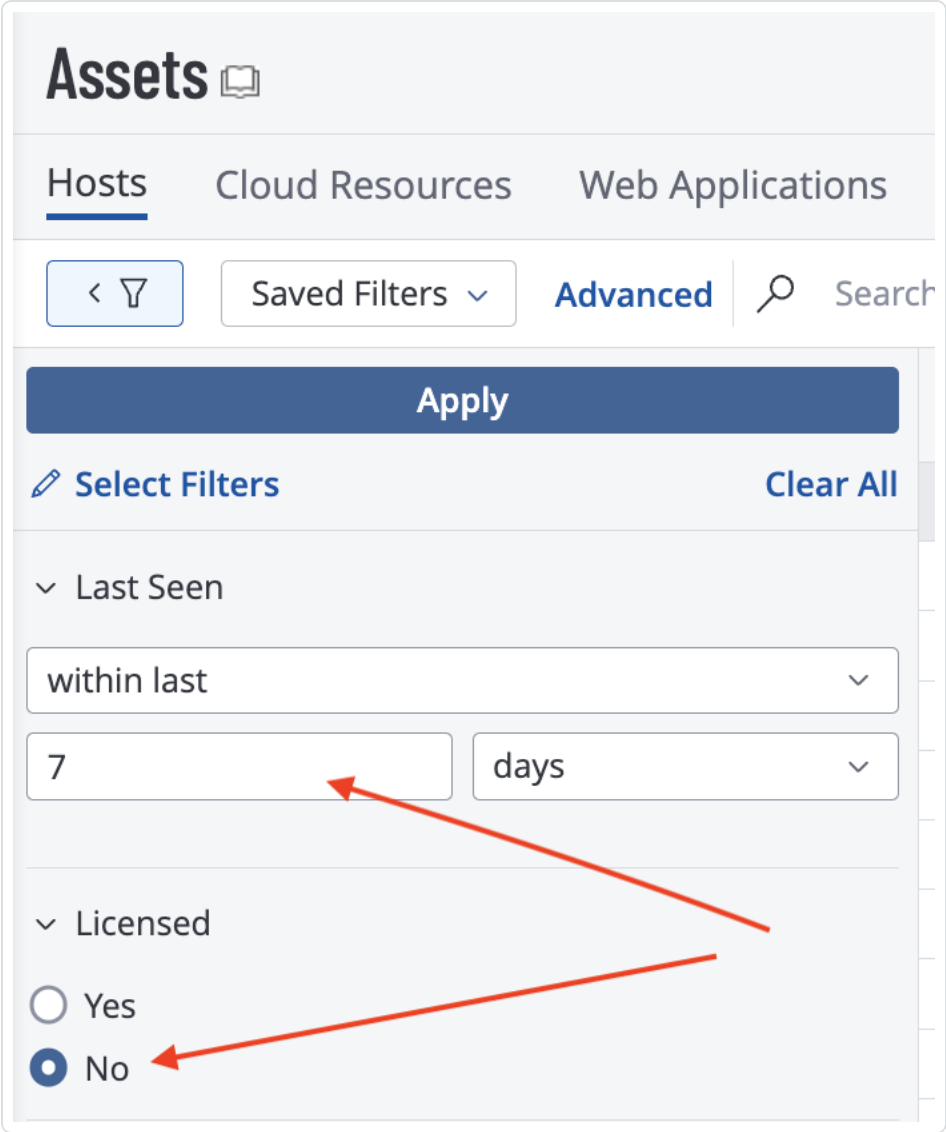
Third Party Asset Discovery

The **Third Party Asset Discovery** widget displays the count of assets that have been imported and considered discovered but not scanned, grouped by time ranges from when the last import occurred. The data is organized over time periods for 7,14, 30, 60, 90, and 90+ days using the **Last Seen** filter. As with the "**Asset By Source**" widget, the source filter is set to remove any asset that is discovered by Tenable sensors. Once a third party asset is scanned, the asset becomes licensed and will be removed from this widget. This widget is a useful gauge to determine the maturity of the vulnerability management program, since it demonstrates whether or not assets are scanned on a regular basis as they are added to the network. For example, organizations may scan the network weekly, or even daily. If there are gaps in scanning activity there may be higher counts in the longer timeframes.

Third Party Asset Discovery

Days / Status	Discovered
7	75
14	0
30	0
60	0
90	0
90+	0
Total	75

The queries in the **Third Party Asset Discovery** widget can be created manually via the **Explore Overview → Assets** page in Tenable Vulnerability Management as shown below. Select **Last Seen** as a filter option and choose a time frame. Then add a second filter for **Licensed** and select **No** to display only the assets that have not been scanned for vulnerabilities. Click **Apply** to apply the filter to the results.


Assets
Hosts
Cloud Resources
Web Applications
Saved Filters
Advanced
Search
Apply
Select Filters
Clear All
Last Seen
within last
7
days
Licensed
Yes
No

Asset Status Detected by Tenable

The **Asset Status Detected by Tenable** widget provides an overview of assets that have been recently discovered or scanned with or without credentials. The timeframe displayed shows key time periods for 7,14,30, 60, 90, and 90+ days using the **Last Seen** filter to help determine what new devices are entering the environment. New devices that have not been evaluated introduce unknown risk. Assets that are scanned or discovered are only counted towards the license limit if that asset has been assessed for vulnerabilities.

The **Days/Status** column contains static rows displaying time ranges from 7 to 90+ days. Each row utilizes the **last_observed** filter to display information for the specified time range. These rows are the primary focal point for the other columns.

The **Tenable Discovered** column displays assets that have been discovered with host discovery plugins. A healthy environment will have low numbers in the Tenable Discovered column, with those numbers increasing as they progress downwards in the matrix. This is a clear indication that no new devices have been recently discovered. The "**Is Licensed is equal to False**" filter is used for this column.

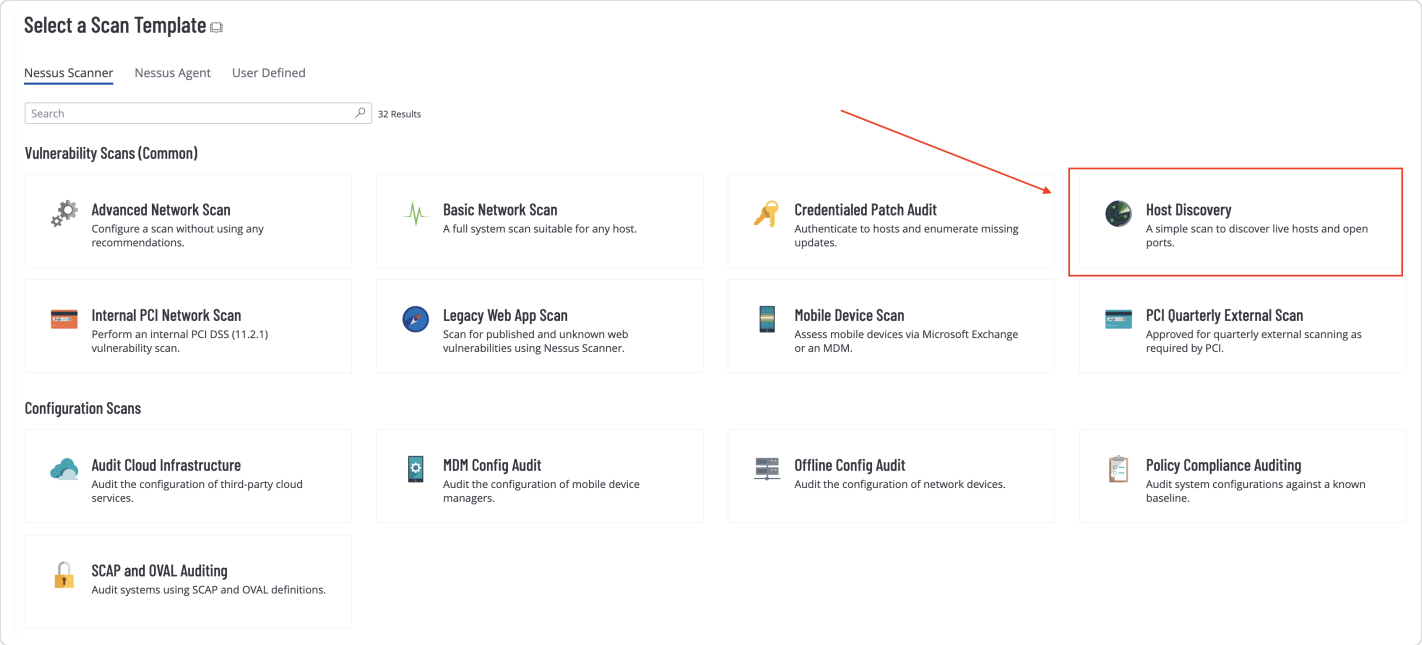
The **Scanned** column displays assets that have been scanned using credentials. Organizations with good security practices will have the largest numbers at the top with lowest numbers at the bottom (the reverse of the **Tenable Discovered** column), indicating that devices are being scanned on a regular and frequent basis. The "**Is Licensed is equal to True**" filter is used for this column.

The **Total** column and row displays the total number of assets for each row or column.

Asset Status Detected by Tenable

Days / Status	Tenable Discovered	Scanned	Total
7	0	151	151
14	0	0	0
30	0	3	3
60	0	10	10
90	0	71	71
90+	424	0	424
Total	424	235	659

Assets that have been scanned using a **Host Discovery** template, as shown below, scanned with discovery-only plugins, or have been imported and do not contain vulnerability data (such as ServiceNow data) are not associated with any risk-based vulnerabilities.



Data from Tenable Nessus Network Monitor running in discovery mode will also not count towards the license limit. Scanned assets with risk-based vulnerability data count against the license,

regardless of the source (Nessus Agent or Tenable Vulnerability Management). These vulnerability records indicate some level of a risk assessment has been performed. Organizations with a robust vulnerability management program will continuously close the loop between those assets which are discovered and assets which are assessed within an acceptable period of time.

In addition to IP addresses, Tenable Vulnerability Management uses asset attributes to identify an asset. When an asset is first discovered, information is gathered that may include a BIOS UUID, MAC Address, NetBIOS name, FQDN, and other attributes that can be used to reliably identify an asset. Additionally, authenticated scanning and Nessus agents assign a Tenable UUID to the device. When an asset is subsequently scanned, the information is compared to previously discovered assets. If the information does not match a previously discovered asset, the new device is added to the asset inventory. Tenable Vulnerability Management leverages a variety of methods and proprietary algorithms to avoid double counting the same asset. This process increases the accuracy of tracking and identifying assets across the network.

More details on how Tenable Vulnerability Management can be leveraged to identify assets can be found on the Mapping, Classification, and Categorization of Assets and the Key Asset Attributes pages. For more information related to networks, please refer to the Networks section of the documentation.

Asset Assessment

Vulnerability assessments are excellent for testing visible network services and finding vulnerabilities or misconfigurations that may expose sensitive information. The health of an organization's scanning program is based on the level of access the scanner is assigned during the vulnerability scan. When organizations scan with invalid or unprivileged credentials, proper and thorough assessments are not completed, and lead to false sense of security or in accurate risk assessments.

Credentialed scans provide more detailed results that can help to detect outdated software, vulnerabilities, and compliance issues. Credentials enable the scanner to login to the asset as an authorized user and view configuration and other data that the provided credentials are permitted to see. Credentials from a privileged user, such as the administrator or root, provide the most accurate information, enabling organizations to have a more comprehensive view of cyber risk for that asset.

Tenable provides several plugins to assist with common scan problems, such as determining if scans are incomplete, have errors, or credentials are bad or missing. Organizations with good scan health leverage this information to ensure scans are configured to use the appropriate plugins and settings for the devices being scanned. In addition to reporting on complete scans, the Scan Health widget identifies the most common scan issues, such as no credentials, bad credentials, incomplete scans, and scan errors. This information can be used to demonstrate that organizations are using appropriate authentication for scanning. Tenable recommends scanning at least twice per week with all plugins to achieve the most complete scan and vulnerability data.

Scan Health

The **Scan Health** widget is separated into two sets of data points: assets scanned with authentication; and assets scanned without authentication. The rose colored cells indicate errors from scans where authentication was not configured or failed. The teal colored cells indicate a degree of authentication was successful. All data points within this widget are dependent on the level of authentication. If a majority of the assets are scanned without credentials, the vulnerability counts could potentially be much lower. The vulnerability counts could also be lower for assets that are scanned with credentials that do not provide administrative access.

> **Note**: Assets where the scanner has the highest privileged credentialed access will have the best data on the risk exposure to the asset.

Scan Health

Scanned Assets	235	Authenticated Scanned Asset	117
Not Assessed	Count by Findings	Findings from Assets	Percentage
No Creds, Bad Creds	185	50	78.72 %
Incomplete Scans	163	72	69.36 %
Authenticated Scans	Count by Findings	Findings from Assets	Percentage
Scan Errors	14	103	11.97 %
Patch Assessment Checks Not Supported	10	107	8.55 %
Complete Scan	93	24	79.49 %

Each of the rows of the **Scan Health** widget are defined below:

No Creds, Bad Creds - This row provides the asset count for each scan result with plugin No Credentials (110723), Failure for Provided Credentials (104410), or OS Security Patch Assessment Not Available (117886) detected. The results indicate that either no credentials were used in the scan or the credentials used were not valid for the asset. These results are compared against the overall

scanned assets, for a percentage of assets where a successful vulnerability scan was not completed.

Incomplete Scans – This row provides the asset count for each scan result with Windows SMB Registry Not Fully Accessible (10428), OS Security Patch Assessment Failed (21745), or SSH Commands Require Privilege Escalation (102094) plugins. The results indicate that successful authentication was not fully achieved, the patch assessment failed to execute or there was some other related login problem. These scans may have used valid credentials but some other problem occurred and the scan was aborted. These results are compared against the overall scanned assets, for a percentage of assets where a successful vulnerability scan was not completed.

Scan Errors – This row provides the asset count for each scan result with Insufficient Privilege (110385) or Patch Assessment Checks Not Supported (110695). These assets had successful authentication, and therefore are compared against the Authenticated Scan result column. However, an error was detected by a plugin or scan results for the operating systems were not available.

Complete Scan – This row provides the asset count for each scan result with the OS Security Patch Assessment Available (117887) plugin present. These assets have local checks enabled and the most complete scan possible was achieved at that time. These assets had successful authentication, and therefore are compared against the Authenticated Scan result column. Having a majority of assets present in this row demonstrates organizations with a healthy vulnerability management program.

Authenticated Scanning

Understanding the differences between an authenticated scan, and a non-authenticated scan is critical. A non-authenticated scan, discovery scan, or default scan is a remote test performed without authentication. Non-authenticated scans probe the target with various packets. This external view of the target can often determine the type of the device, what ports are open, and what services are running on those ports. However, scanning without credentials does not provide much detail on missing OS or third-party patches or compliance with industry benchmarks and frameworks, such as the CIS Benchmarks or the NIST Cybersecurity Framework (CSF).

When a scan is initiated, Nessus probes the target to determine which ports can be used to login to the target. If credentials have been provided, Nessus will use the credentials to login to the asset, and attempt to perform a more thorough assessment. Privileged access to the asset is necessary during an authenticated scan to determine information such as installed software, including the version, anti-virus software configuration, password policies, missing patches, and misconfigurations. If no credentials are provided, or the credentials are invalid, Nessus will continue to probe the device externally.

The quantity of vulnerabilities reported between an authenticated and unauthenticated scan can often be 10 times greater when scan use privileged credentials. Tenable Vulnerability Management customers can use Predictive Prioritization and Vulnerability Priority Rating (VPR) to help manage this vulnerability overload. These vulnerabilities always existed; authenticated assessments provide visibility that an unauthenticated one cannot. In general, fully credentialed scans are preferred, as they create less network overhead and up to ten times more information is returned to help with risk identification and prioritization. The integrity of the vulnerability scan results are based on the level of access provided to the scanner, for complete vulnerability assessment, Tenable recommends using credentials or agent based scans. Reference the Credentials in Vulnerability Management Scans document for more information on scan credentials configuration.

Risk Prioritization

Asset Criticality Rating (ACR) establishes the priority of each asset based on indicators of business value and criticality. ACR is based on several key metrics such as business purpose, asset type, location, connectivity, capabilities and third-party data. ACRs range from 0 to 10. Assets with a low ACR are not considered business critical. Assets with a high ACR are considered to be the organization's most critical and carry the greater business impact if compromised. This section displays

risk by ACR, Common Vulnerability Scoring System (CVSS), exploitability by Attack Vector and Framework.

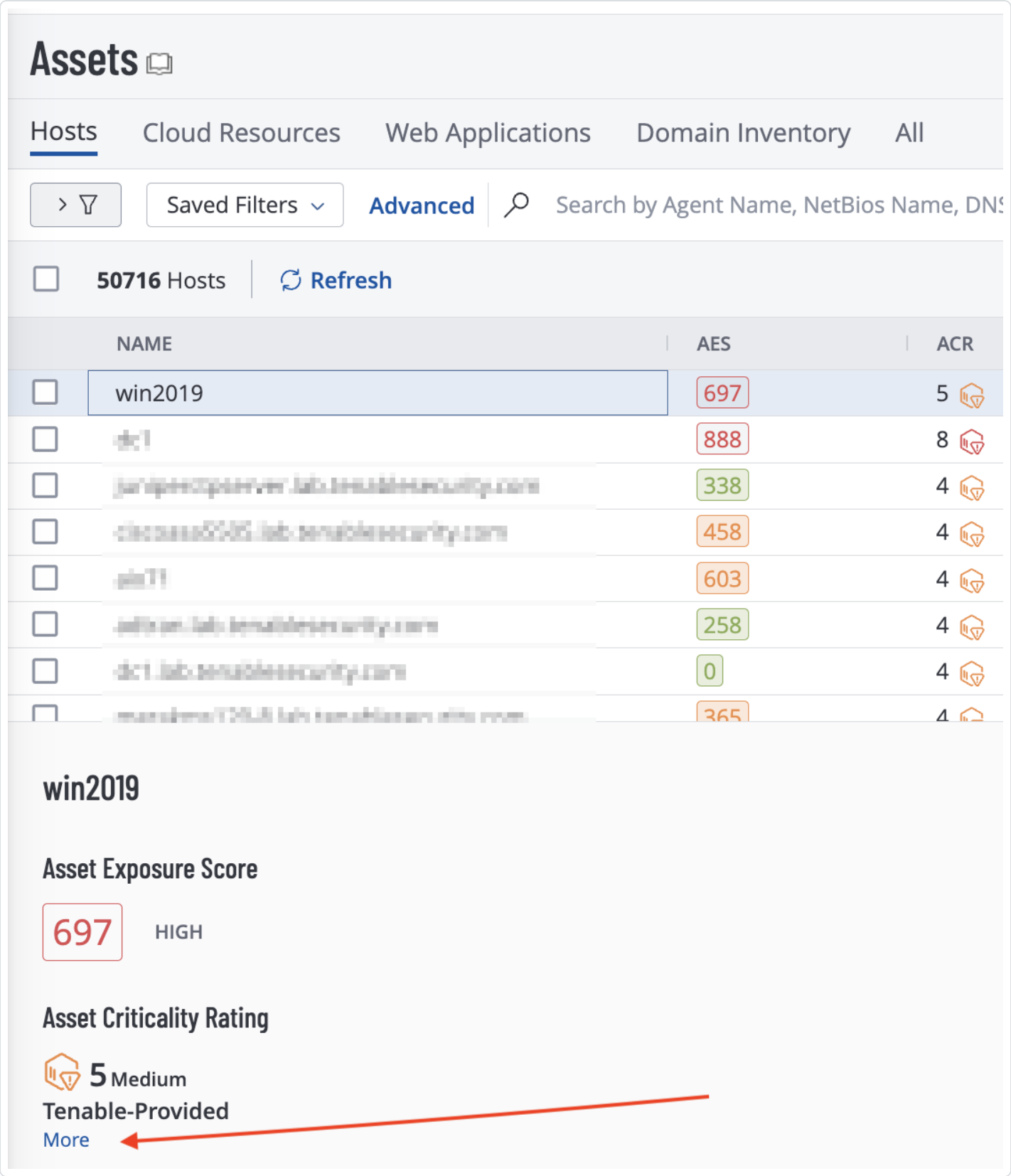
Vulnerabilities by ACR

The **Vulnerabilities by ACR** widget enables organizations 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 organization presents a higher risk of a data breach. A high count of patched vulnerabilities demonstrates that the organization is addressing cyber risk promptly, and has a mature vulnerability management program.

Vulnerabilities by ACR

ACR / Vulnerability State	Open Vulnerability Count	Patched Vulnerability Count
ACR 10	0	0
ACR 9	0	0
ACR 8	3.04K	171
ACR 7	1.49K	173
ACR 6	1.32K	87
ACR 5	1.4K	290
ACR < 4	5.17K	481

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**.



The key drivers will be displayed.

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. Lumin customers have the ability to adjust the default Tenable ACR to more accurately reflect organizational risk. Please refer to the Edit an ACR Manually page for more information.

> **Note:** For customers without Lumin, the ACR is set to 0, and will be reflected accordingly. Leveraging Lumin provides context of the risk per asset, making the vulnerability management program more effective.

Open Vulnerabilities ACR to CVSSv3

Leveraging ACR with CVSS provides an improved risk-based view of the attack surface, and a more accurate representation and prioritization of risk. In the Open Vulnerabilities ACR to CVSSv3 widget, CVSS Base Score is supplemented with ACR. CVSSv3 Base Scores and ACR Scores are used in this heat map with the bottom-right corner containing the most critical concerns. Organizations with a robust vulnerability management program will have the highest counts in the top left portion, indicating that vulnerabilities identified have the least severity, and least potential impact to the organization. Vulnerabilities in the last row and far right column represent the most severe concerns, with the bottom right indicating the highest priority concerns. These numbers can help drive prioritization efforts in compliance with SLAs.

Open Vulnerabilities ACR to CVSSv3

Severity / ACR	Low (ACR 0-3.9)	Medium (ACR 4-6.9)	High (ACR 7-8.9)	Critical (ACR 9-10)
Severity Low	11	134	70	0
Severity Medium	2.29K	1.4K	683	0
Severity High	416	2.44K	1.51K	0
Severity Critical	97	1.02K	587	0

The Common Vulnerability Scoring System (CVSS) is a metric from 0 to 10 that is assigned by the product vendor or the National Vulnerability Database (NVD) to indicate the severity of a vulnerability. CVSS scores are produced by the entity or organization that produces and maintains the product or a third party scoring on their behalf. CVSS Base Scores alone are not a measure of business risk nor do CVSS values account for real-world risk or asset criticality within an organization's specific environment as scores are not likely to change once published.

Tenable recommends supplementing CVSS Base Scores with another temporal or environmental score to more accurately measure severity and rank threats. Such factors may include the risk of monetary loss due to breach, risks of damage or threat to life or property.

Temporal metrics are metrics that change over time. Factors that can alter the Temporal score are: Exploit Code Maturity, Remediation Level, and Report Confidence. If a vendor has created a patch that is widely available, the Temporal score will be lower, likewise if known exploits are widely available, the score will be higher. Environmental metrics are specific to the organization, and include attributes related to business criticality of the exposed asset, and any mitigation measures or compensating controls that are in place. Organizations can modify Environmental attributes if compensating controls are in place, thereby modifying the overall CVSS Score. The core concern is that incorrectly used Environmental score changes will have a significant impact. For example:

A vulnerability with a CVSS Base Score of 9.9 (Critical) and a CVSS Temporal Score of 9.9 (also Critical) will have an overall score of 9.9. Combine these scores with CVSS Environmental score of 3.2 and the Overall Score will be reduced to 3.2 (Low). This is an extreme example, but illustrates what may occur if the CVSS Environmental score is modified incorrectly.

These critical pieces of information are included in ACRs, and help organizations to effectively prioritize remediation and enhance CVSS Base scores.

Vulnerability Management

Exploitability data for various exploit frameworks, including attack vectors, are presented in this section. Exploits leveraged in attacks are imported into various tools and services when the attack is made public. A license to use common exploit frameworks is easy to obtain and is used by security researchers and malicious attackers alike. The primary difference is that some tools require a considerable initial licensing cost to be useful, and others, such as Metasploit, may be freely available to the general public. This section describes risks associated with vulnerabilities that are included in exploit frameworks.

Exploitation frameworks, such as Metasploit, Canvas, and others, are designed to detect and exploit software and hardware vulnerabilities in target systems. These frameworks are powerful tools that enable penetration testers to probe and test devices for flaws and vulnerabilities. Often, these tools are used by those with malicious intent to easily compromise a target asset. Exploit frameworks do not require a high degree of technical knowledge to use. Open Source frameworks, such as Metasploit, are freely available and have the potential to carry more risk than a closed source costly

alternative framework since they are readily available to download. Exploits in the frameworks that require significant initial cost, such as Canvas or Core, have the potential to carry less risk than the same number of exploits available with Metasploit.

Exploitability by Framework

The **Exploitability by Framework** widget provides a summary of exploitable vulnerabilities by framework. This widget determines risks that may require prioritization over other vulnerabilities, by displaying vulnerabilities that can be exploited by a specific framework.

Each row in the widget focuses on a specific framework, except for the first two rows. The first row of the widget includes all exploit frameworks. However the “Exploitability Ease” property can be set to any plugin that is known to be exploitable, even when a framework is not used to exploit the vulnerability. The "Malware" property is set when there are vulnerabilities known to be exploited by malware in the wild. The frameworks will often be duplicated, meaning a vulnerability that is exploitable by Metasploit may also be exploitable using Core or Canvas. This is important to understand and recognize that the Exploitable row is not a sum of all the subsequent rows in count, but the plugins covered in the Exploitable row will be covered in the subsequent rows.

Each of the columns in the matrix focus on severity levels using the previously mentioned CVSSv3 ranges, with the exception of the Exploitable column. The Exploitable column is the sum of all severity levels, including the plugins with a CVSSv3 score less than 3.9, where the other columns focus on respective score ranges. Overall the metrics provided in this matrix enable organizations to understand the immediate threat of the vulnerability being present in the network. Should these metrics be present on a large percentage of assets, then the organization has a less mature vulnerability management program.

Exploitable by Framework

Framework / Severity	Exploitable	Critical	High	Medium
Exploitable	4.17K	893	1.77K	280
Malware	2.48K	613	996	101
Core	0	0	0	0
Canvas	612	178	220	43
Elliot	6	0	4	0
ExploitHub	1	0	0	0
Metasploit	888	264	305	1

Exploitability by CVSSv3 Attack Vector

The **Exploitability by CVSSv3 Attack Vector** widget expands on the previous data by adding Attack Vector information to the exploit frameworks. Attack Vectors are part of the Base Metric group related to CVSS scoring and reflect an intrinsic characteristic that does not change over time. Local (AV:L), Network (AV:N), and Adjacent Network (AV:A vectors are displayed, which determine if the vulnerability is locally or remotely exploitable. Exploits that are available to the Network can be exploited remotely from the public internet. These exploits are the most serious threat since the attack vector is the entire internet. Exploits that are Adjacent have a smaller attack vector, since they must be launched from the shared physical or logical network or administrative domain. Exploits that are Local require access from an authorized, non-privileged user. Exploits that require local access are more difficult to carry out since the attacker must first gain access to an authorized account, or trick the authorized user into executing the exploit code.

Exploitability By CVSSv3 Attack Vector

Framework / Vector	Local Vulnerabilities	Network Vulnerabilities	Adjacent Network Vulnerabilities
Exploitable Vulnerabilities	667	2.22K	69
Metasploit Exploits	125	422	23
Core Exploits	0	0	0
Canvas Exploits	100	341	0
Malware Exploits	0	0	0

SLAs and Remediation

Vulnerability Management Service Level Agreements (SLAs) often change from one organization to the next, however meeting these SLAs is a common issue among organizations industry wide. SLAs

define an expected level of service by which measurements, metrics, or penalties can be established. SLA compliance is a critical component of a vulnerability management program.

There is no set timetable to resolve vulnerabilities that fits every situation. SLAs can vary from organization to organization, and even vary between business units within the organization. Tenable recommends aligning SLAs with technology or business objectives, starting with the most important assets. The Department of Homeland Security has made available 10 resource guides to help organizations implement business practices to reduce cyber risk. Volume 4: Vulnerability Management provides guidance for organizations to work with stakeholders to develop remediation timeframes that align with business goals.

As vulnerabilities are identified, remediation must be prioritized and tracked. Reviewing remediated vulnerabilities and the remediation time frame provides valuable information to the organization on the success of the risk remediation program.

Vulnerability SLA Widget

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

Vulnerabilities SLA

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

Outstanding Remediations

The time between when a vulnerability is discovered and when the vulnerability is typically exploited; called the 'time to exploit' is rapidly decreasing. The CISA INSIGHTS report titled Remediate Vulnerabilities for Internet-Accessible Systems notes that adversaries are able to exploit a vulnerability within 15 days, on average. This is down from a previous average of over 30 days the previous year. For organizations this means that patching must be a priority to reduce threat as unpatched vulnerabilities over 15 days old begin to present a significant risk.

The **Outstanding Windows Remediations** and the **Vendor/Open Source Outstanding Remediations** widgets use plugin families along with patch publication date filters to communicate the presence of vulnerabilities in the network. The time frame shown are the days since a patch or other mitigation was offered by the software vendor, and not the time the vulnerability has affected the asset. The exploitable column denotes the vulnerability counts in combination with CVSSv3 rating, while the severity based column focuses on the CVSSv3 score only. This distinction is important as not all vulnerabilities are known to be exploitable.

Vendor/Open Source Outstanding Remediations

Days / Severity	Exploitable	Critical	High	Medium	Low
< 30	0	0	0	0	0
31-90	0	2	3	0	0
91-180	1	4	22	4	0
>181	1.09K	814	2.28K	1.28K	102

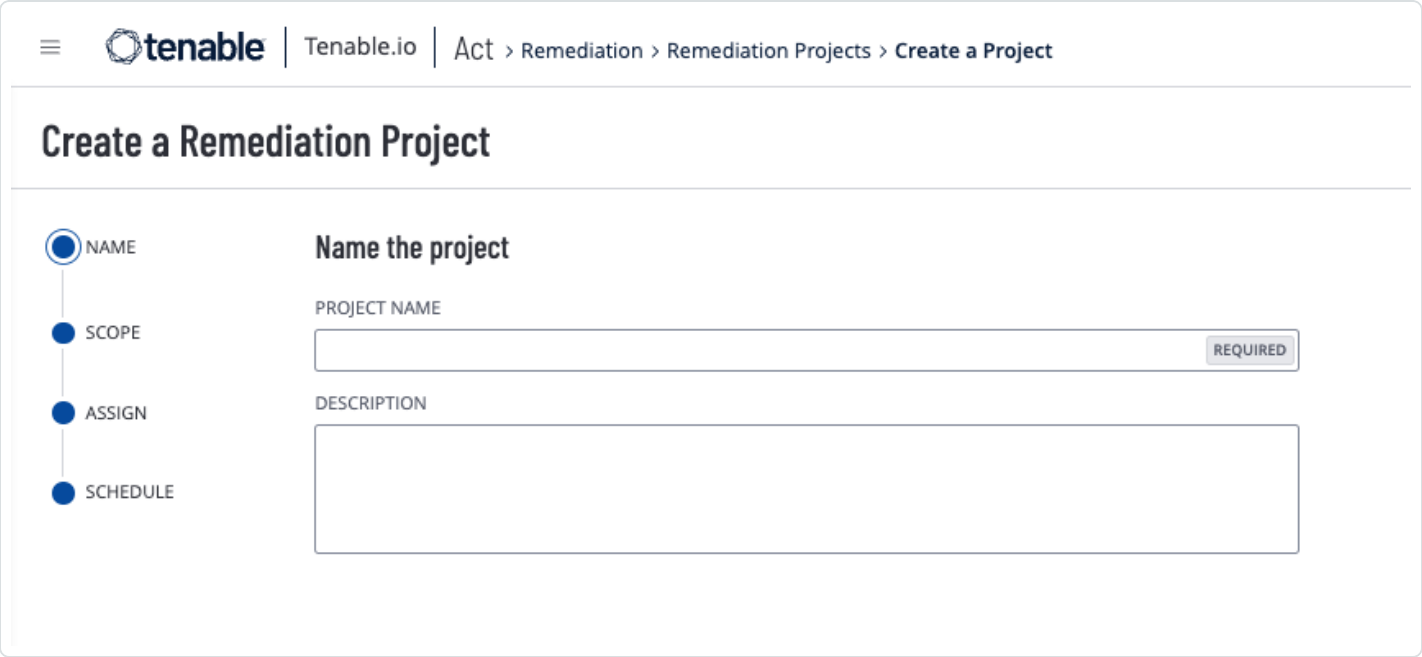
Outstanding Windows Remediations

Days / Severity	Exploitable	Critical	High	Medium	Low
< 30	14	18	4	0	0
31-90	27	18	24	8	15
91-180	44	16	39	6	0
>181	2.87K	708	1.82K	264	27

Unpatched assets expose organizations to vulnerabilities that could be exploited. As new assets are added to the network, and scanned for the first time, the system shows counts for vulnerabilities with known patches available. As new assets are detected, any related vulnerabilities have not been present in the network for a long time, but a patch has been available that has not been applied yet. Organizations with a mature vulnerability management process will address these concerns during the initial build process.

Assets with the largest number of missing patches typically represent a higher level of remediation effort and may be the most time-consuming to address. Vulnerability severity, exploitability, and time since patch availability age are displayed as the key points of vulnerability management. Organizations with an effective vulnerability management program will typically patch within 90 days of the date the patch is made available, and usually will have lower counts in the last two rows of these matrices. These organizations will most likely only have data presented in the first row (under 30 days), especially for the highest severity vulnerabilities.

Assets that are exploitable or have a higher severity rating represent a fast lane for attackers. Prioritizing remediation of these vulnerabilities is an effective strategy to reduce risk. Tenable has provided a method to create a Remediation Project so findings can be prioritized, scope of work can be defined, projects can be assigned, and progress can be tracked. Remediation projects can be set to be completed at a fixed date, or within a specified timeframe.



More information on the creation , viewing, editing, closing, or suspending of remediation projects can be found on the Remediation Projects page of the Tenable documentation. Remediation projects that are created within Tenable Vulnerability Management can also be exported as a .csv for use outside of Tenable Vulnerability Management.

Learn More

Tenable Resources

- Tenable Compliance and Audit Files
- Tenable Cyber Exposure Studies

External Resources

- **Triple I Blog :** CISA Releases Long-Awaited Plan For National Cyber Resilience
- **CISA:** CISA Strategic Plan
- **CISA:** CRR Supplemental Resources Guides
- **CISA:** CISA INSIGHTS: Remediate Vulnerabilities for Internet-Accessible Systems
- **CISA:** Alerts
- **ENISA:** Risk Management