



## How-to Guide: Tenable.sc for CyberArk

---

Last Updated: February 05, 2020

---

# Table of Contents

<b>How-to Guide: Tenable.sc for CyberArk</b> .....	<b>1</b>
<b>Welcome to Tenable.sc for CyberArk</b> .....	<b>3</b>
<b>Integrations</b> .....	<b>4</b>
Windows Integration .....	5
Database Integration .....	9
Add the Credential to the Scan .....	13
<b>SSH (Privilege Escalation) Integration</b> .....	<b>17</b>
<b>Additional Information</b> .....	<b>22</b>
CyberArk Domain and DNS Support .....	23
Tenable.sc Priority Scanning for CyberArk .....	24
Retrieving Addresses to Scan from CyberArk .....	25
Debugging CyberArk .....	26
About Tenable .....	27

---

# Welcome to Tenable.sc for CyberArk

---

This document provides information and steps for integrating Tenable Tenable.sc with CyberArk Enterprise Password Vault (CyberArk).

Security administrators know that conducting network vulnerability assessments means getting access to and navigating an ever-changing sea of usernames, passwords, and privileges. By integrating CyberArk with Tenable.sc, customers have more choice and flexibility.

The benefits of integrating Tenable.sc with CyberArk include:

- Credential updates directly in Tenable.sc, requiring less management.
- Reduced time and effort documenting where credentials are stored in the organizational environment.
- Automatic enforcement of security policies in specific departments or business unit requirements, simplifying compliance.
- Reduced risk of unsecured privileged accounts and credentials across the enterprise.

---

# Integrations

---

Configure CyberArk with either Windows or SSH. Click the corresponding link to view the configuration steps.

[Windows Integration](#)

[SSH Integration](#)

# Windows Integration

To configure Windows integration:

1. Log in to Tenable.sc.
2. In the top navigation bar, click **Scanning**.

A menu appears.

The screenshot shows the Tenable SecurityCenter dashboard. The top navigation bar includes 'Dashboard', 'Analysis', 'Scans', 'Reporting', 'Assets', 'Workflow', and 'Users'. The 'Scans' menu is open, showing options: 'Active Scans', 'Agent Scans', 'Scan Results', 'Policies', 'Audit Files', 'Credentials', and 'Blackout Windows'. The 'Credentials' option is highlighted with a red box. The dashboard displays three main sections: 'Executive 7 Day - Current Vulnerability Type Matrix', 'Executive 7 Day - Exploitable Vulnerability Type Matrix', and 'Executive 7 Day - Mitigated Vulnerability Type Matrix'. Each section includes a table of vulnerability counts and a pie chart showing the distribution by severity (Critical, High, Medium, Low, Info). The 'Current Vulnerability Type Matrix' table shows 55 Critical, 70 High, and 568 Medium vulnerabilities. The 'Exploitable Vulnerability Type Matrix' table shows 67% Exploit %, 24% Metasploit, 43% Core Impact, 24% Canvas, and 24% Malware. The 'Mitigated Vulnerability Type Matrix' table shows 0% for all categories. The 'Current Vulnerability Summary by Severity' pie chart shows a high percentage of Medium severity vulnerabilities. The 'Exploitable Vulnerability Summary by Severity' pie chart shows a high percentage of High severity vulnerabilities. The 'Previously Mitigated Vulnerability Trend' section is currently empty.

3. Click **Credentials**.

The **Credentials** page appears.

SecurityCenter SC Dashboard Analysis Scans Reporting Assets Workflow Users qahead

### Credentials

+ Add

Active Scans Agent Scans Scan Results Policies Audit Files **Credentials** Blackout Windows

Name	Tag	Type	Group	Owner	Last Modified
CyberArk Windows		Windows	Full Access	qahead	4 hours ago
CyberArk SSH		SSH	Full Access	qahead	5 hours ago
BeyondTrust SSH		SSH	Full Access	qahead	4 hours ago
BeyondTrust Windows		Windows	Full Access	qahead	4 hours ago
bt - edit - edit - agin		SSH	Full Access	qahead	1 hour ago
another bt		SSH	Full Access	qahead	4 hours ago
password - edit		SSH	Full Access	qahead	1 hour ago

4. Click **+Add** at the top of the screen.

SecurityCenter SC Dashboard Resources Repositories Organizations Users Scanning System Admin User

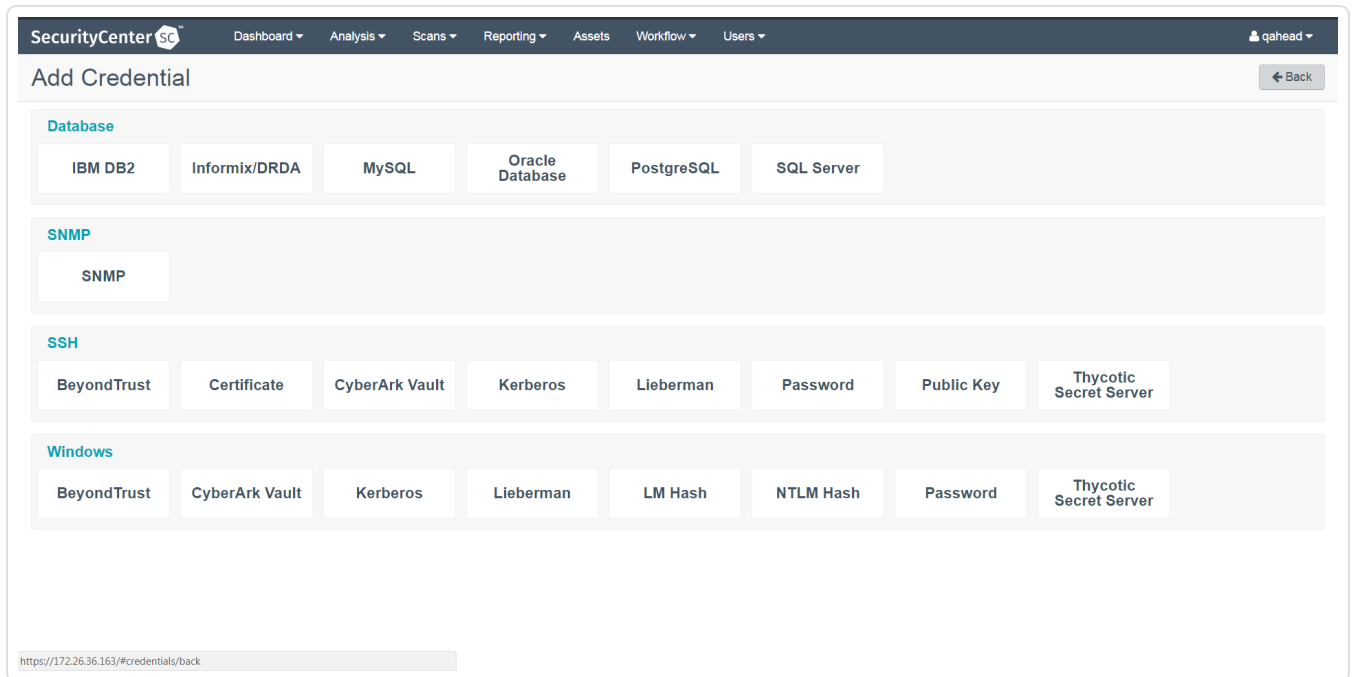
### Credentials

+ Add

Policies Audit Files **Credentials**


The **Add Credential** page appears.

5. In the **Windows** section, click **CyberArk Vault**.



The **Add Credential** page appears.

6. Configure each field for **Windows** authentication. See the [Tenable.sc User Guide](#) to get detailed descriptions for each option.

SecurityCenter  Dashboard ▾ Analysis ▾ Scans ▾ Reporting ▾ Assets Workflow ▾ Users ▾ qahead ▾

## Add Credential ← Back

### General

Name\*

Description

Tag

### CyberArk Vault Credential

Username\*

Domain

Central Credential Provider URL Host\*

Central Credential Provider URL Port\*

Vault Username

Vault Password

Safe\*

CyberArk Client Certificate

CyberArk Client Certificate Private Key

CyberArk Client Certificate Private Key passphrase

AppID\*

Folder\*

PolicyID

CyberArk Account Details Name

Vault Use SSL

Vault Verify SSL

CyberArk AIM Service URL

**Caution:** Tenable strongly recommends encrypting communication between the Tenable.sc scanner and the CyberArk AIM gateway using HTTPS and/or client certificates. For information on securing the connection, refer to [Tenable.sc User Guide](#) and the **Central Credential Provider Implementation Guide** located at [cyberark.com](https://cyberark.com) (login required).

- Click **Submit**.
- Next, follow the steps for [adding the credential to a scan](#).

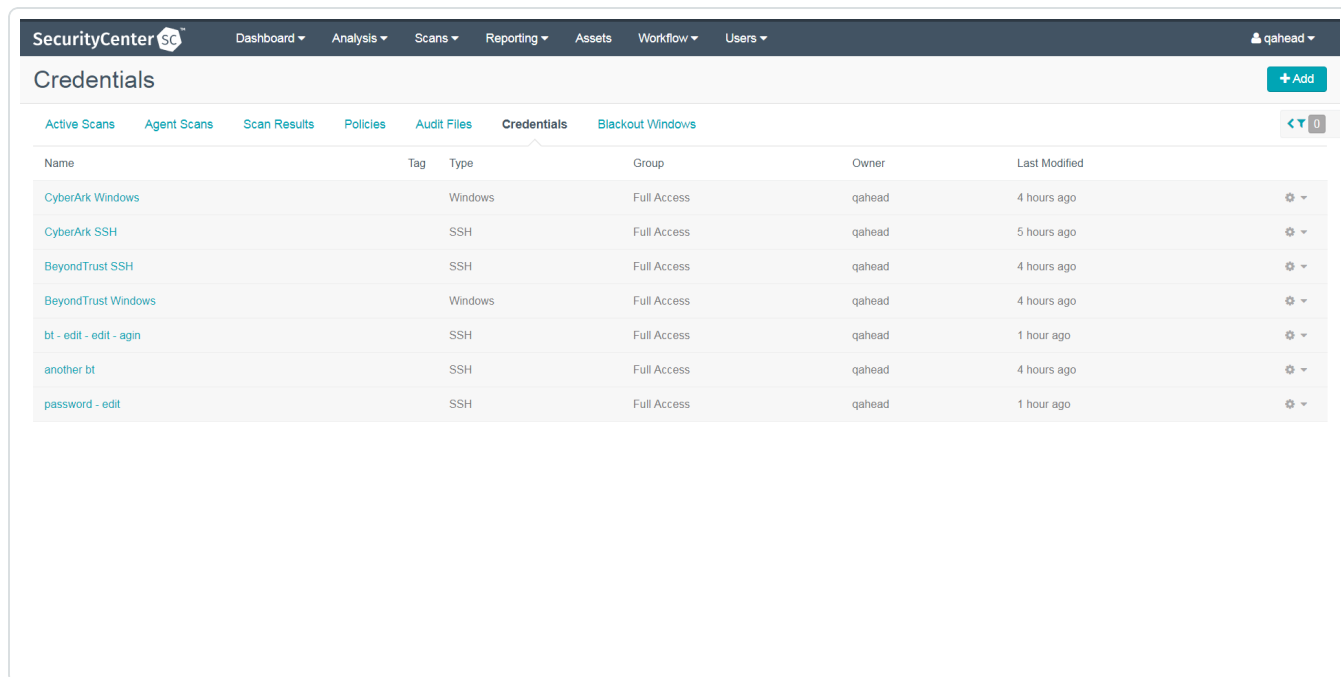


# Database Integration

To configure database integration:

1. Log in to Tenable.sc.
2. In the top navigation bar, click **Scans > Credentials**.

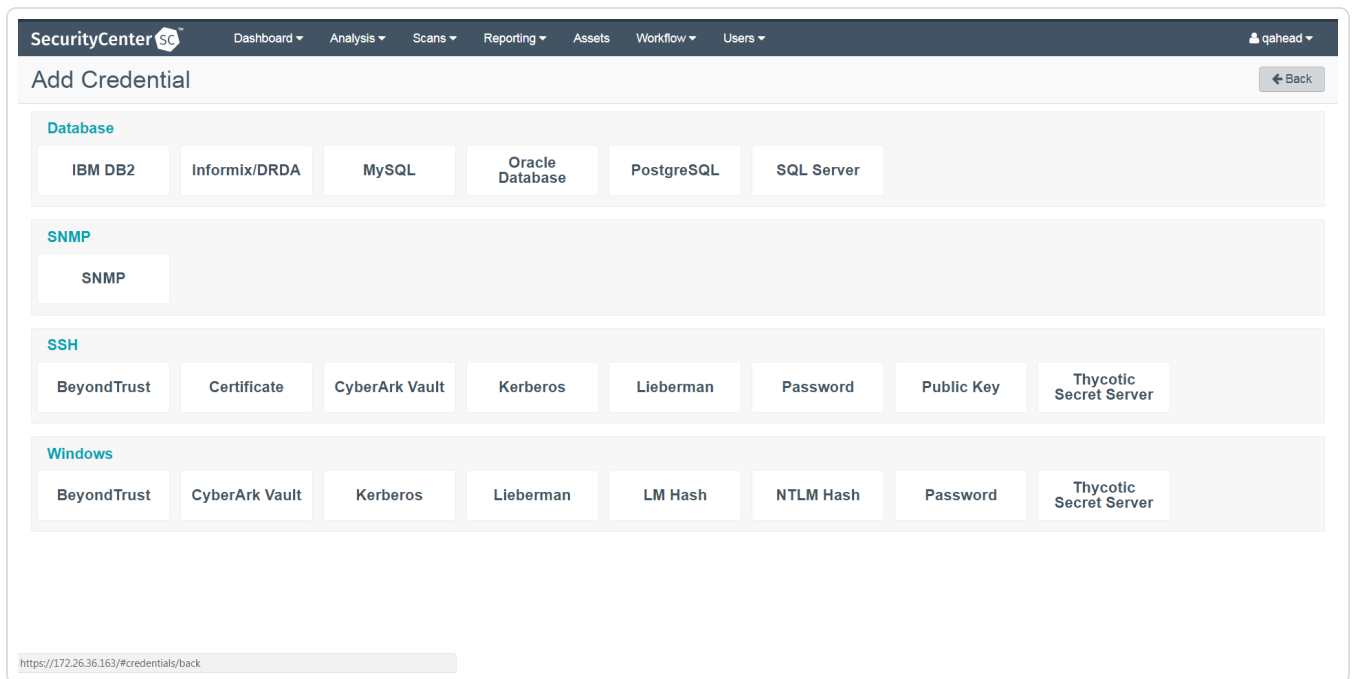
The **Credentials** page appears.



3. In the top right corner, click **+Add**.

The **Add Credential** page appears.

4. In the **Database** section, click **Oracle Database**.



The **Add Credential** page appears.

5. Enter a descriptive **Name**.
6. (Optional) Enter a **Description**.
7. (Optional) Select a **Tag**.
8. In the **Oracle Database Credential** section, select **CyberArk**.

The **CyberArk** field options appear.

tenable.sc
Admin User

Dashboard Resources Repositories Organizations Users Scanning System
← Back

### Add Credential

#### General

Name\*

Description

Tag

#### Oracle Database Credential

Authentication Method

Username\*

Port

Authentication

Service Type

Service

Central Credential Provider URL Host\*

Central Credential Provider URL Port\*

Vault Username

Vault Password

Safe\*

CyberArk Client Certificate

CyberArk Client Certificate Private Key

CyberArk Client Certificate Private Key Passphrase

AppID\*

Folder\*

PolicyID

CyberArk Account Details Name\*

Vault Use SSL

Vault Verify SSL

CyberArk AIM Service URL

9. Configure each field for the **Oracle Database** authentication. See the [Tenable.sc User Guide](#) to view detailed descriptions for each option.

---

**Caution:** Tenable strongly recommends encrypting communication between the Tenable.sc scanner and the CyberArk AIM gateway using HTTPS and/or client certificates. For information on securing the connection, refer to [Tenable.sc User Guide](#) and the **Central Credential Provider Implementation Guide** located at [cyberark.com](https://cyberark.com) (login required).

10. Click **Submit**.

## Next Steps

1. Complete the steps for [adding the credential to a scan](#).

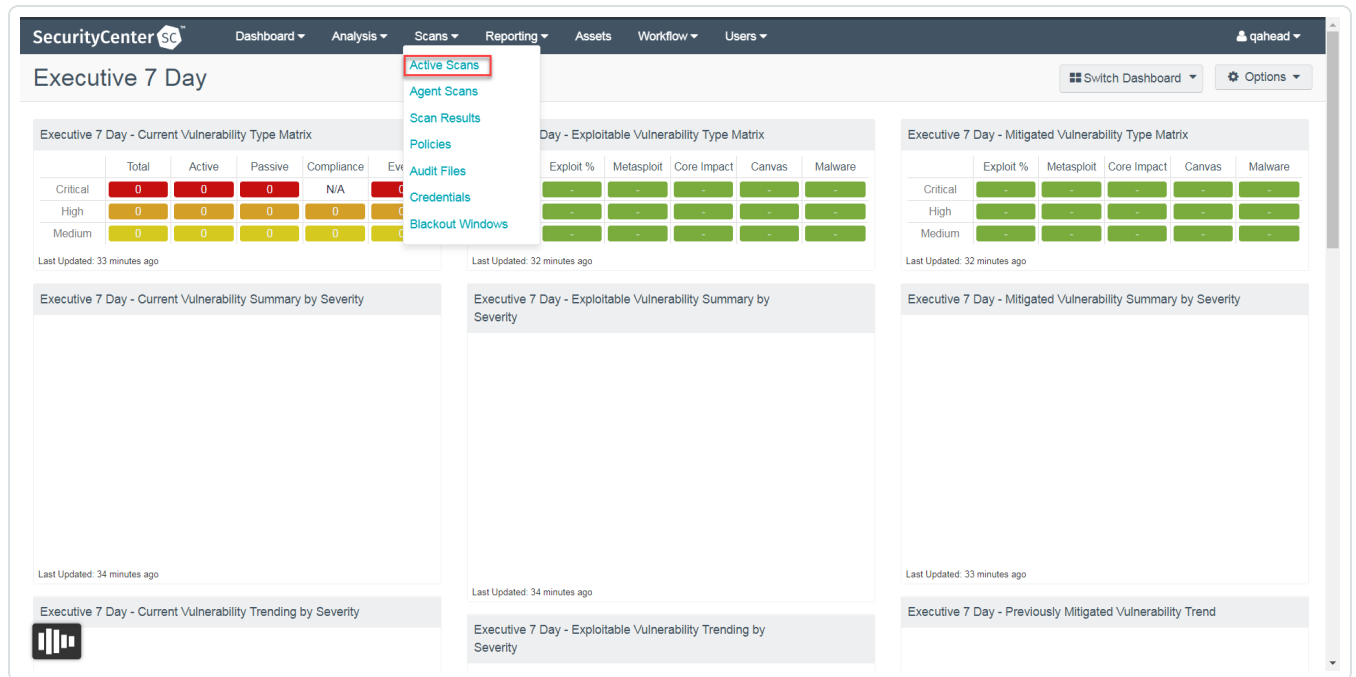
# Add the Credential to the Scan

To add a credential to the scan:

1. In the top navigation bar in Tenable.sc, click **Scans**.

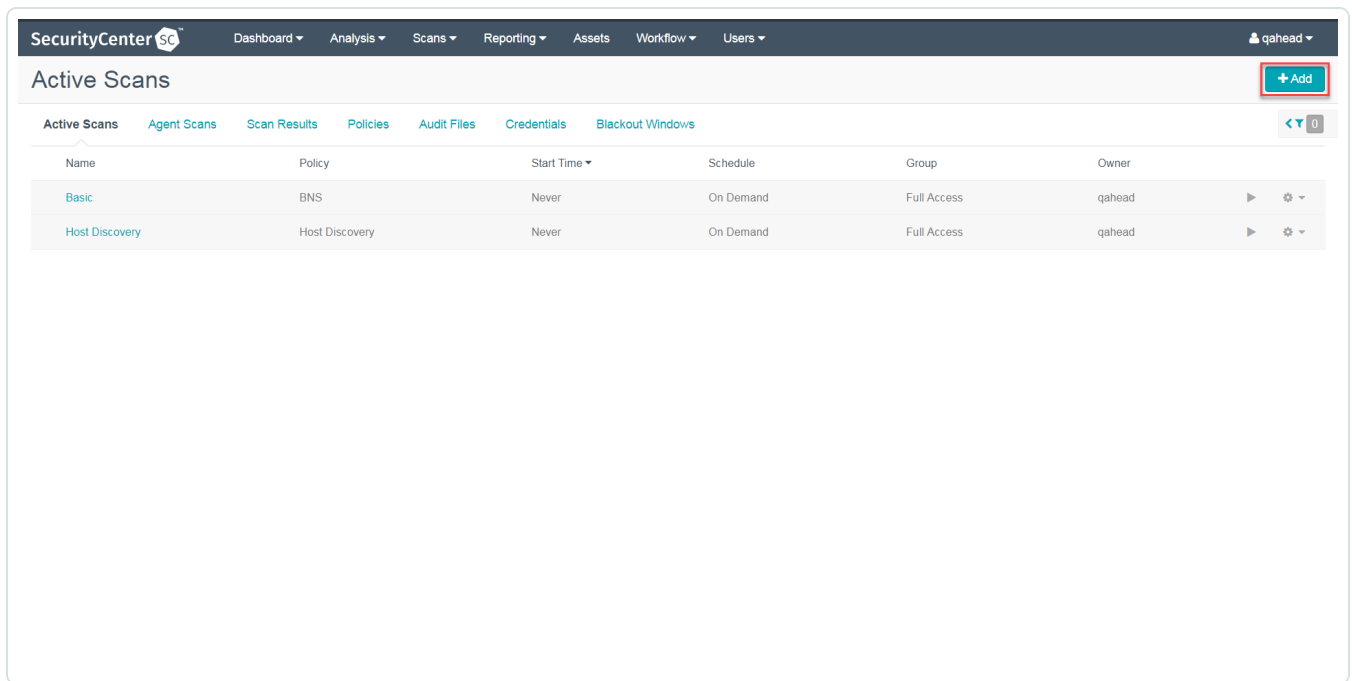
A drop-down menu appears.

2. Select **Active Scans**.



The **Active Scans** window opens.

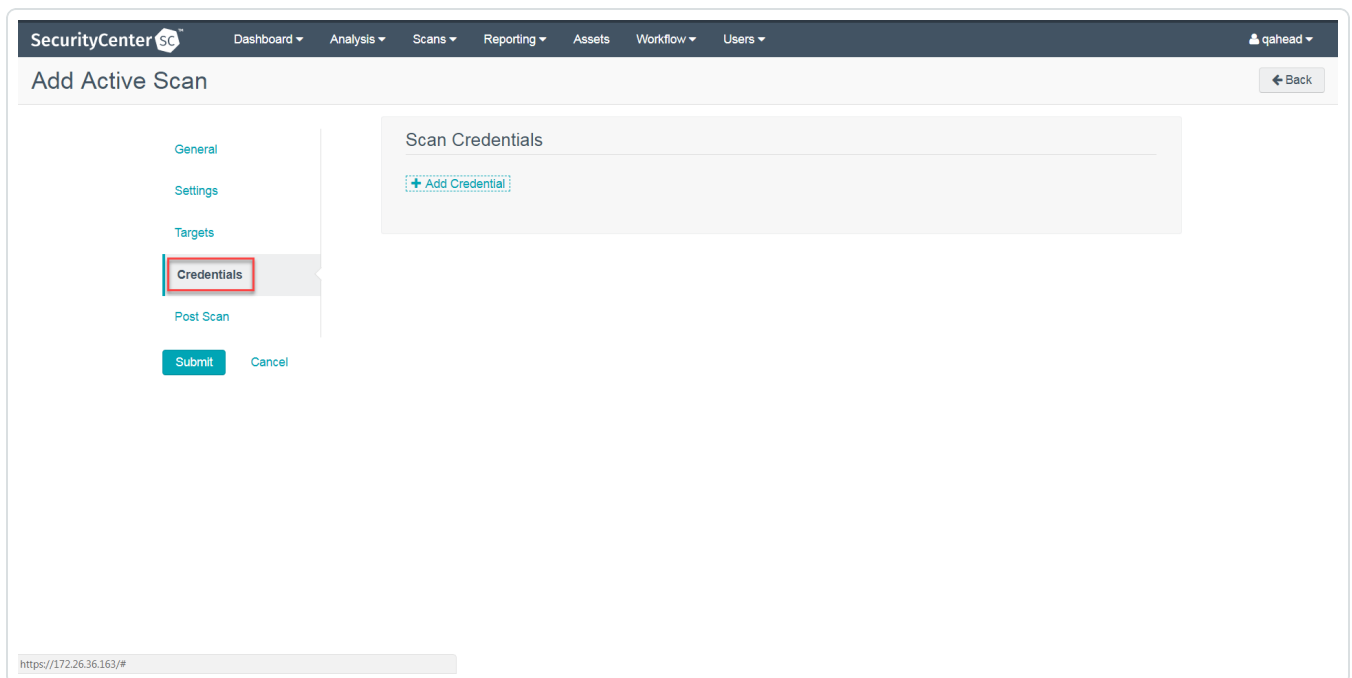
3. In the top right corner, click **+Add**.



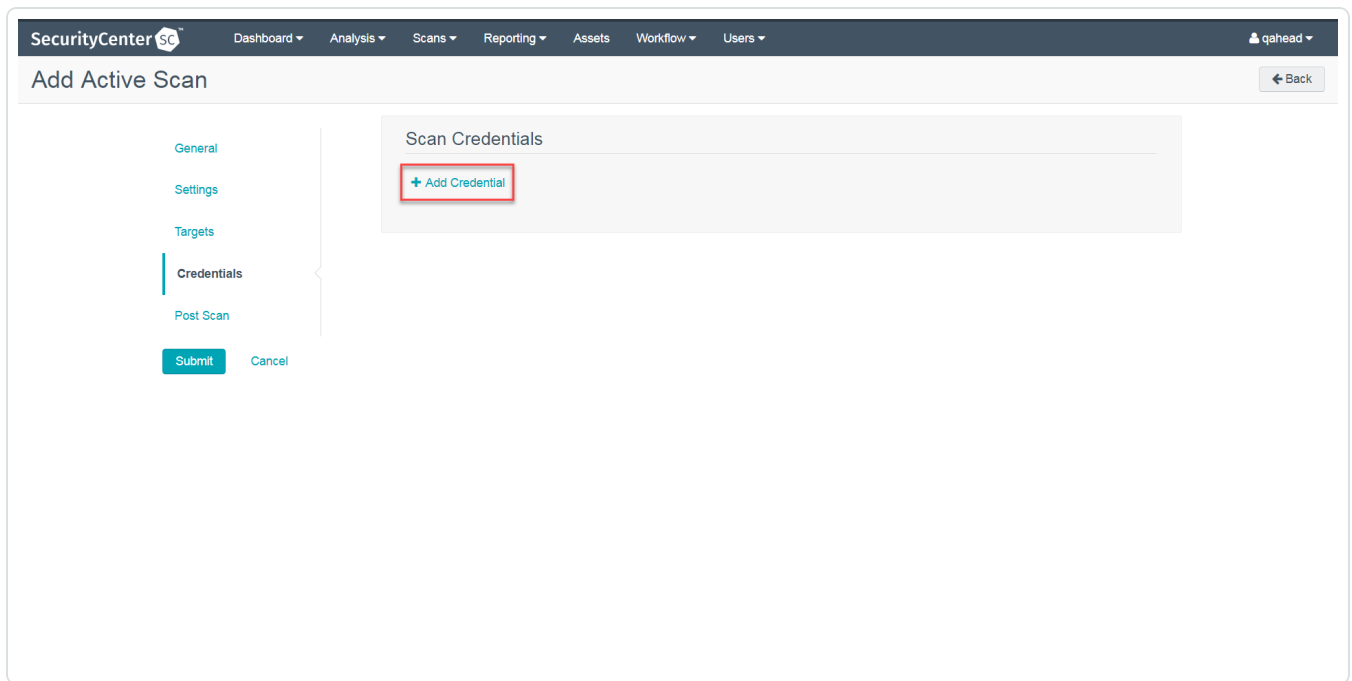
The **Add Active Scan** window opens.

4. In the left column, click **Credentials**.

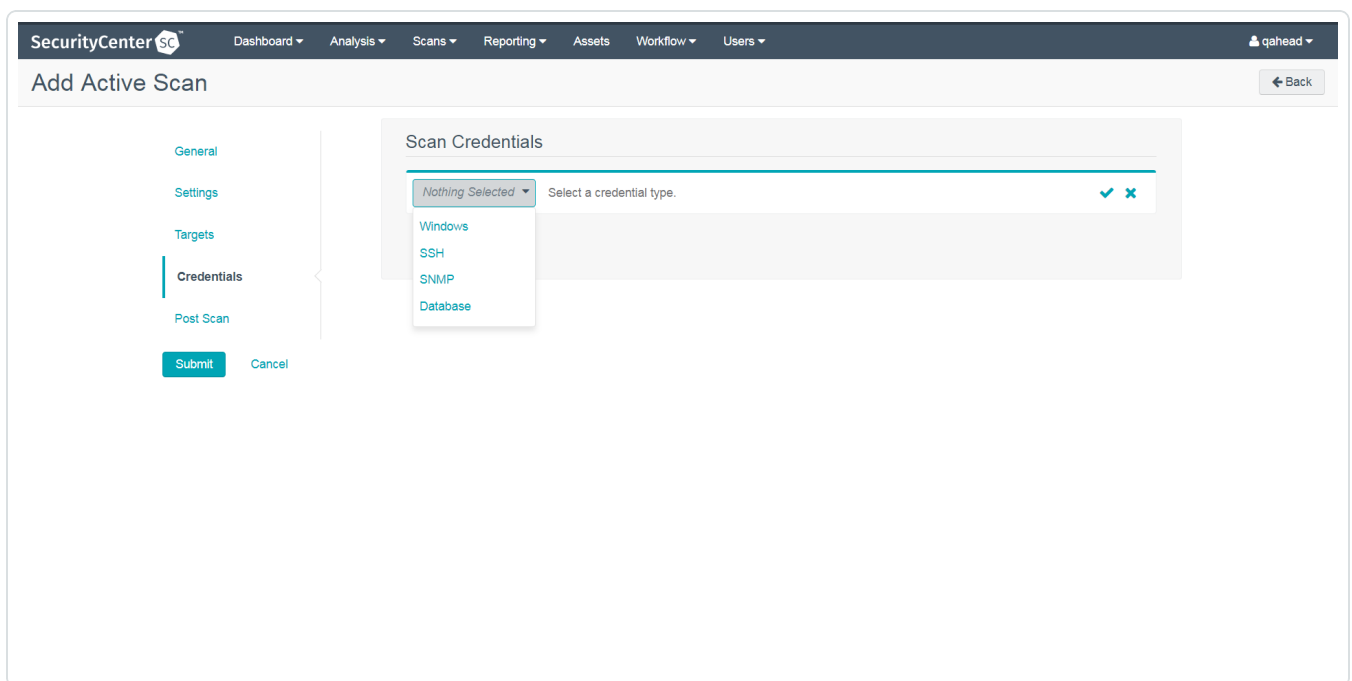
The **Scan Credentials** section appears.



5. In the **Scan Credentials** section, click **+Add Credential**.



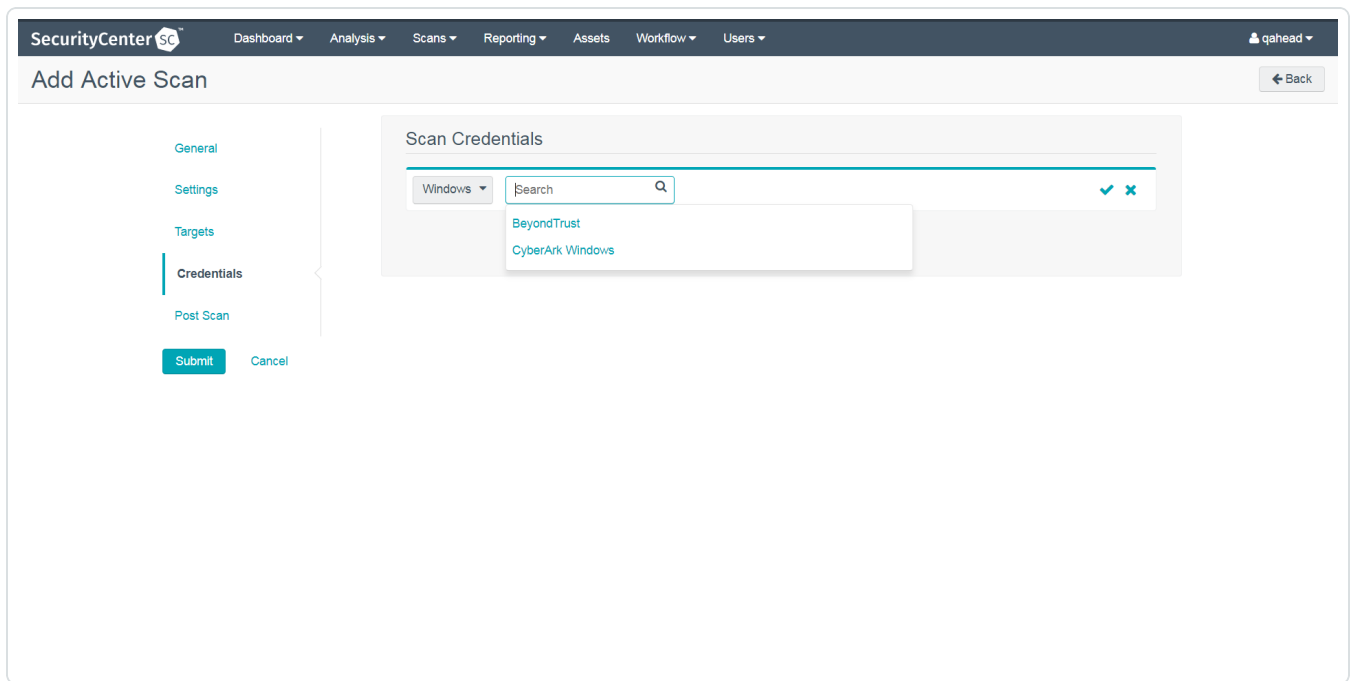
A drop-down appears.



6. Select the system type.

The **Select Credential** option appears.

7. Click **Select Credential**.



A drop-down appears.

8. Select the previously created credential.
9. Enter information for the **General**, **Settings**, **Targets**, and **Post Scan** sections.
10. Click **Submit**.

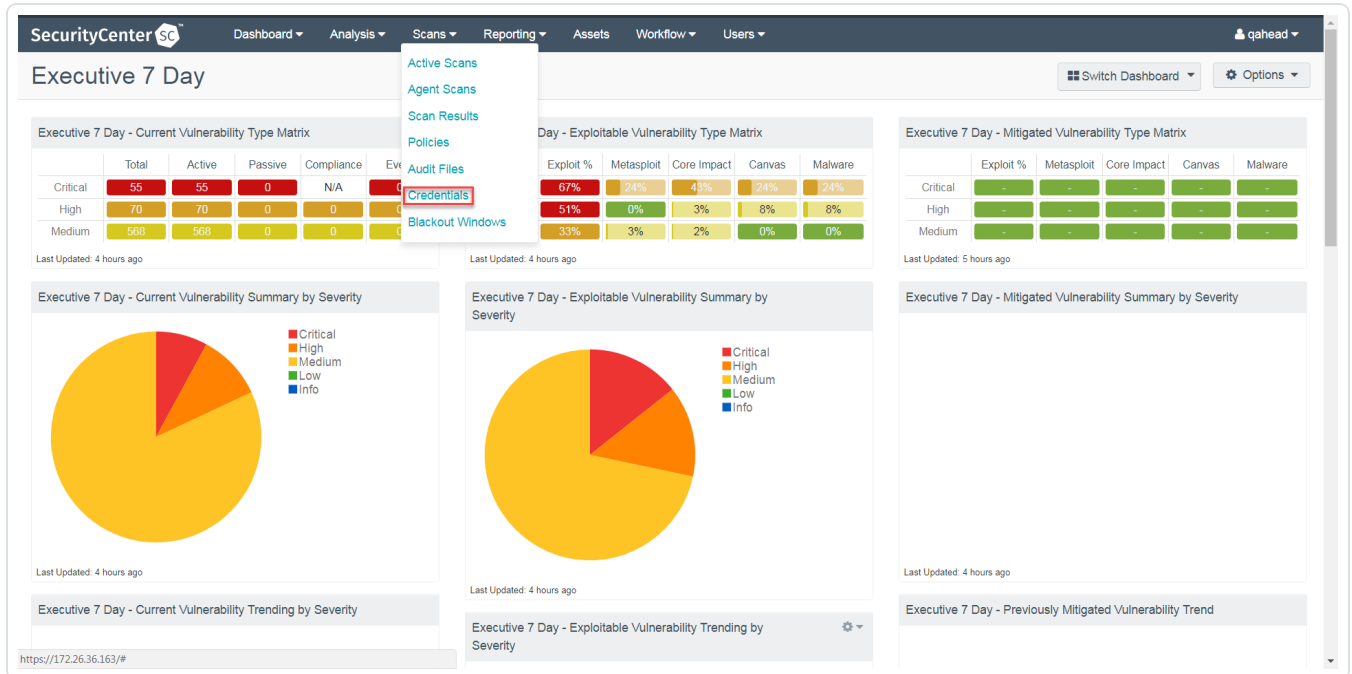


# SSH (Privilege Escalation) Integration

To configure SSH integration:

1. Log in to Tenable.sc.
2. In the top navigation bar, click **Scanning**.

A menu appears.



The screenshot shows the Tenable SecurityCenter dashboard. The top navigation bar includes 'Dashboard', 'Analysis', 'Scans', 'Reporting', 'Assets', 'Workflow', and 'Users'. The 'Scans' menu is open, showing options: 'Active Scans', 'Agent Scans', 'Scan Results', 'Policies', 'Audit Files', 'Credentials', and 'Blackout Windows'. The 'Credentials' option is highlighted with a red box. The dashboard displays three main sections: 'Executive 7 Day - Current Vulnerability Type Matrix', 'Executive 7 Day - Exploitable Vulnerability Type Matrix', and 'Executive 7 Day - Mitigated Vulnerability Type Matrix'. Each section includes a table of vulnerability counts and a pie chart showing the distribution by severity (Critical, High, Medium, Low, Info). The 'Current Vulnerability Type Matrix' table shows 55 Critical, 70 High, and 568 Medium vulnerabilities. The 'Exploitable Vulnerability Type Matrix' table shows 67% Exploit %, 24% Metasploit, 43% Core Impact, 24% Canvas, and 24% Malware. The 'Mitigated Vulnerability Type Matrix' table shows 0% for all categories. The 'Executive 7 Day - Current Vulnerability Summary by Severity' pie chart shows a high percentage of Medium severity vulnerabilities. The 'Executive 7 Day - Exploitable Vulnerability Summary by Severity' pie chart shows a high percentage of Medium severity vulnerabilities. The 'Executive 7 Day - Mitigated Vulnerability Summary by Severity' pie chart shows 0% for all categories. The dashboard also includes 'Executive 7 Day - Current Vulnerability Trending by Severity', 'Executive 7 Day - Exploitable Vulnerability Trending by Severity', and 'Executive 7 Day - Previously Mitigated Vulnerability Trend' sections.

3. Click **Credentials**.

The **Credentials** page appears.

SecurityCenter **SC** Dashboard Analysis Scans Reporting Assets Workflow Users qahead

### Credentials

Active Scans Agent Scans Scan Results Policies Audit Files **Credentials** Blackout Windows

Name	Tag	Type	Group	Owner	Last Modified
CyberArk Windows		Windows	Full Access	qahead	4 hours ago
CyberArk SSH		SSH	Full Access	qahead	5 hours ago
BeyondTrust SSH		SSH	Full Access	qahead	4 hours ago
BeyondTrust Windows		Windows	Full Access	qahead	4 hours ago
bt - edit - edit - agin		SSH	Full Access	qahead	1 hour ago
another bt		SSH	Full Access	qahead	4 hours ago
password - edit		SSH	Full Access	qahead	1 hour ago

4. In the SSH section, click **CyberArk Vault**.

SecurityCenter **SC** Dashboard Analysis Scans Reporting Assets Workflow Users qahead

### Add Credential

Database

- IBM DB2
- Informix/DRDA
- MySQL
- Oracle Database
- PostgreSQL
- SQL Server

SNMP

- SNMP

SSH

- BeyondTrust
- Certificate
- CyberArk Vault**
- Kerberos
- Lieberman
- Password
- Public Key
- Thycotic Secret Server

Windows

- BeyondTrust
- CyberArk Vault
- Kerberos
- Lieberman
- LM Hash
- NTLM Hash
- Password
- Thycotic Secret Server

<https://172.26.36.163/#credentials/back>

The **Add Credential** page appears.

# Add Credential

← Back

**General**

Name\*

Description

Tag

**CyberArk Vault Credential**

Username\*

Privilege Escalation

Central Credential Provider URL Host\*

Central Credential Provider URL Port\*

Vault Username

Vault Password

Safe\*

CyberArk Client Certificate

CyberArk Client Certificate Private Key

CyberArk Client Certificate Private Key passphrase

AppID\*

Folder\*

**CyberArk Vault Credential**

Username\*

Privilege Escalation

Central Credential Provider URL Host\*

Central Credential Provider URL Port\*

Vault Username

Vault Password

Safe\*

CyberArk Client Certificate

CyberArk Client Certificate Private Key

CyberArk Client Certificate Private Key passphrase

AppID\*

Folder\*

PolicyID

CyberArk Account Details Name

Vault Use SSL

Vault Verify SSL


CyberArk AIM Service URL

5. In the **CyberArk Vault Credentials** section, click **Privilege Escalation**.

The **Privilege Escalation** options appear.

**Note:** Multiple options for Privilege Escalation are supported, including *su*, *su+sudo* and *sudo*. If *sudo* is selected, additional fields for **sudo user**, **CyberArk Account Details Name** and **Location of sudo** (directory) are provided and can be completed to support authentication and privilege escalation through CyberArk. See the [Tenable.sc User Guide](#) for additional information about the supported privilege escalation types and their accompanying fields.

The screenshot shows the 'Add Credential' form in the SecurityCenter interface. The form is divided into two main sections: 'General' and 'CyberArk Vault Credentials'. The 'Privilege Escalation' dropdown menu is open, showing options: 'None', 'su', 'su+sudo', and 'sudo'. The 'General' section includes fields for Name, Description, and Tag. The 'CyberArk Vault Credentials' section includes fields for Username, Privilege Escalation (set to 'None'), Central Credential Provider URL Host (vault\_host.yourcompany.com), Central Credential Provider URL Port (443), Vault Username, Vault Password, Safe, CyberArk Client Certificate (Choose File), CyberArk Client Certificate Private Key (Choose File), CyberArk Client Certificate Private Key passphrase, AppID (Nessus), Folder (root), PolicyID, CyberArk Account Details Name, Vault Use SSL (toggle), Vault Verify SSL (toggle), and CyberArk AIM Service URL. At the bottom, there are 'Submit' and 'Cancel' buttons.

- 
- 
6. Configure each field for **SSH** authentication. See [Tenable.sc User Guide](#) to get detailed descriptions for each option.
  7. Click **Submit**.
  8. Next, follow the steps for [adding the credential to a scan](#).

---

## Additional Information

---

[CyberArk Domain and DNS Support](#)

[Tenable.sc Priority Scanning for CyberArk](#)

[Retrieving Addresses to Scan from CyberArk](#)

[Debugging CyberArk Issues](#)

---

## CyberArk Domain and DNS Support

---

Tenable's support for CyberArk allows Tenable.sc to use its target list to query CyberArk Enterprise Password Vault for the target system's credentials, and Tenable.sc can use a flexible system to allow for DNS and domain support. See [Tenable.sc Priority Scanning for CyberArk](#) for explanation of the logic used by Tenable.sc for scans using credentials from CyberArk Enterprise Password Vault.

---

# Tenable.sc Priority Scanning for CyberArk

---

Tenable.sc sets a priority system that allows for flexible querying. The following describes the order Tenable.sc tries values and the logic behind it.

1. Tenable.sc queries CyberArk with the target value entered into the Tenable.sc **Targets** configuration field. For example, if you put a FQDN in the target list, Tenable.sc will query CyberArk with the address value of the FQDN. If you enter an IP address or range such as 192.168.1.1-20, Tenable.sc tries to query using the IP address or IP range of the target system(s) in the CyberArk **Address** value. If the target system uses FQDN and can be resolved, then is contacted.
2. If the target value fails, Tenable.sc looks to see if there is a domain value (for a Windows system). If a domain value is present, Tenable.sc queries CyberArk using the domain value for the address value to attempt to use domain credentials.
3. If the configured target value and the domain value both fail, Tenable.sc pulls the IP address of the system. If the IP address does not match one of the IP addresses supplied in the target list, Tenable.sc then queries CyberArk using the IP address of the target itself. This is checked against the target value in the configuration to prevent querying CyberArk twice with the same value.



---

# Retrieving Addresses to Scan from CyberArk

---

Tenable.sc is able to use a feature in CyberArk to pull a list of targets to scan. Below is a description of how to pull the target system values and how to use them.

**Note:**The following method of target address retrieval cannot be done from the default administrator account. You must create an account that is a member of the PVWAMonitor group to generate the following reports.


1. Click on **Report** at the top of the CyberArk Enterprise Password Vault web interface.
2. Click **Generate Report** at the top of the Report page.
3. Choose **Privileged Account Inventory**.
4. Click **Next**.
5. Specify the search parameters for the systems you want to scan.
6. Click **Next**.
7. Click **Finish**.
8. Download the CSV or XLS report.
9. Confirm the targets for Tenable.sc to scan.
10. Confirm the values can all be resolved by Tenable.sc.
11. Copy the values from the **Target system address** column.
12. Enter the values into Tenable.sc. Either:
  - a. Paste the values from addresses into the target list in Tenable.sc.
  - b. Paste the values into a file and use a file target list in Tenable.sc.

---

# Debugging CyberArk

---

To enable debugging when you configure a scan in Tenable.sc:

1. In Tenable.sc, click **Scans > Active Scans**.
2. In the row for the scan where you want to run a diagnostic scan, click the  menu.  
The actions menu appears.
3. Click **Run Diagnostic Scan**.

If a debug output for the system exists in the debug log, one or more of the following files will be present:

- `logins.nasl`: Used for Windows credentials. Shows higher level failures in Windows authentication
- `logins.nasl-CyberArk`: Used to output specific CyberArk-related debug information
- `ssh_settings`: Used for SSH credentials. Shows higher level failures in SSH authentication
- `ssh_settings~CyberArk`: Used to output specific CyberArk-related debug information

---

## About Tenable

---

Tenable transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats, and reduces exposure and loss. With more than one million users and more than 20,000 enterprise customers worldwide, organizations trust Tenable for proven security innovation. Tenable's customers range from Fortune Global 500 companies, to the U.S. Department of Defense, to mid-sized and small businesses in all sectors, including finance, government, healthcare, higher education, retail, and energy. Transform security with Tenable, the creators of Nessus and leaders in continuous monitoring, by visiting [tenable.com](https://tenable.com).