Lumin Exposure View User Guide

Last Revised: June 28, 2023

Table of Contents

Welcome to Tenable One Lumin Exposure View

The Tenable One Exposure Management Platform helps organizations gain visibility across the modern attack surface, focus efforts to prevent likely attacks and accurately communicate cyber risk to support optimal business performance.

The platform combines the broadest vulnerability coverage spanning IT assets, cloud resources, containers, web apps and identity systems, builds on the speed and breadth of vulnerability coverage from Tenable Research and adds comprehensive analytics to prioritize actions and communicate cyber risk. Tenable One allows organizations to:

- Gain comprehensive visibility across the modern attack surface
- Anticipate threats and prioritize efforts to prevent attacks
- Communicate cyber risk to make better decisions

Tip: For additional information on getting started with Tenable One products, check out the Tenable One Deployment Guide.

Tenable One is a package that includes the following products:

Product	Tenable One Package
Tenable Vulnerability Management	Tenable One Standard, Tenable One Enterprise
Tenable Cloud Security	Tenable One Standard, Tenable One Enterprise
Tenable Web App Scanning	Tenable One Standard, Tenable One Enterprise
Lumin Exposure View	Tenable One Standard, Tenable One Enterprise
Tenable Identity Exposure	Tenable One Standard, Tenable One Enterprise
Asset Inventory	Tenable One Standard, Tenable One Enterprise
Attack Path Analysis	Tenable One Enterprise
Tenable.asm	Tenable One Enterprise

What to expect in this guide:

This user guide covers the following interfaces, which can be used alone or in tandem to support these common use cases:

User Type	Use Case
CISO/Executives	Utilize the Lumin Exposure View to: • Quickly quantify your overall enterprise risk exposure and identify which areas need further investigation. • Create custom exposure cards to view data based on specific business contexts. • Measure and prioritize risk exposure progress or regression. • Easily communicate important risk information to teams and include in presentations. • Understand how effective your program is via the **Remediation Maturity** metric.
Security Practitioner	Utilize the Attack Path Analysis section to: • Evaluate the impact of insecure assets and communicate these insecurities to appropriate parties. • Proactively identify hidden security issues within my assets and their relationships.
Both CISO/Executives and Security Practitioners	Utilize the Asset Inventory to: • Utilize existing tags or create new tags that can be used to create custom exposure cards. • View and manage all assets, regardless of their source. **Note:** You must purchase an additional upgrade to access the Asset Inventory interface. Contact your Tenable representative for more information.

For more information, see Get Started with Lumin Exposure View.

Get Started with Lumin Exposure View

Tenable recommends following these steps to get started with Tenable One data and functionality.

Tip: For additional information on getting started with Tenable One products, check out the Tenable One Deployment Guide.

Prepare

- Familiarize yourself with the Tenable One key terms.
- Familiarize yourself with the categories and data metrics within Tenable One.
- Review the Tenable One Example Workflow.

License, Access, and Log In

- Acquire a license:
    1. Determine the interface that best suits your business objectives. For more information on use cases, see Welcome to Tenable One Lumin Exposure View.
    2. Contact your Tenable representative to purchase the appropriate package.

Configure Lumin Exposure View for Use

- Configure your Lumin Exposure View settings.
- View your data sources.

Assess Your Exposure

Review your CES and perform analysis:

- Access the **Lumin Exposure View**, where you can:
    - View, create, and manage cyber exposure cards.
    - View CES and CES trend data.

- View **Remediation SLA** information.

- View **News** posts related to vulnerability events.

Key Terms

The following key terms apply to the Lumin Exposure View user interface.

Term	Definition
Active Directory (AD)	Attack Path Analysis integrates AD data from Tenable Identity Exposure.
Asset	Any IT or security element in your organization such as user accounts, computers, and software. The **Discover** section represents an asset as a node in the graph.
Asset Exposure Graph	A visualization of an attack path from multiple assets down to one asset.
Asset Exposure Score (AES)	Your Cyber Exposure Score (CES) is an aggregate of the AES for all of your licensed assets. AES values range from 0-1000 and represent an individual asset's relative risk.
Benchmark	A group of scores to which you can compare your scores and assess your performance.
Blast Radius	A visualization of one or more attack paths from one asset to multiple other assets.
CES Trend	A measurement that defines how your CES improves or regresses over time.
Chief Information Security Officer (CISO)	The head of cybersecurity for a company. A CISO can use the Exposure View to quickly quantify the overall enterprise risk exposure, measure its progress or regression over time and easily communicate impact and ROI to key stakeholders.
Cyber Exposure Score (CES)	Your CES quantifies the relative risk of your organization based on the threat exposure and criticality of your licensed assets. CES values range from 0 - 1000, where higher values indicate higher exposure and higher risk.
Data Source	A product that feeds data into Tenable One (for example, Tenable Vul-

	nerability Management).
Evidence	The empirical data from different data sources confirming the feasibility of a Step as part of an attack path.
Exposure Card	A card that represents the incoming data from your configured data sources. Users can create custom cards or use Tenable-provided cards.
Exposure Card View	The section of the Exposure View that includes data about the selected exposure card. This section includes CES, trend, Remediation SLA, and business context information.
Exposure View	A holistic and unified view combining internal and external data sources to provide a complete view of risk in a singular location.
Finding	A feasible implementation of a technique or sub-technique in one or more attack paths that an adversary can leverage. Each finding has a Path Priority Rating (PPR) that determines its urgency and potential impact.
Industry Benchmark	A benchmark based on members of your Tenable-assigned industry which you can compare your scores and assess your performance.
MITRE ATT&CK®	MITRE ATT&CK® is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The MITRE ATT&CK® knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.
Path Priority Rating (PPR)	The priority of a finding. Attack Path Analysis calculates the PPR based on the relative number of attack paths to critical assets. Attack Path Analysis categorizes priority levels as **Low**, **Medium**, **High**, and **Critical**.
Population Benchmark	A benchmark based on members of the entire population to which you can compare your scores and assess your performance.
Query Builder	A customizable visualization of one or more attack paths based on configurable source and target assets.
Query Library	Predefined queries that visualize scenarios of potential attack paths based

	on real-world attacks.
Security Practitioner	A Security Practitioner can use the Asset Inventory to evaluate the impact of unsecured assets, proactively identify hidden security issues in assets relationships, and quickly locate areas where a breach or risk is likely to happen.
Service Level Agreement (SLA)	A control by which you can identify whether assets comply with customer security requirements.
Step	A feasible implementation of a technique or sub-technique in an attack path that an adversary can leverage. The **Discover** section illustrates a step as a "bracket" between two or more assets.
Technique / Sub-Technique	Represents "how" an adversary achieves a tactical goal by performing an action. For example, an adversary can dump credentials to achieve credential access.
Tags	A way to group assets by business context. For example, you can group assets by product, permissions, business owner, etc.
Vulnerability Management (VM)	Attack Path Analysis integrates VM data from Tenable Vulnerability Management and Tenable Security Center.
Web Application Scanning (WAS)	Attack Path Analysis integrates web app scanning data from Tenable Web App Scanning.

Example Workflow

The following scenario describes a common use case where the Lumin Exposure View, Asset Inventory, and Attack Path Analysis interfaces work in conjunction to assist a company in analyzing and prioritizing their data.

Getting Started

Joe logs in and lands on the Workspace landing page, where he can see all of his Tenable products and the Tenable One pages he can access. Since he needs to see his exposure risks globally, he selects **Lumin Exposure View**. Joe then lands on the **Global** Lumin Exposure View, where he can see Vulnerability Management, Tenable Identity Exposure, Tenable Web App Scanning, and Cloud data unified into a single score. He may be wondering, "Which category is driving the score?". For this, in the CES section, he can select **Per Category** > **Computing Resources**, and filter all the data on the page.

As Joe reviews the metrics to prepare for his next executive meeting, he can change the date ranges so that he can see what's changed over time and high level indicators of why the changes occurred. Since there was a significant change in the score last week, he decides to comment on the CES Trend section to ask his coworker, Rachel, for more details.

Prioritize

Now that Joe has a better understanding of the score and which category is driving it, his next question is ”Which business owners (i.e., tags) do we need to chase?”. Now, he can look at the Tag Performance section to quickly see which tags are the highest contributors to his score. This helps Joe prioritize his focus. Again, If he needs more details or has an action item for Rachel, Joe can comment directly on the **Tag Performance** section in the **Exposure View**. Rachel can then drill down into the Tag Details to get further information.

Since there's been a priority in process and products, Joe decides to review how his internal Remediation SLA efficiency has improved. By expanding the date range to include the past 6 months, he can report on the positive trend in addressing the crucial risks within the set number of days. Seeing how he missed his target SLA efficiency last week, Joe can look at what's outside of SLA (how many risks, how many days, and which tags) to determine what he needs to follow up on.

He wants to share this **Exposure View** with his entire team, so he exports and emails to the team with a high level summary and action items.

Joe takes note of the businesses he wants to focus on within the **Tag Performance** widget, and then creates a custom exposure card for each one.

Customize

Now, Joe takes a look at his **Exposure Card Library**. At a glance, he can see his **General** and **Custom** exposure cards, where he can also see a high level preview of each card's CES and CES trend.

Should he need to create a **Lumin Exposure View** with a different segment, he may ask Rachel to help create a custom tag within the **Asset Inventory**. Rachel creates a tag that is data agnostic (so he can mix and match assets for a tag) and then a custom card using the new tag. She shares this new **Lumin Exposure View** with Joe. Since Joe needs more details, he clicks on the **Top Affecting tags** link and jumps directly to the **Asset Inventory** where he can see all the assets associated with this tag. Here, he can also view asset details, and can even navigate directly to the data source product for more information. Rachel realizes that the static tag should actually be a dynamic tag, so she edits the tag configuration.

Incidents and Actions

Thomas is on the InfoSec team and is responsible for any incidents. His main focus is the **Attack Path Analysis** section, where he can build a custom query highlighting his most sensitive assets. He can then interact with the attack path data and proactively see potential attack paths and techniques. Here, Thomas can answer the following key questions:

- In my environment, what are all possible attack paths between two assets or asset types?
- In my environment, what are all possible attack paths that leverage a specific technique?
- What assets are in jeopardy if one specific asset is compromised? (Blast Radius)
- How do all assets in my network affect one specific asset in my environment? (Asset Exposure)
- Where is an asset within the attack path?
- How critical is an asset?

Lumin Exposure View Metrics

The following metrics are used to assess data within Tenable One:

Cyber Exposure Score (CES)

Tenable One calculates a dynamic CES that represents exposure risk as an integer between 0 and 1000, based on the Asset Exposure Score (AES) values for assets. Higher CES values indicate higher risk.

> **Note:** Tenable One does not include assets older than 90 days in your CES.

CES Category	CES Range
High	650 to 1000
Medium	350 to 649
Low	0 to 349

Asset Exposure Score (AES)

Tenable One calculates a dynamic AES for each asset on your network to represent the asset's relative exposure as an integer between 0 and 1000. A higher AES indicates higher exposure.

> **Note:** Tenable One does not calculate an AES for unlicensed assets.

AES Category	AES Range
High	650 to 1000
Medium	350 to 649
Low	0 to 349

Tenable One Categories

Tenable One products refer to data sources as **Categories**. For more information, see Data Sources.

Additionally, the **Lumin Exposure View** uses specific icons to represent each category within the user interface.

Category	Icon
Web Applications	▣
Computing Resources	☰
Identities	👥
Cloud Resources	☁

Tenable One Scoring Explained

The building blocks for the Cyber Exposure Score (CES) in the Tenable One Exposure Management Platform are similar to those used for years in Tenable products (e.g., Tenable Vulnerability Management, Tenable Lumin). These mechanisms have to date only been used for vulnerability management data. Tenable One expands these concepts into new realms of the attack surface: **Web Applications** (Tenable Web App Scanning), **Cloud Resources** (Tenable Cloud Security), and **Identity** (Tenable Identity Exposure).

For more information on Tenable One scoring, see the*Tenable One Scoring Explained Quick Reference Guide*.

Log in to the Lumin Exposure View

To log in to Lumin Exposure View:

1. In a supported browser, navigate to https://cloud.tenable.com/. The login page appears.
2. Type your **Username** and **Password** credentials.
3. Click **Login**.

   The **Workspace** page appears.
4. Click the **Lumin Exposure View** tile.

   The **Lumin Exposure View** interface appears, where you can view exposure cards, CES data, and more.

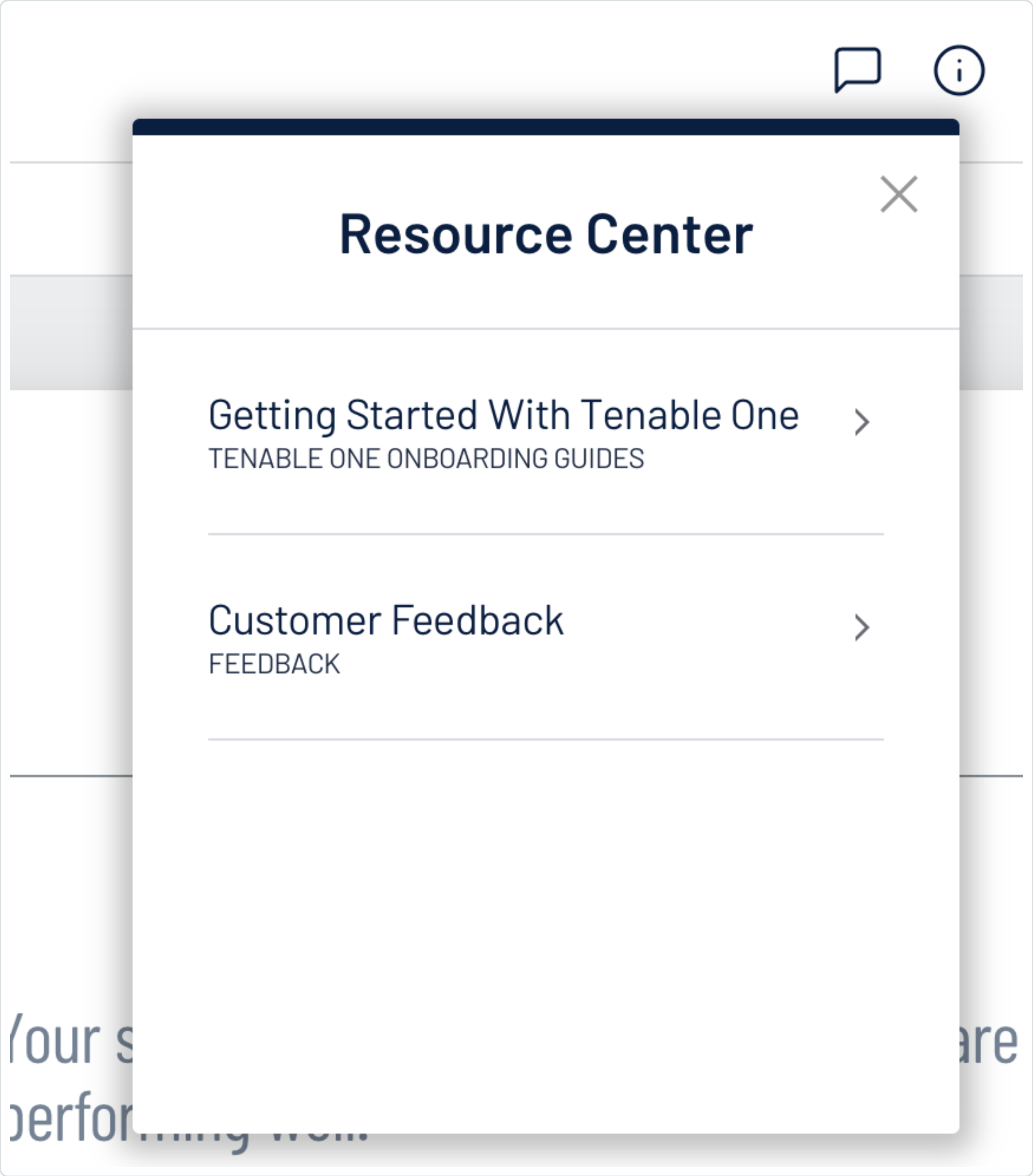
Access the Resource Center

The **Resource Center** displays a list of informational resources including product announcements, product walkthroughs, and user guide documentation.

To access the Resource Center:

1. In the upper-right corner, click the ⓘ button.

   The **Resource Center** menu appears.



Resource Center

Getting Started With Tenable One
TENABLE ONE ONBOARDING GUIDES

Customer Feedback
FEEDBACK

2. Click a resource link to navigate to that resource.

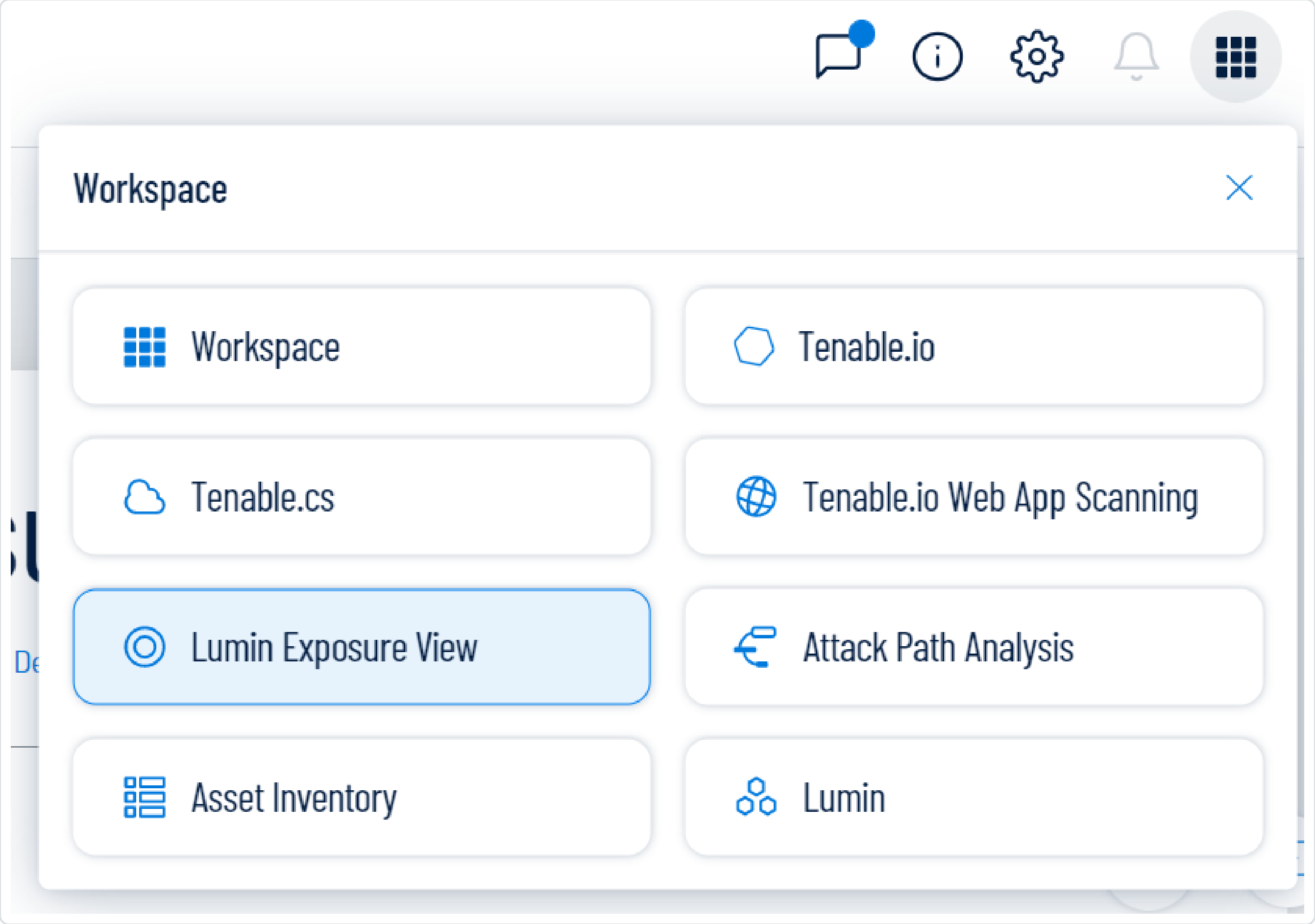
Access the Workspace

On the **Workspace** page and in the **Workspace** menu, you can view and access all of your Tenable products in one location.

To access the Workspace menu:

1. On any page, in the upper-right corner, click the ▦ button.

   The **Workspace** menu appears and displays all of your Tenable products.



2. Click on a product name to navigate to that product's home page.

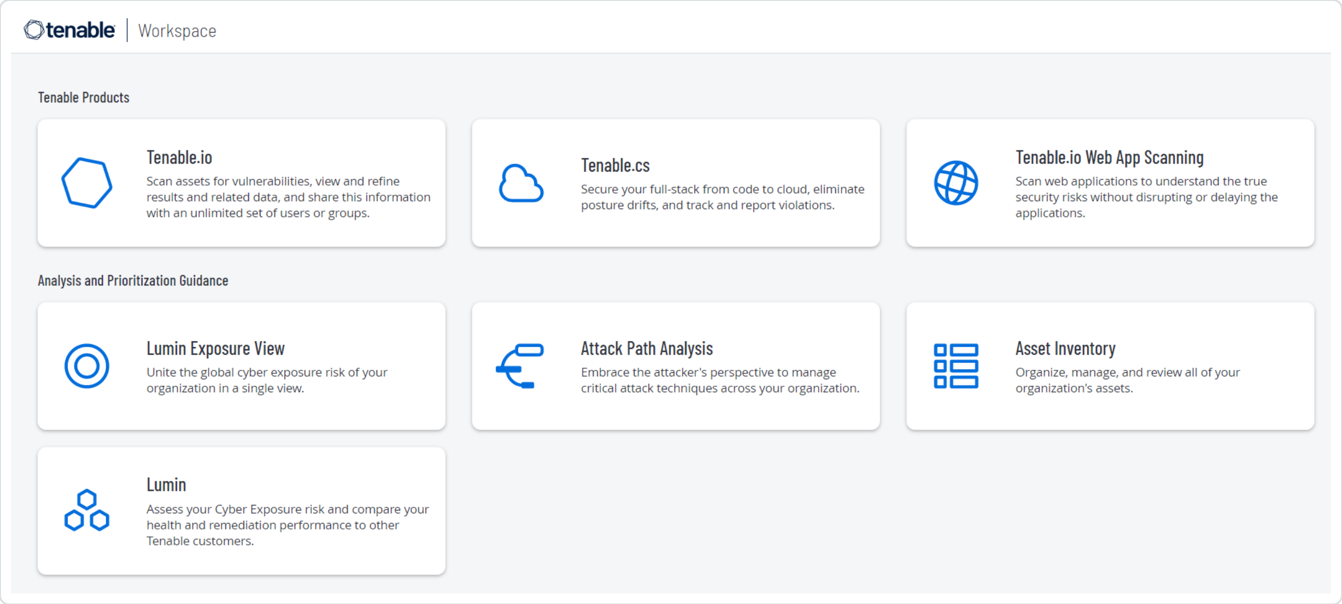
To access the full Workspace page:

1. Do one of the following:

    - Log in to Lumin Exposure View.
    - Access the **Workspace** menu.

        a. In the **Workspace** menu, click ▦ **Workspace**.

    The full **Workspace** page appears and displays all of your Tenable products.



tenable | Workspace

Tenable Products

Tenable.io
Scan assets for vulnerabilities, view and refine results and related data, and share this information with an unlimited set of users or groups.

Tenable.cs
Secure your full-stack from code to cloud, eliminate posture drifts, and track and report violations.

Tenable.io Web App Scanning
Scan web applications to understand the true security risks without disrupting or delaying the applications.

Analysis and Prioritization Guidance

Lumin Exposure View
Unite the global cyber exposure risk of your organization in a single view.

Attack Path Analysis
Embrace the attacker's perspective to manage critical attack techniques across your organization.

Asset Inventory
Organize, manage, and review all of your organization's assets.

Lumin
Assess your Cyber Exposure risk and compare your health and remediation performance to other Tenable customers.

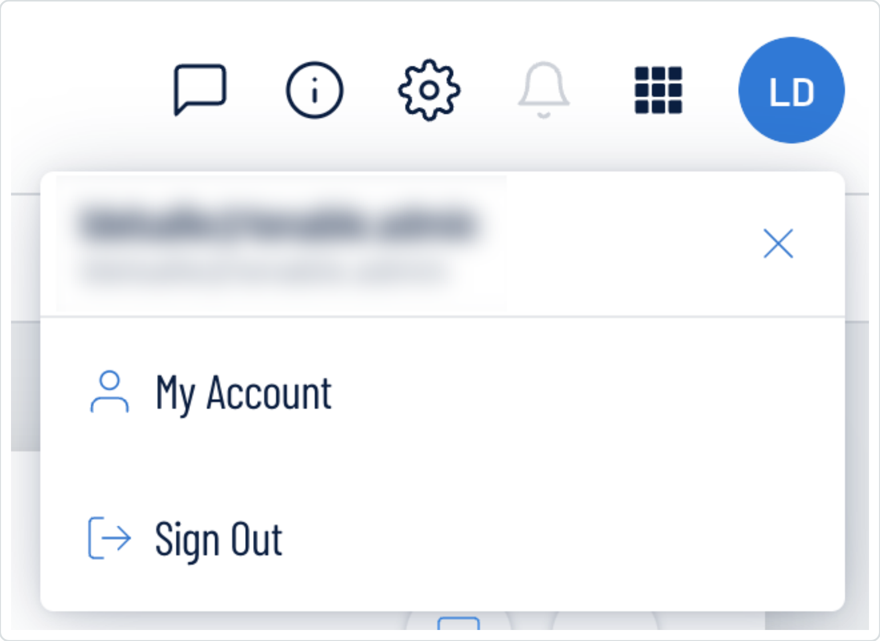
2. Click on a product name to navigate to that product's home page.

Access the User Account Menu

To access the user account menu:

1. In the upper-right corner, click the blue user circle.

   The user account menu appears.

2. Do one of the following:

   - Click **My Account** to make changes to your own user account. See My Account for more information.
   - Log out of Tenable Vulnerability Management. See Log out of the Lumin Exposure View for more information.

My Account

The **My Account** option in the user account menu directs you to the **My Account** page, where you can make changes to your own user account. For more information, see Settings within the *Tenable Vulnerability Management User Guide* .

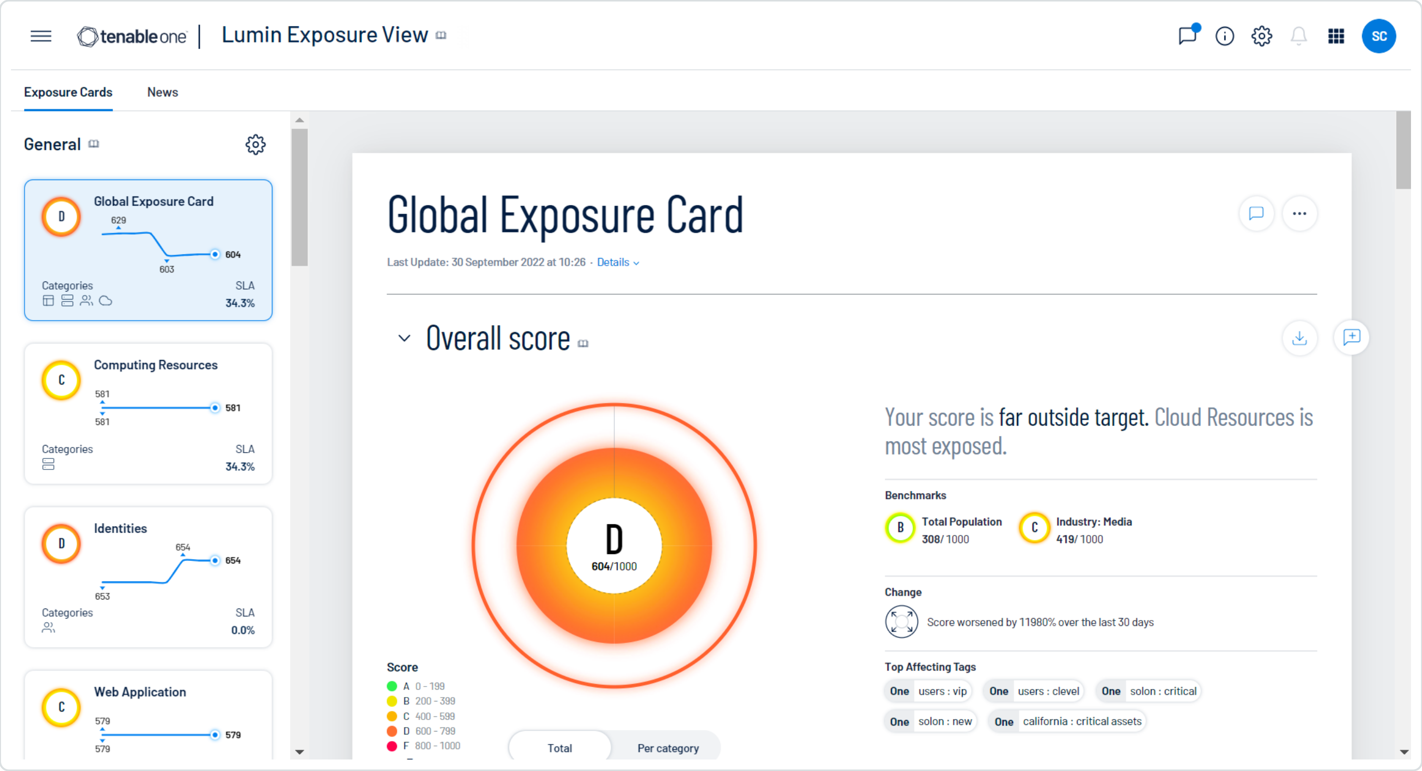
Log out of the Lumin Exposure View

To log out of the Lumin Exposure View:

1. Access the user account menu.
2. Click **Sign Out**.

Lumin Exposure View

The **Tenable Lumin** in Tenable One allows you to quickly view your global CES, see its changes over time, identify which categories to prioritize, and assess your overall risk. The **Lumin Exposure View** includes several tools that help you understand your overall security posture as defined by your business context, asset criticality, and the effectiveness of your remediation efforts.



Your score is far outside target. Cloud Resources is most exposed.

Score worsened by 11980% over the last 30 days

To access the **Exposure View**:

1. In the upper-left corner of the page, click the ☰ button.

2. In the **Analytics** section, click **Lumin Exposure View**.

   The **Lumin Exposure View** page appears.

In the **Lumin Exposure View**, you can:

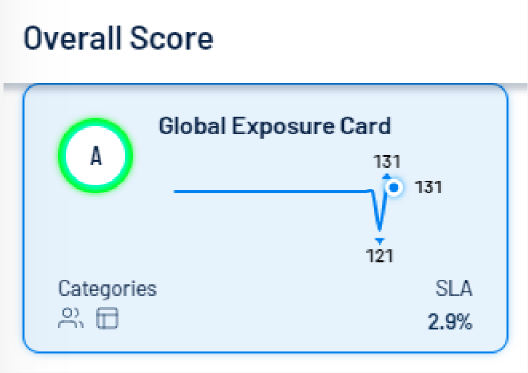
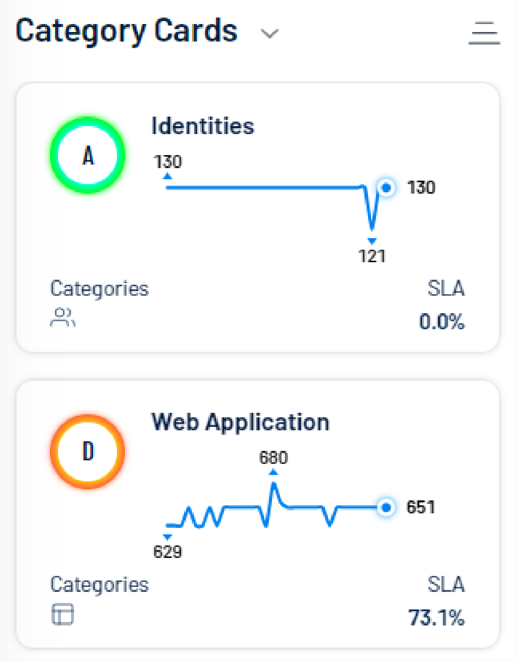
- View the available exposure cards for which you can view data via the **Exposure Cards** tab.
- View your CES for Tenable-provided datasets, or view the CES for a custom set of data via a custom exposure card.

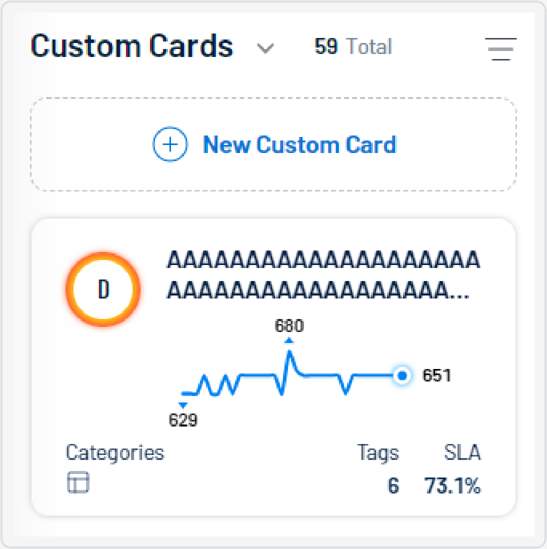
- View CES trend data for any exposure card.
- View Remediation Service Level Agreement (SLA) data.
- View Tag Performance data.
- Comment on the **Exposure View** or its widgets.
- Export the **Exposure View** or its widgets.
- View Tenable blog posts related to vulnerability events via the **News** tab.

Tip: When scrolling the **Exposure View**, in the upper-right corner, click **Back to Top** to return to the top of the page.

View the Exposure Cards Library

In Tenable One, the **Exposure Cards** library in the **Lumin Exposure View** allows you to view the following types of exposure cards:

Card type	UI Image
A Tenable-provided **Global Exposure Card** that shows your **Overall Score** based on all internal and external data within Tenable One.	 Overall Score A Global Exposure Card 131 131 121 Categories SLA 2.9%
Tenable-provided **Category Cards** based on data from the following categories: • **Computing Resources** – All data from Tenable Vulnerability Management sources. • **Identities** – All data from Tenable Identity Exposure sources. • **Web Application** – All data from Tenable Web App Scanning sources. • **Cloud Resources** – All data from Tenable Cloud Security sources.	 Category Cards A Identities 130 130 121 Categories SLA 0.0% D Web Application 680 651 629 Categories SLA 73.1%

Data from user-created custom exposure cards.	 Custom Cards 59 Total New Custom Card D AAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAA... 680 651 629 Categories Tags 6 SLA 73.1%

To view the **Exposure Cards** library:

1. Access the **Lumin Exposure View**.
2. On the left side of the page, click the **Exposure Cards** tab.

   A list of Tenable-provided and user-created exposure cards appears.
3. Click on an exposure card to view:
   - The CES for the card.
   - The CES trend for the card.
   - Remediation SLA data for the card.
   - Tag performance information for the card.

Create a Custom Exposure Card

In Tenable One, you can create a custom exposure card to specify the categories for which you want to see data. Once you create a custom exposure card, you can then select the card in the **Exposure Cards** library to view its data in the **Lumin Exposure View**. You can create a custom exposure card either through the **Exposure Cards** library or from a news event via the **News** tab.

Before you begin:

- Create a tag to apply to the card.

To create a custom exposure card:

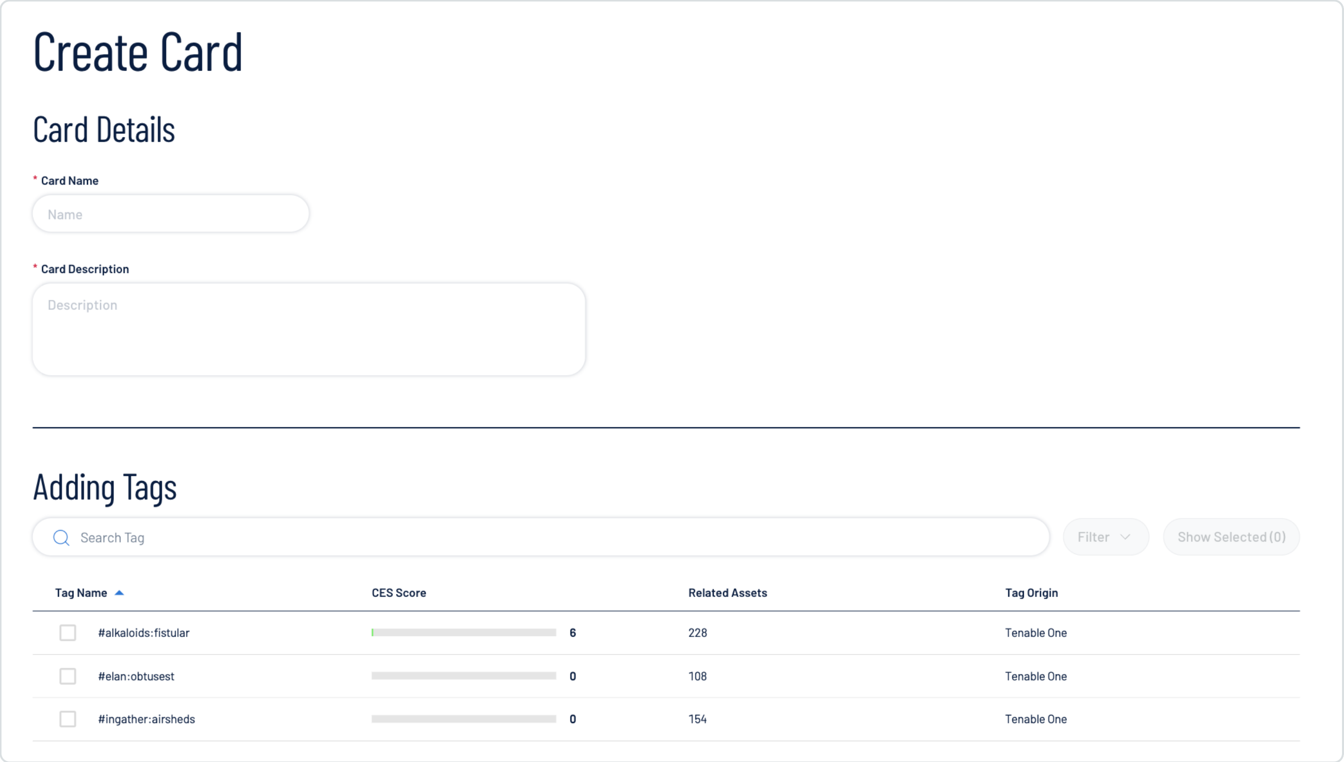
1. Access the **Lumin Exposure View**.

2. On the left side of the page, click the **Exposure Cards** tab.

   A list of exposure cards appears.

3. At the top of the **Exposure Cards** library or in the **Custom Cards** section, click the ⊕ **New Custom Card** button.

   The **Create Card** page appears.



Create Card

Card Details

* Card Name

Name

* Card Description

Description

Adding Tags

Search Tag

	Tag Name	CES Score	Related Assets	Tag Origin
□	#alkaloids:fistular	6	228	Tenable One
□	#elan:obtusest	0	108	Tenable One
□	#ingather:airsheds	0	154	Tenable One

4. In the **Card Details** section, in the **Card Name** box, type a name for the exposure card.
5. In the **Card Details** section, in the **Card Description** box, type a name for the exposure card.
6. In the **Adding Tags** section, select the tags you want to use to provide data for the exposure card:
   1. (Optional) Use the **Search** box to search for specific tags.
   2. Select the check box next to each tag you want to use to provide data for the exposure card.
   3. (Optional) to view only the tags you've added to the exposure card, click **Show Selected**.
7. Click **Save** 💾 .

   The **Lumin Exposure View** saves the exposure card and adds it to the **Custom Cards** section of the **Exposure Cards** library.

Edit an Exposure Card

To edit an exposure card:

1. Access the **Exposure Cards** library.

   A list of exposure cards appears.

2. Click the card you want to edit.

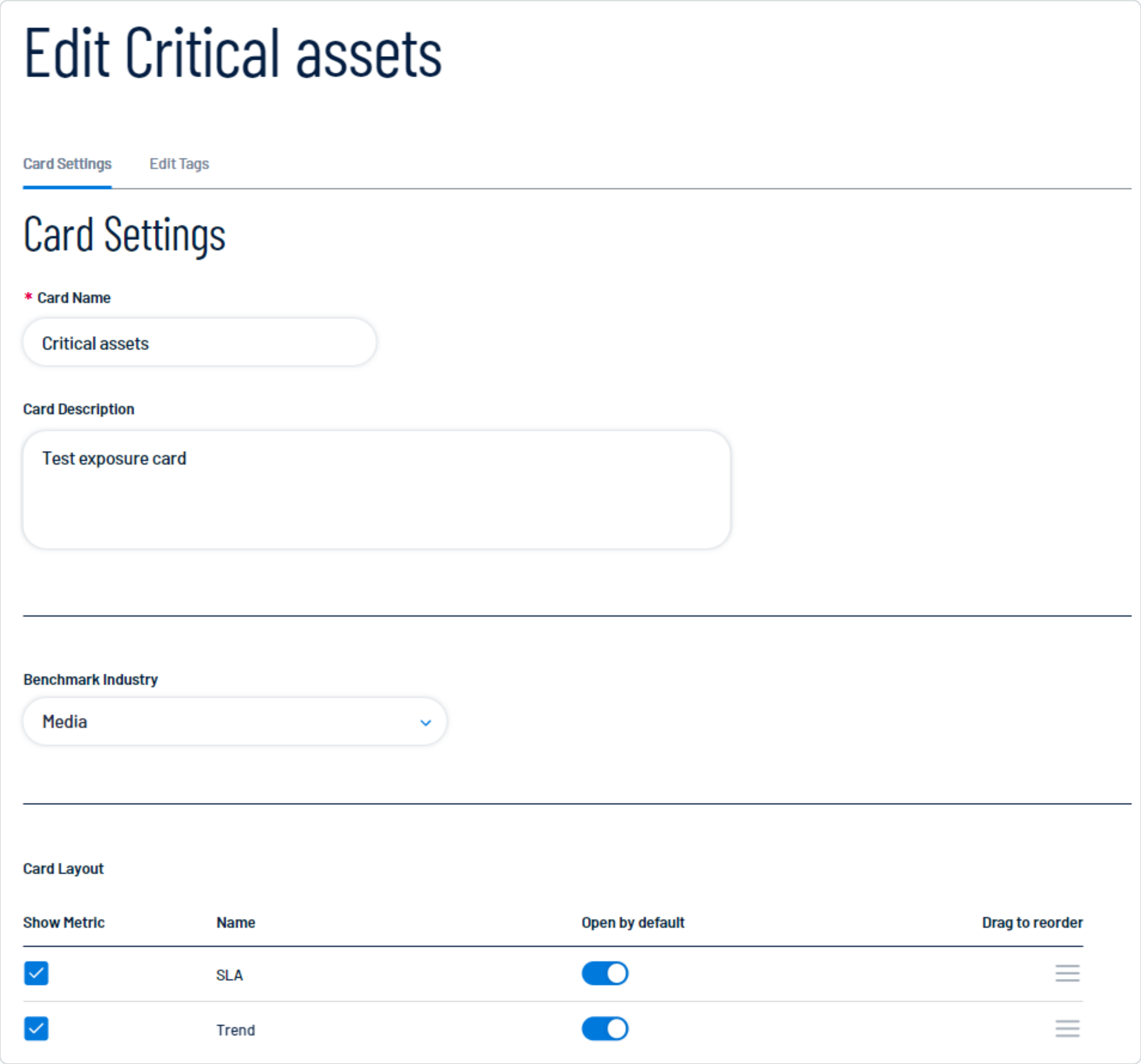
   The card information appears in the **Lumin Exposure View**.

3. At the top of the **Lumin Exposure View**, click the ⋯ button.

   A menu appears.

4. Click ✎ **Edit**.

   The edit card page appears.



Edit Critical assets

Card Settings

* Card Name

Critical assets

Card Description

Test exposure card

Benchmark Industry

Media

Card Layout

Show Metric	Name	Open by default	Drag to reorder
☑	SLA	●	≡
☑	Trend	●	≡

5. On the **Card Settings** tab, make any desired changes:

- Card Settings

Option	Description
Card Name	Edit the name of the card.
Card Description	Edit the card description.

- Benchmark Industry

Option	Description
Benchmark Industry	In the drop-down menu, select the industry to use as a benchmark when comparing your metrics. For more information, see Lumin Exposure View Metrics.

- Card Layout

Option	Description
Show Metric	Do any of the following: • Select the check box next to any metric that you want to include in the exposure card. • Deselect the check box next to any metric that you do not want to include in the exposure card.
Open by Default	Do any of the following: • Enable the toggle for any metric that you want to open by default when viewing the exposure card. • Disable the toggle for any metric that you do not want to open by default when viewing the exposure card.
Drag to Reorder	Drag and drop the rows of metrics to edit the order in which they appear on the exposure card.

- Card Targets

Option	Description
Default/Custom toggle	Do any of the following: • Enable the toggle to use the default options for this section. • Disable the toggle to set custom options for this section.
Card Targets	The **Card Targets** section allows you set the overall target for the card. Select the radio button next to one of the following options: • **Custom** – Manually select a target benchmark for the exposure card by doing one of the following: ◦ In the text box, manually type a target benchmark number for the card. ◦ Click and drag the slider to select a target benchmark number for the card. • **Set to Industry Benchmark** – Automatically set the target to match the industry benchmark for the data. • **Set to Population Benchmark** – Automatically set the target to match the population benchmark for the data. • **Set to Global CES Target** – Automatically set the target to match your Global CES for the data.

- Category Targets

Option	Description
Category Targets • **Cloud**	The **Category Targets** section allows you set the target benchmark for each individual category whose data pop-

Resources - **Computing Resources** - **Identity** - **Web Applications** - **Source Code**	ulates the card. For each category, select the radio button next to one of the following options: - **Custom** – Manually select a target benchmark for the category by doing one of the following: ◦ In the text box, manually type a target for the category. ◦ Click and drag the slider to select a target for the category. - **Set to Industry Benchmark** – Automatically set the target to match the industry benchmark for the data. - **Set to Population Benchmark** – Automatically set the target to match the population benchmark for the data.

- **Trend**

Option	Description
Default/Custom toggle	Do any of the following: - Enable the toggle to use the default options for this section. - Disable the toggle to set custom options for this section.
Default Timespan Shown	In the drop-down menu, select the timespan to use for the **Trend** section within the **Lumin Exposure View**.

- **Remediation SLA**

Option	Description
Default/Custom toggle	Do any of the following: • Enable the toggle to use the default options for this section. • Disable the toggle to set custom options for this section.
Low, **Medium**, **High**, and **Critical** ranges	For each category, type the number of days within which each risk level of SLA must be addressed. For example, if you have an internal SLA to address critical **Computing Resources** risks within 4 days, in the **Critical** text box for that category, type **4**.
View Severity on Card	Do any of the following: • Select the check box below any risk range that you want to include in the exposure card. • Deselect the check box below any risk range that you do not want to include in the exposure card.
Graph Range	For each risk range, type the date range to use for the graph in the **SLA** section within the Lumin Exposure View.

6. On the **Edit Tags** tab, make any desired changes to the tags used to provide data for the exposure card:

   a. (Optional) Use the **Search** box to search for specific tags.

   b. (Optional) Use the **Filter** top filter the list of tags by specific criteria.

   c. (Optional) Add or remove any tag values or categories to or from the exposure card.

   d. (Optional) To view only the tags you've added to the exposure card, click **Show Selected**.

7. Click **Save** 🖫 .

   The **Lumin Exposure View** saves your changes to the exposure card.

Delete a Custom Exposure Card

To delete a custom exposure card:

1. Access the **Exposure Cards** library.

   A list of exposure cards appears.

2. In the **Custom** section, click the custom card you want to edit.

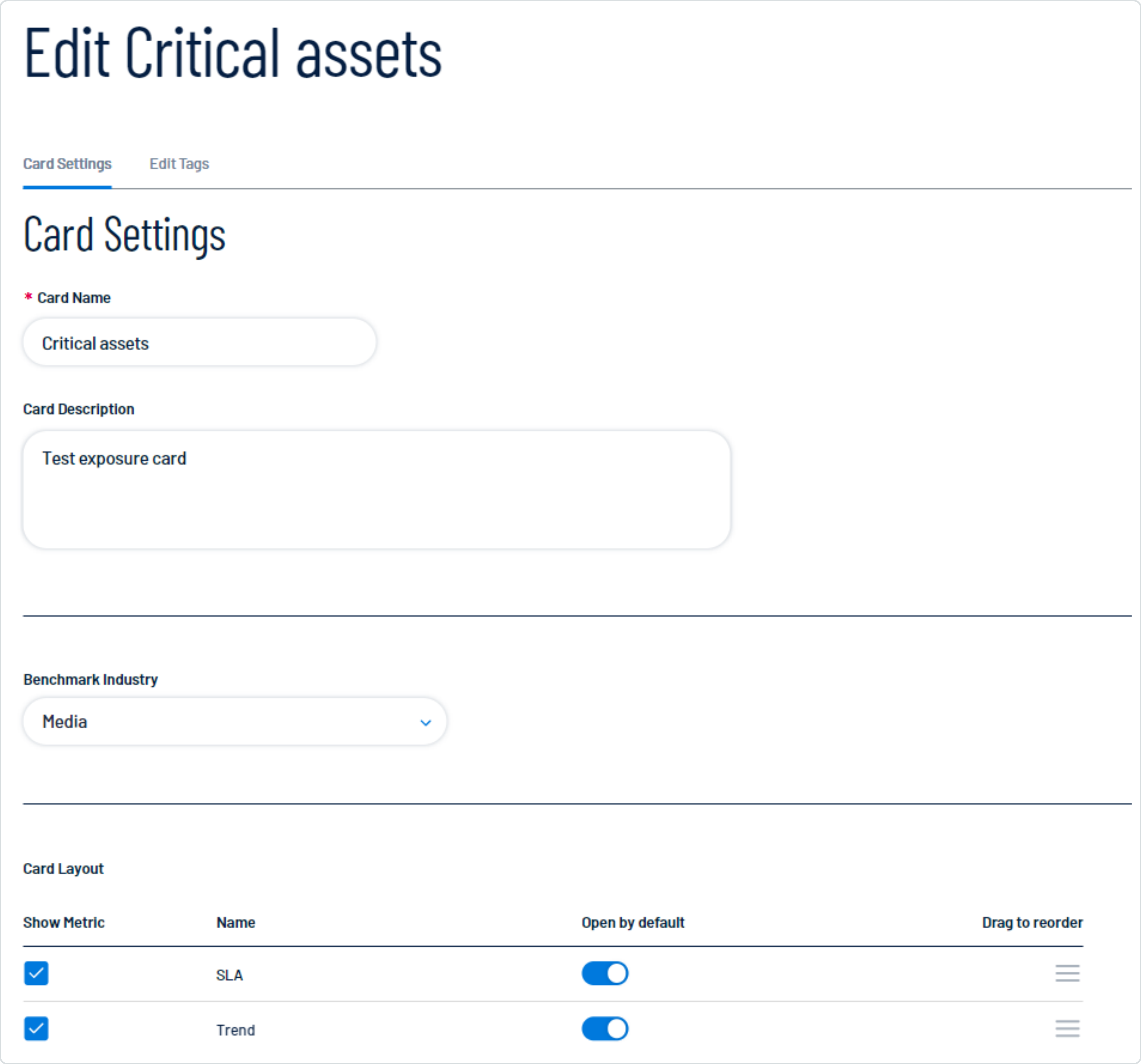
   The card information appears in the **Lumin Exposure View**.

3. At the top of the **Lumin Exposure View**, click the ⋯ button.

   A menu appears.

4. Click ✎ **Edit**.

   The edit card page appears.



Card Settings

* Card Name: Critical assets

Card Description: Test exposure card

Benchmark Industry: Media

Card Layout

Show Metric	Name	Open by default	Drag to reorder
☑	SLA	●	☰
☑	Trend	●	☰

5. At the bottom of the page, click **Delete** 🗑 .

   A confirmation message appears.

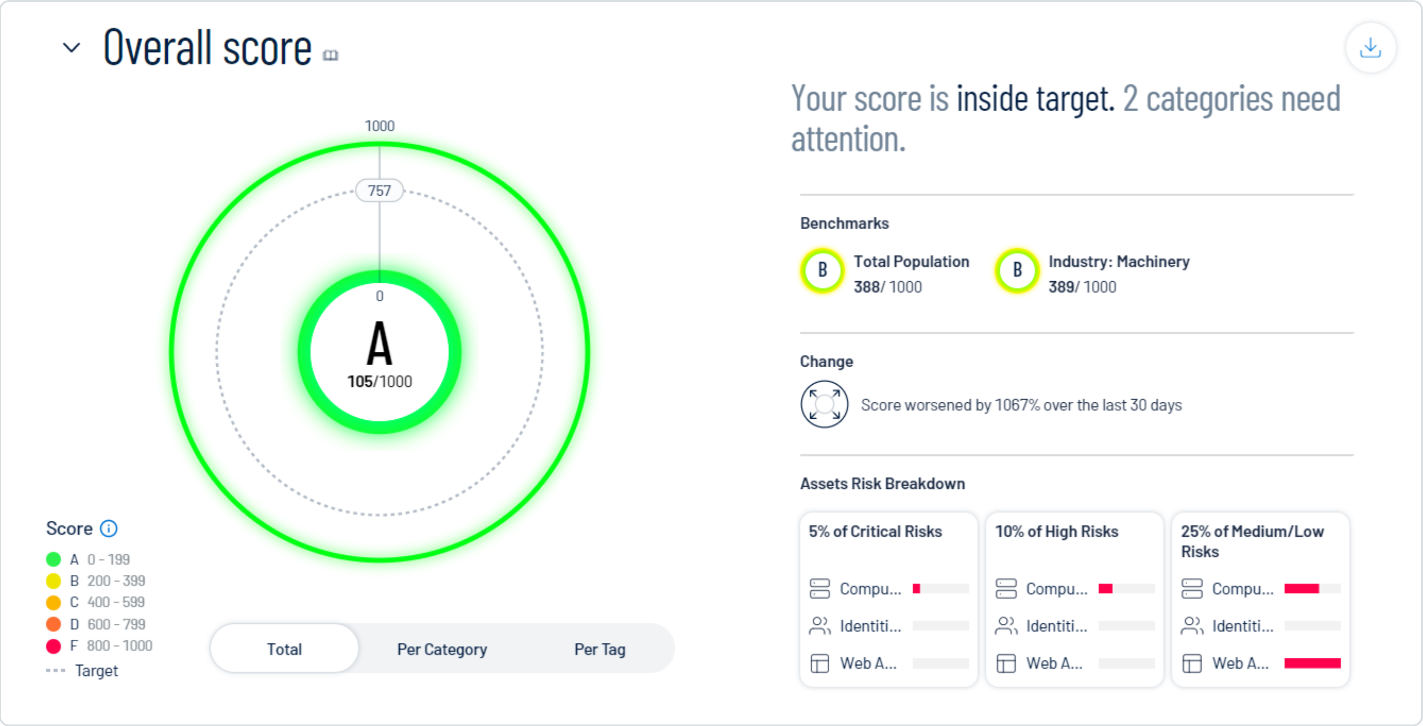
6. Click **Delete card**.

   The **Lumin Exposure View** deletes the custom exposure card.

View Your CES

By default, the Lumin Exposure View displays your **Global** Cyber Exposure Score. You can select a specific card via the Exposure Cards library to view your Cyber Exposure Score for that card. CES data is available for the following categories:

- Tenable-provided exposure cards, which include:
  - **Global** – All internal and external data within Tenable One.
  - **Computing Resources** – All data from Tenable Vulnerability Management sources.
  - **Identities** – All data from Tenable Identity Exposure sources.
  - **Web Application** – All data from Tenable Web App Scanning sources.
  - **Cloud Resources** – All data from Tenable Cloud Security sources.
- Data from user-created custom exposure cards.



Overall score

Your score is inside target. 2 categories need attention.

Benchmarks

B Total Population 388/ 1000

B Industry: Machinery 389/ 1000

Change

Score worsened by 1067% over the last 30 days

Assets Risk Breakdown

5% of Critical Risks	10% of High Risks	25% of Medium/Low Risks
Compu...	Compu...	Compu...
Identiti...	Identiti...	Identiti...
Web A...	Web A...	Web A...

Note: Tenable One does not include assets older than 90 days in your CES.

To view your CES for an exposure card:

1. Access the [Exposure Cards](#) library.

   A list of exposure cards appears.

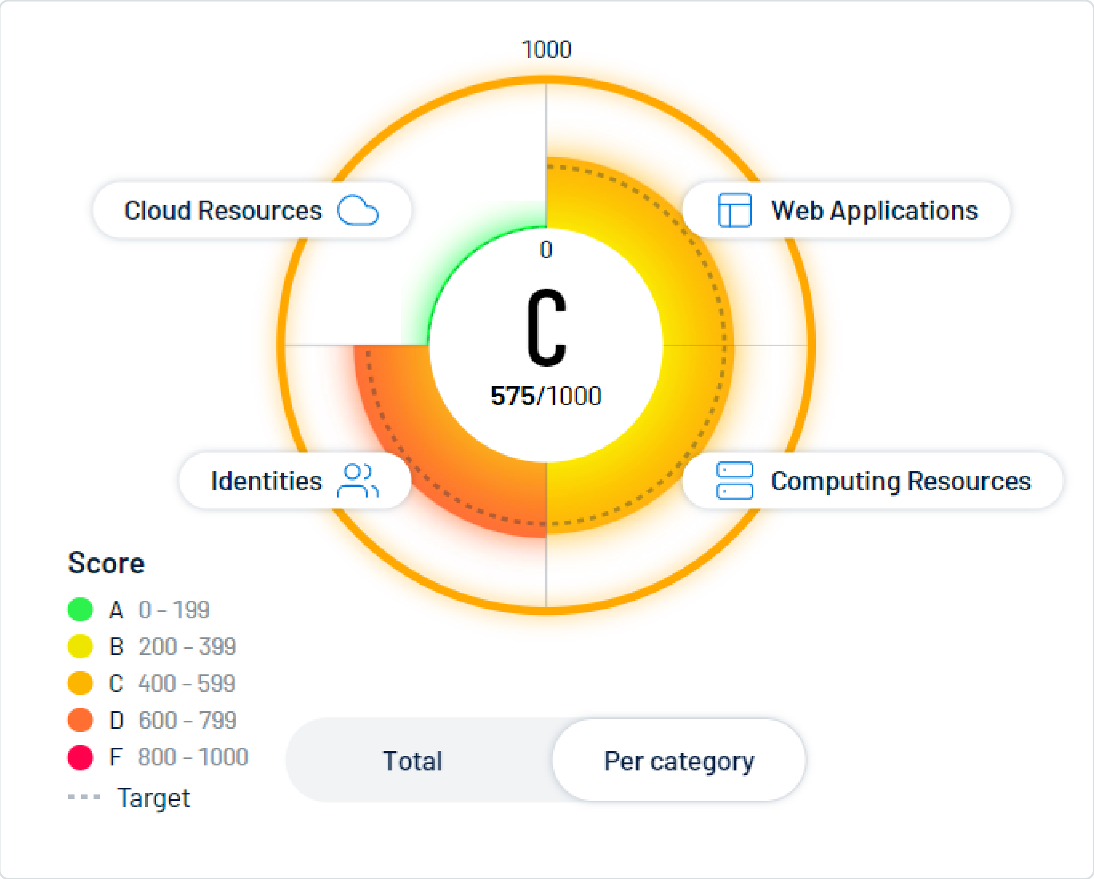
2. Select the exposure card for which you want to view your CES.

   The **Exposure View** displays the CES details for the selected card.

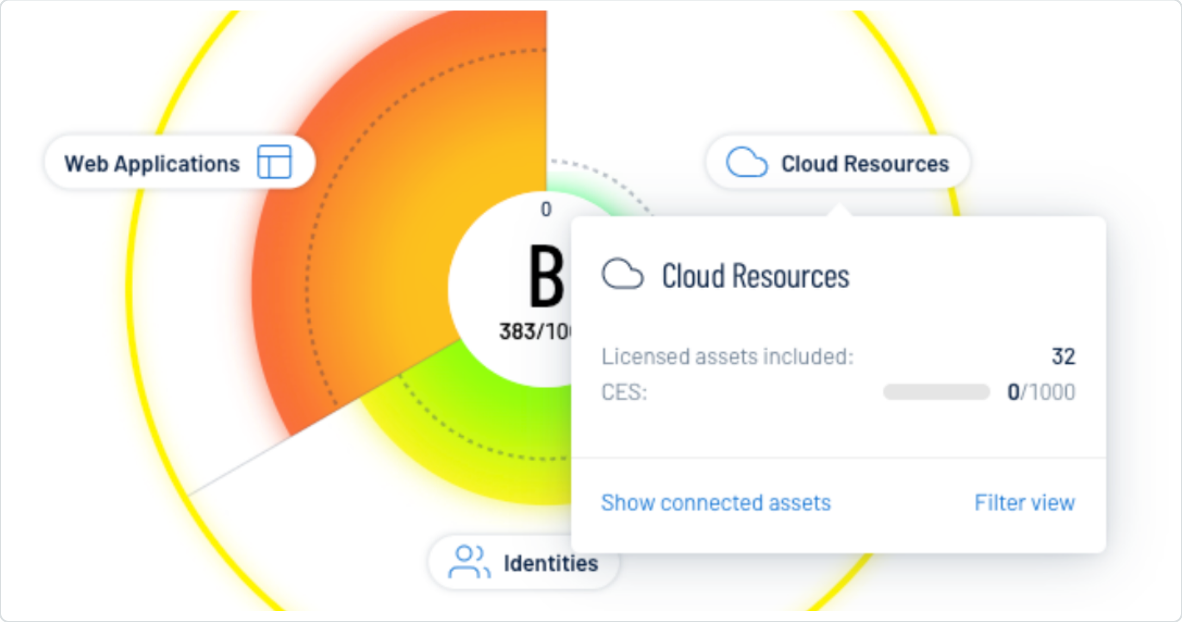
While viewing the CES details for a card, you can:

- In the upper-left corner of the page, view the time at which the **Lumin Exposure View** last updated the CES.
- In the upper-left corner of the page, click **Details** to view the following exposure card information:
  - The number of assets associated with the exposure card.
    - Click the asset number to view the assets directly in the [Asset Overview](#).
  - The user that created the exposure card.
  - The date and time at which the exposure card was created.
  - Where applicable, the card description.
- View a graphical representation of your CES grade as it compares to your industry and the total population:
  - To view your total CES regardless of the data source, below the circle graph, click **Total**.
  - To view your CES separated based on the source of the data, below the circle graph, click **Per Category**.

    The CES graph splits into sections that represent each category. For more information, see [Lumin Exposure View Metrics](#).



- Within the CES graph, click an individual category name to view additional category information, connected assets, and to filter the Lumin Exposure View by the selected category.



Cloud Resources

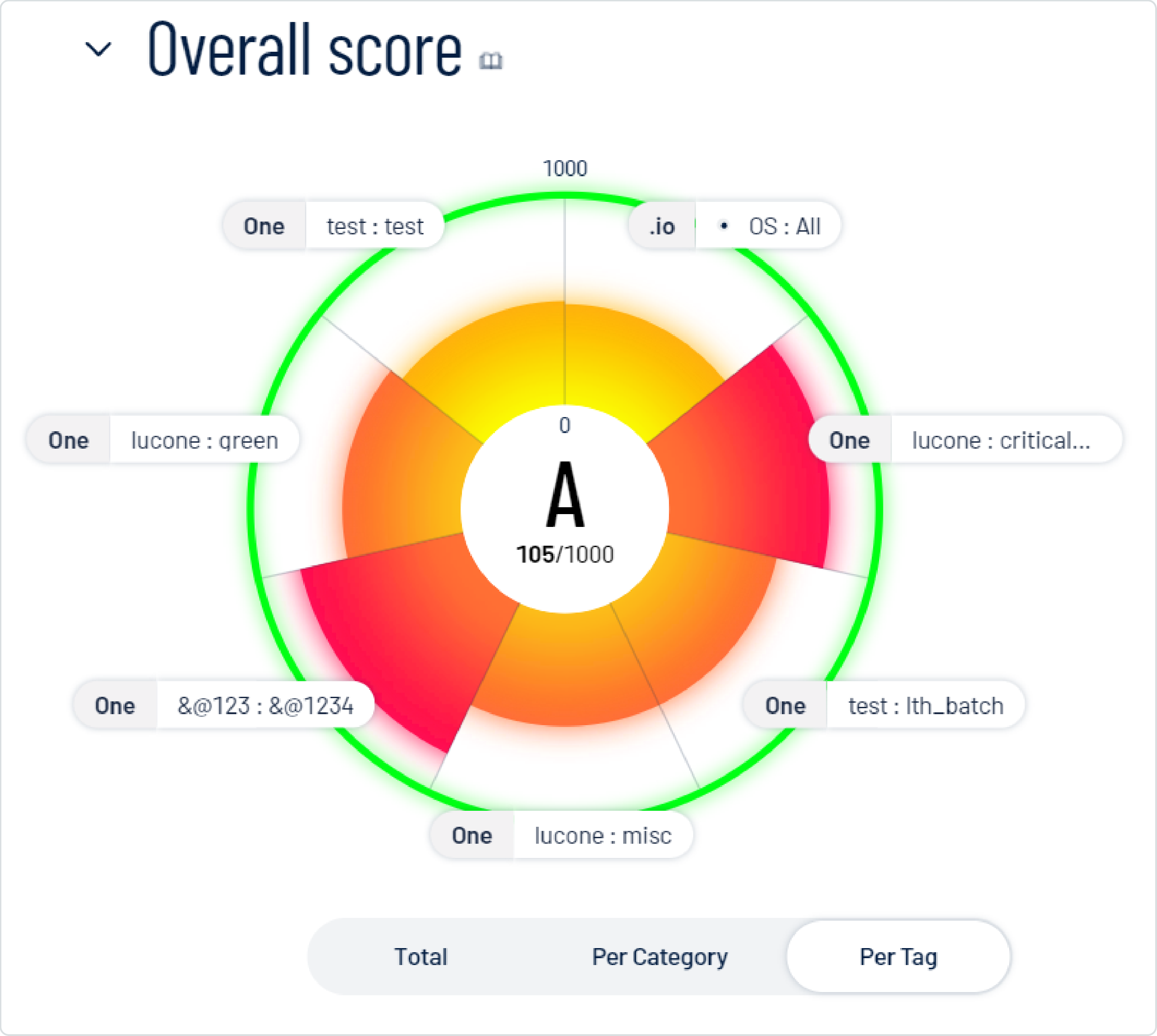
Licensed assets included: 32

CES: 0/1000

- ◦ To view the top tags driving your score, below the circle graph, click **Per Tag**.

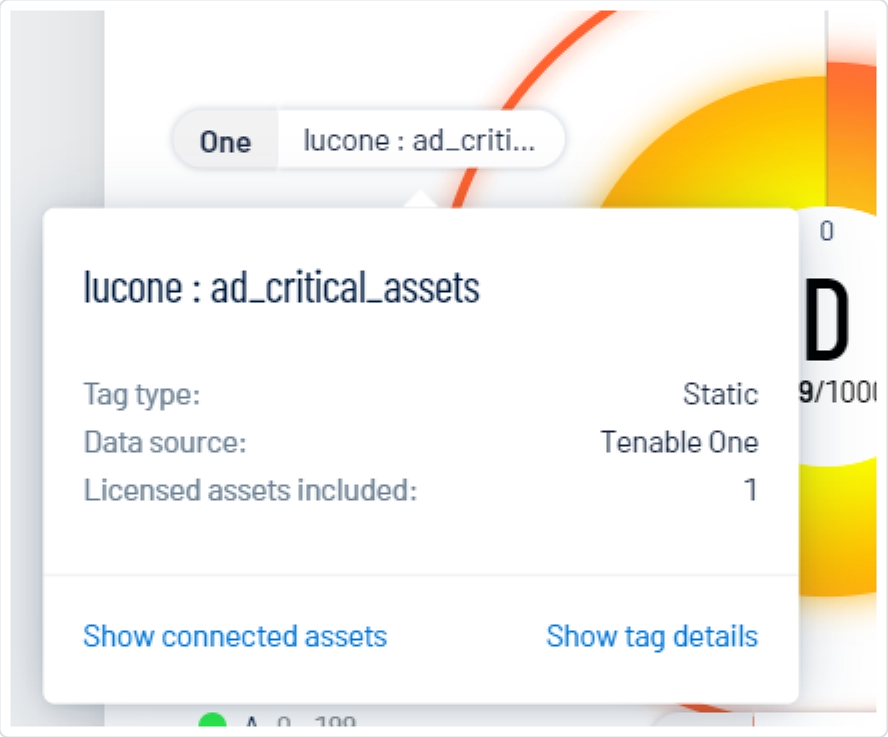
> **Note:** The Lumin Exposure View displays up to 10 tags within the graph.

The CES graph splits into sections that represent each tag. For more information on tags, see View Your Tag Overview.



Overall score

- Within the CES graph, click an individual tag name to view additional tag information, connected assets, and tag details.



lucone : ad_critical_assets

Tag type: Static
Data source: Tenable One
Licensed assets included: 1

- To the right of the CES graph, view a small blurb that:
  - Indicates how your score compares to the baseline target.
  - Identifies the performance of your categories. For example, this blurb may explain that you have two critical categories.
- On the right side of the page, in the **Benchmarks** section, view how your CES compares to others is your industry and in the total population.
- In the **Change** section, view how your CES has changed within the last 30 days.
- In the **Asset Risk Breakdown** section, view tiles that indicate your asset risk:
  - The **Critical Risks** tile shows the percentage of your assets with associated vulnerabilities of critical severity, as well as the data source(s) of those assets.
  - The **High Risks** tile shows the percentage of your assets with associated vulnerabilities of high severity, as well as the data source(s) of those assets.

- ○ The **Medium/Low Risks** tile shows the percentage of your assets with associated vulnerabilities of medium or low severity, as well as the data source(s) of those assets.

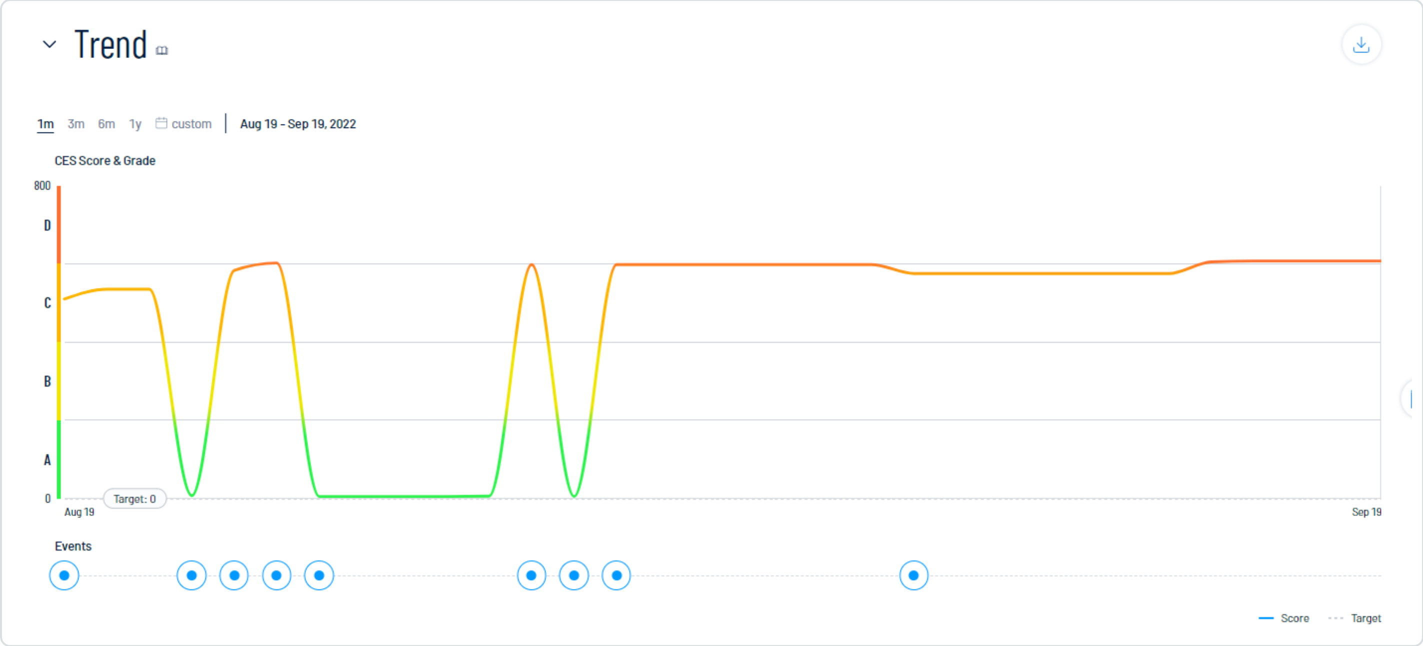
Click any tile to navigate to the **Asset Inventory** filtered by the asset severity type you selected.

Caution: Data in the **Asset Risk Breakdown** section is based on your Vulnerability Priority Rating (VPR). As a result, if you configure your Tenable Vulnerability Management vulnerability severity setting to use CVSS, data in this section may be inconsistent.

Note: Since an asset can have multiple risks across all severities, the sum of the percentages in the **Asset Risk Breakdown** section may exceed 100%.

View CES Trend

The **Trend** section of the Lumin Exposure View shows how your CES has trended over time. You can also view information about specific events that have contributed to your CES.



To view your CES trend for an exposure card:

1. Access the Exposure Cards library.

   A list of exposure cards appears.

2. Select the exposure card for which you want to view the CES trend.

   The **Lumin Exposure View** updates based on your selection.

3. Scroll down to the **Trend** section.

In the **Trend** section, you can:

- View a graphical representation of your CES trend over time.
- At the top of the trend graph, select a timeframe for which you want to view your CES trend:
  - **1m** –View your CES trend over the previous month.
  - **3m** –View your CES trend over the previous 3 months.

    - **6m** –View your CES trend over the previous 6 months.
    - **1y** –View your CES trend over the previous year.
    - **Custom** date range – Use the calendar tool to select a specific date range over which to view your CES trend.

- At the bottom of the trend graph, click an ⊙ event marker. In the **Events** section, the **Lumin Exposure View** displays specific information about that event and how it affects your CES.

View Remediation SLA Data

The **SLA** section of the **Exposure View** shows Remediation Service Level Agreement (SLA) data for Tenable One. SLA represents the acceptable time frame between when a finding is discovered and when it fixed or remediated. Here, you can visualize risks by severity and by compliance with your SLAs to determine how well you are aligning to your organization's policy.

How is my SLA calculated?

Tenable One calculates your SLA efficiency by comparing the number of active findings inside your SLA versus the number of active findings that are inside AND outside your SLA:

Findings inside / Findings (Inside + Outside)

Tenable One includes all active findings in SLA calculations, but only includes remediated findings if they were fixed during the remediation timeframe. To determine if a finding is inside or outside of your SLA, compare the following finding properties:

- All active findings: *current-date* / *first-observed-at*
- Remediated findings: *last-fixed-at* / *first-observed-at*

The data in the **SLA** applies to all exposure cards within the Lumin Exposure View and are only based on vulnerability findings. Findings without a Vulnerability Priority Rating (VPR) do not count towards SLA calculations.

> **Tip:** You can configure your SLA in Tenable One through the Lumin Exposure View. For more information, see Configure Lumin Exposure View Settings.

To view remediation SLA data:

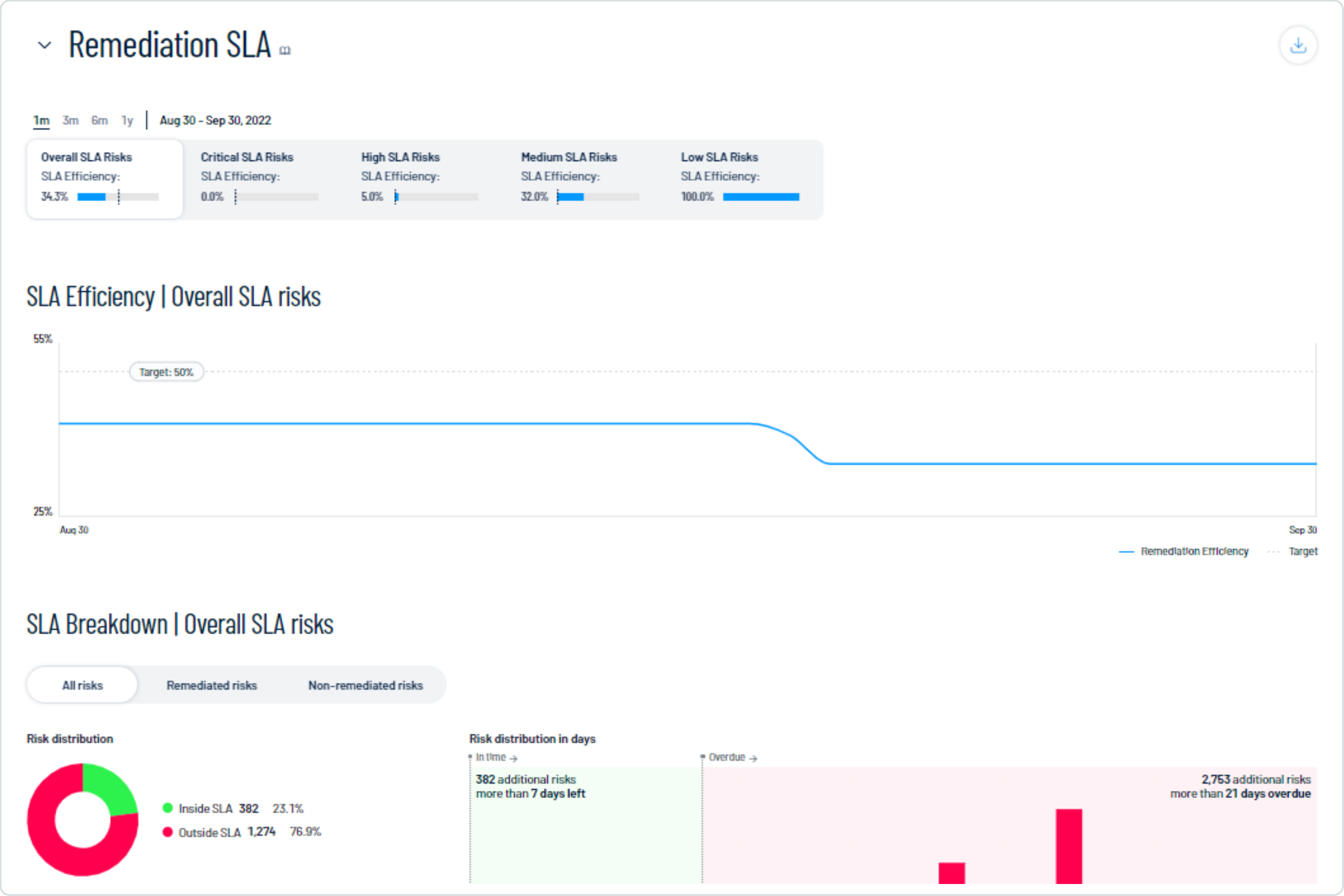
1. Access the **Exposure Cards** library.

   A list of exposure cards appears.

2. Select the exposure card for which you want to view Remediation SLA data.

   The **Lumin Exposure View** updates based on your selection.

3. Scroll down to the **Remediation SLA** section.



In the **Remediation SLA** section, you can:

- Select a timeframe for which you want to view the Remediation SLA data:
  - **1m** –View Remediation SLA data for the previous month.
  - **3m** –View Remediation SLA data for the previous 3 months.
  - **6m** –View Remediation SLA data for the previous 6 months.
  - **1y** –View Remediation SLA data for the previous year.
  - **Custom** date range – Use the calendar tool to select a specific date range over which to view Remediation SLA data.

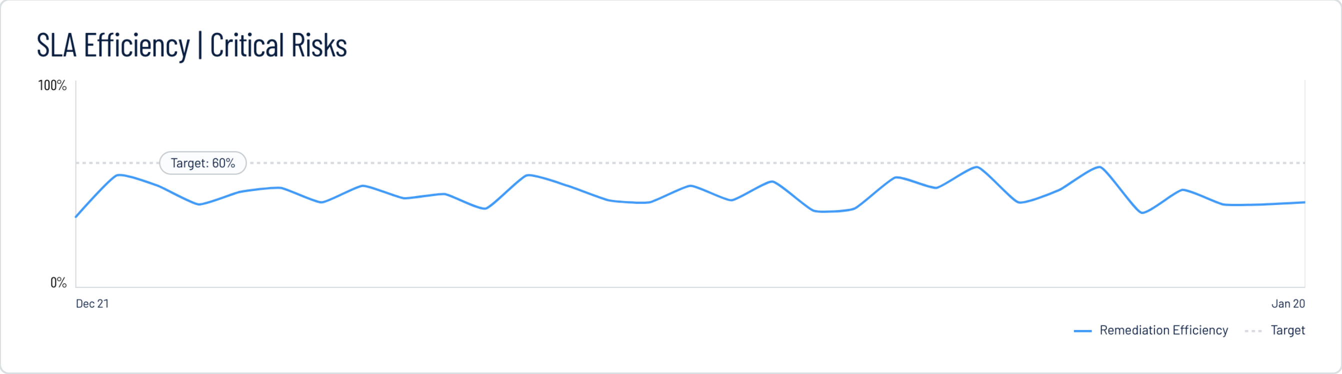
  All data within the **Remediation SLA** section updates accordingly, including the **SLA Efficiency** and **SLA Breakdown** subsections.

- Select a severity level by which you want to filter Remediation SLA data:

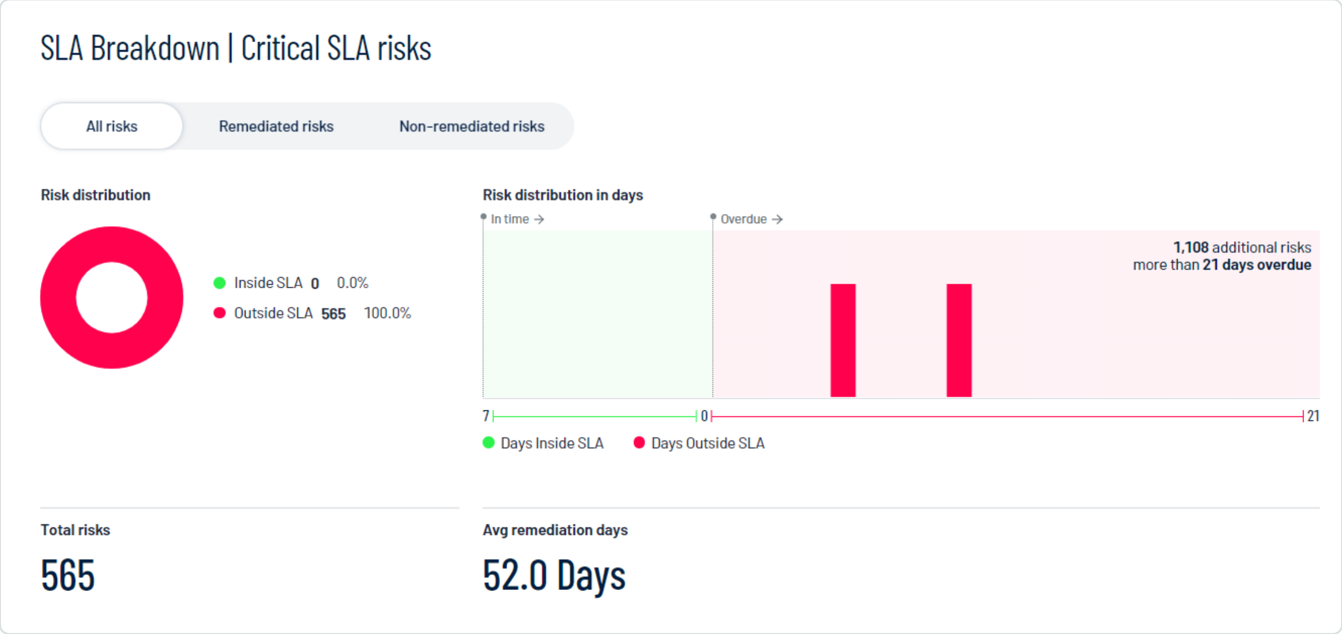
- **Critical Risks** – View only risks that have a critical severity.
- **High Risks** – View only risks that have a high severity.
- **Medium Risks** – View only risks that have a medium severity.
- **Low Risks** – View only risks that have a low severity.

All data within the **Remediation SLA** section updates accordingly, including the **SLA Efficiency** and **SLA Breakdown** subsections.

- In the **SLA Efficiency** trend graph, view SLA trend metrics for a specific range of dates.


SLA Efficiency | Critical Risks

- View your **SLA Breakdown**:


SLA Breakdown | Critical SLA risks

Total risks

565

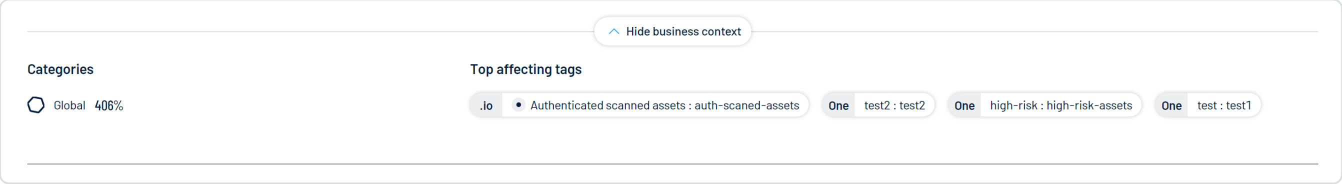
Avg remediation days

52.0 Days

  - Click a risk group type to filter the **SLA Breakdown** data:
    - **All Risks** – All risks regardless of remediation status.
    - **Remediated Risks** – Only remediated risks.
    - **Non-remediated Risks** – Only non-remediated risks.
  - View a graphical representation of your **Risk distribution**, which shows the number and percentage of risks that fall **Inside SLA** and **Outside SLA**.
  - View a graphical representation of your **Risk distribution in days**, which shows your risk distribution based on the number of days your risks are inside or outside the SLA.
  - View the number of **Total risks**.
  - View the number of **Avg. remediation days**.

    > **Note:** This metric only applies to findings that have been fixed or remediated.

- Click **Show business context** to view the category impact and business context tag details:



  - In the **Categories** section, view the percentage of risks outside of your SLA for each data category in Tenable One.
  - In the **Top Affecting Tags** section, view the top tags outside of your SLA, listed in descending order.

View Tag Performance

The **Tag Performance** section of the Lumin Exposure View shows how the tags applied to your assets affect your CES. You can use this information to answer the following questions:

- What tags are part of my current **Lumin Exposure View**?
- Which tags drive my CES?
- Which tags should I focus on to improve my scores?

To view your tag performance:

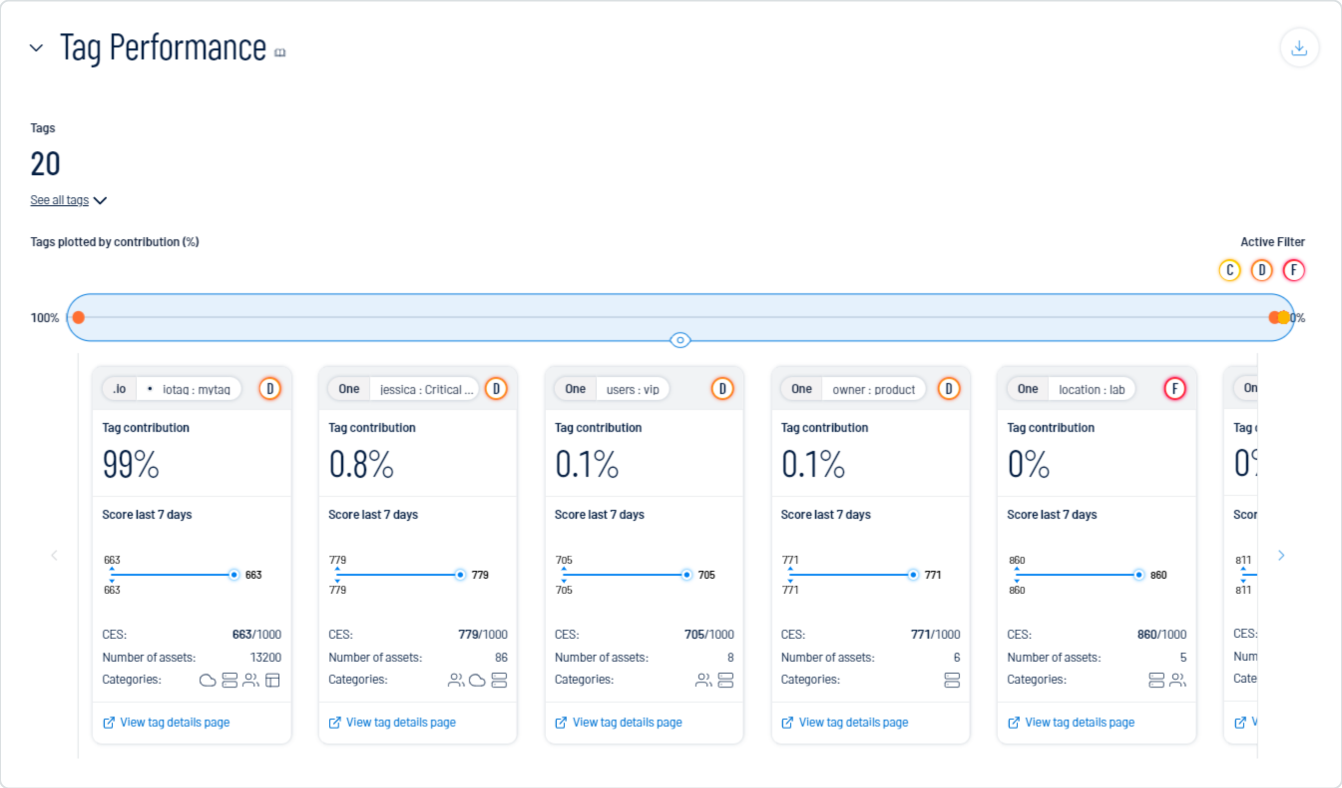
1. Access the Exposure Cards library.

   A list of exposure cards appears.

2. Select the exposure card for which you want to view the tag performance.

   The **Lumin Exposure View** updates based on your selection.

3. Scroll down to the **Tag Performance** section.



Tag Performance

Tags

20

See all tags

Tags plotted by contribution (%)

Active Filter

C D F

100% 0%

.Io · iotag : mytag D
Tag contribution
99%
Score last 7 days
663 663 663
CES: 663/1000
Number of assets: 13200
Categories:
View tag details page

One jessica : Critical ... D
Tag contribution
0.8%
Score last 7 days
779 779 779
CES: 779/1000
Number of assets: 86
Categories:
View tag details page

One users : vip D
Tag contribution
0.1%
Score last 7 days
705 705 705
CES: 705/1000
Number of assets: 8
Categories:
View tag details page

One owner : product D
Tag contribution
0.1%
Score last 7 days
771 771 771
CES: 771/1000
Number of assets: 6
Categories:
View tag details page

One location : lab F
Tag contribution
0%
Score last 7 days
860 860 860
CES: 860/1000
Number of assets: 5
Categories:
View tag details page

On
Tag
0
Scor
811 811
CES:
Num
Cate
V

In the **Tag Performance** section, you can do the following:

- View the number of tags within your Tenable One instance.
  - To see a list of all tags, click **See all tags**.

    A list of your tags appears in *Category*:*Value* pair format.
  - Click on a tag *Category*:*Value* pair to view additional details:
    - **Tag Type** – The tag type (e.g., static).
    - **Data Source** – The application in which the tag was created. For more information, see Data Sources.
    - **Show connected assets** – Click to view a list of assets to which the tag is applied. Tenable One redirects you to the **Asset Overview** filtered by the selected tag.
    - **Show tag details** – Click to view all details for the tag. The **Lumin Exposure View** redirects you to the **Tag Details** page within the **Asset Inventory**.
- View a plot point graph of your tags based on the percentage of their contribution.

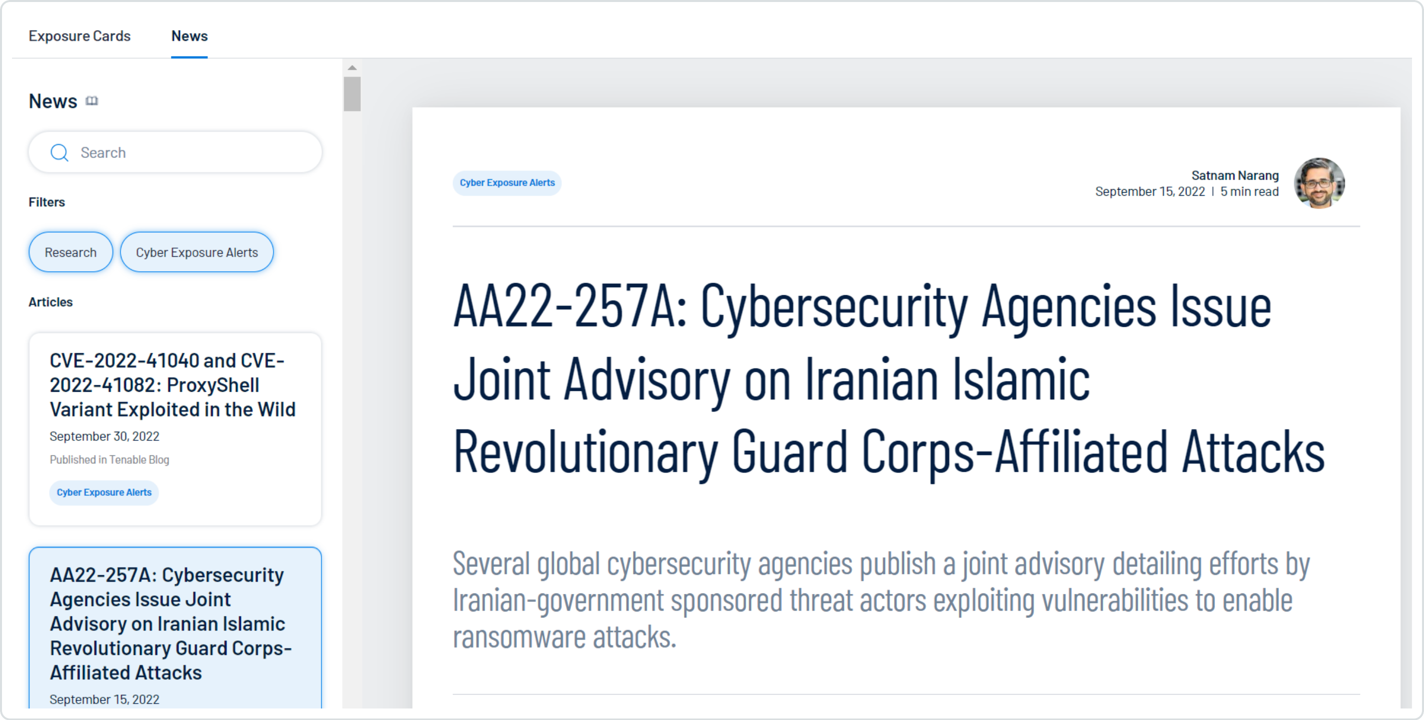
  > **Tip:** Click on a plot point to highlight the corresponding tile below.

  > **Note:** Because an asset can be tagged with more than one tag, tags can overlap, causing your total percentage to exceed 100%.
- In the **Active Filter** section, click on a letter grade score to filter all data in the **Tag Performance** widget by tags that fall under the selected score.
- View tiles that highlight the performance of each tag. On any tile, you can:
  - View the name of the *Category*:*Value* pair.
  - View a letter grade representation of your CES grade as it compares to your industry and the total population.
  - View the **Tag contribution** percentage (i.e., the percentage of your CES score that comes from assets to which this tag is applied).
  - View a graphical representation of the CES trend over the last 7 days.
  - View the tag CES.

- View the **Number of assets** to which the tag is applied.
- View the **Categories** to which the tag belongs. For more information, see Lumin Exposure View Metrics.
- Click **View tag details page** to navigate directly to the **Tag Details** page within the **Asset Inventory**.
- To the right of the tiles, click the › button to scroll through available tiles.

View News Events

The **News** section of the **Lumin Exposure View** lists Tenable blog posts related to vulnerability events. These posts highlight the background of the vulnerability as well as potential impact.



CVE-2022-41040 and CVE-2022-41082: ProxyShell Variant Exploited in the Wild
September 30, 2022
Published in Tenable Blog
Cyber Exposure Alerts

AA22-257A: Cybersecurity Agencies Issue Joint Advisory on Iranian Islamic Revolutionary Guard Corps-Affiliated Attacks
September 15, 2022

Cyber Exposure Alerts

Satnam Narang
September 15, 2022 | 5 min read

AA22-257A: Cybersecurity Agencies Issue Joint Advisory on Iranian Islamic Revolutionary Guard Corps-Affiliated Attacks

Several global cybersecurity agencies publish a joint advisory detailing efforts by Iranian-government sponsored threat actors exploiting vulnerabilities to enable ransomware attacks.

To view news events:

1. Access the Lumin Exposure View.
2. On the left side of the page, click the **News** tab.

   A list of news events appears.
3. (Optional) Use the **Search** box to search for a specific news event.
4. (Optional) Click an event type button in the in the **Filters** section to filter the list of news events.
5. In the left panel, in the **Articles** section, click a post to expand the full details of the event.

View Comment Notifications

When someone comments on the **Lumin Exposure View**, a notification appears in the **Comments** window. For more information about commenting on the **Lumin Exposure View**, see Comment on the Lumin Exposure View.

To view comment notifications:

1. Access the **Lumin Exposure View**.
2. In the upper-right corner, click the 🗨 button.

   The **Comments** window appears and shows your unseen comments and replies.
3. (Optional) To reply to a comment, click on the comment.

   The **Comments** pane appears and displays the selected comment.

   a. In the text box, type your comment.

   b. (Optional) To include a snapshot of the section on which you want to comment, select the **Include snapshot** check box.

   c. Click the ⬆ button.

   The **Lumin Exposure View** posts your reply. Depending on their permissions and notification settings, the **Lumin Exposure View** notifies other users about your comment.

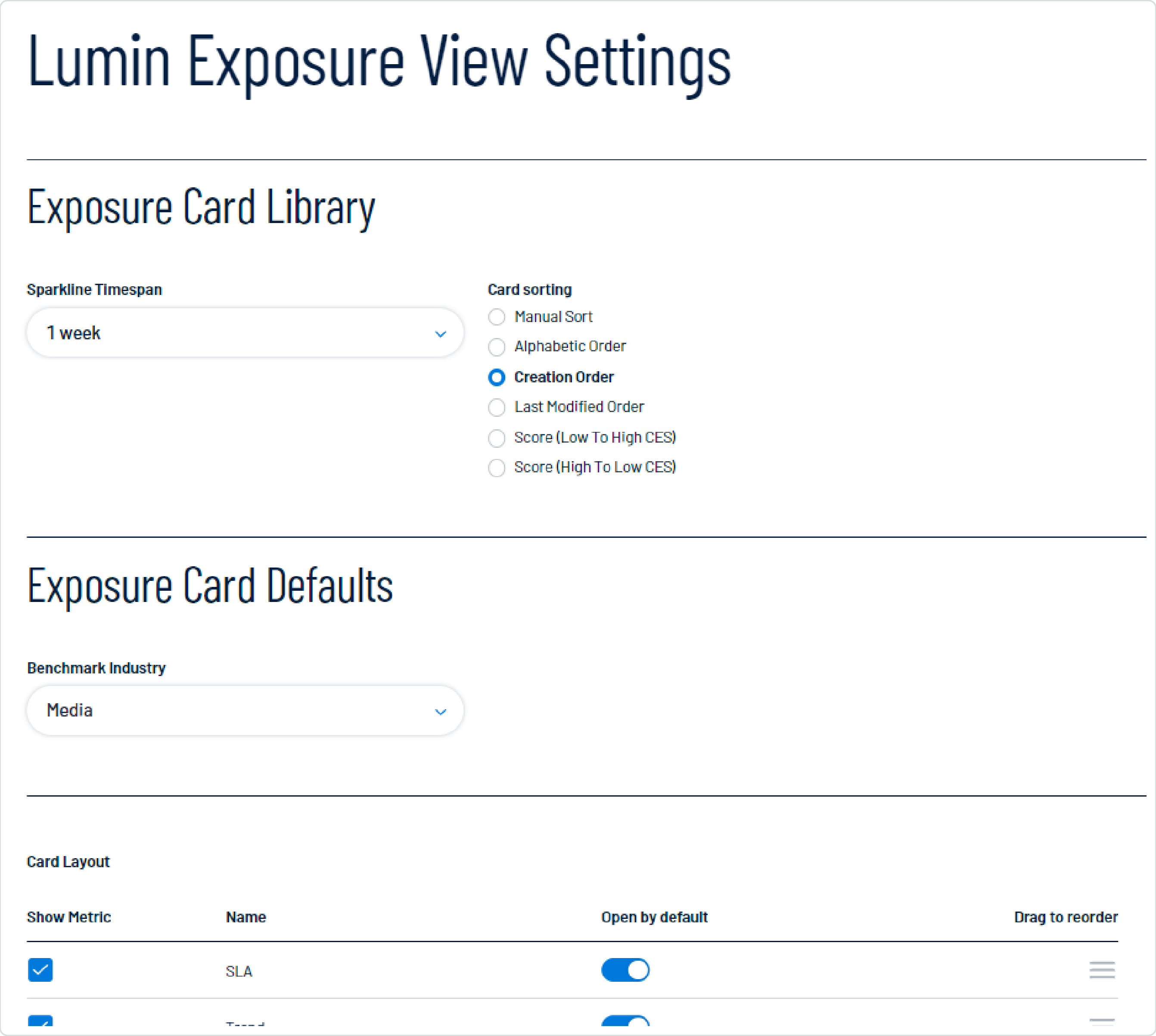
Configure Lumin Exposure View Settings

You can configure how data appears within the Lumin Exposure View, including system defaults and benchmarks, layouts, and data sorting.

To configure your Lumin Exposure View settings:

1. Access the Exposure Cards library.
2. In the upper-right corner, click the ⚙ button.

   The **Lumin Exposure View Settings** page appears.



Lumin Exposure View Settings

Exposure Card Library

Sparkline Timespan: 1 week

Card sorting

- ○ Manual Sort
- ○ Alphabetic Order
- ● Creation Order
- ○ Last Modified Order
- ○ Score (Low To High CES)
- ○ Score (High To Low CES)

Exposure Card Defaults

Benchmark Industry: Media

Card Layout

Show Metric	Name	Open by default	Drag to reorder
☑	SLA	●	☰

3. (Optional) Configure settings in the following sections:

- Exposure Card Library

Option	Description
Sparkline Timespan	In the drop-down menu, select the timespan to use for the sparkline preview on exposure cards within the **Exposure Cards** library.
Card sorting	Select the radio button for how you want to sort the cards within the **Exposure Cards** library.

- Exposure Card Defaults

Option	Description
Benchmark Industry	In the drop-down menu, select the industry to use as a benchmark when comparing your metrics. For more information, see Lumin Exposure View Metrics.
Show Metric	Do any of the following: ◦ Select the check box next to any metric that you want to include in the **Lumin Exposure View**. ◦ Deselect the check box next to any metric that you do not want to include in the **Lumin Exposure View**.
Name	View the name of the metric for which you're configuring the card layout.
Open by default	Do any of the following: ◦ Enable the toggle for any metric that you want to open by default when viewing the **Lumin Exposure View**. ◦ Disable the toggle for any metric that you do not want to open by default when viewing the **Lumin Exposure View**.
Drag to reorder	Drag and drop the rows of metrics to edit the order in

	which they appear within the **Lumin Exposure View**.
Card Targets	The **Card Targets** section allows you set the overall target for the card. Select the radio button next to one of the following options: ○ **Custom** – Manually select a target benchmark for the exposure card by doing one of the following: ■ In the text box, manually type a target benchmark number for the card. ■ Click and drag the slider to select a target benchmark number for the card. ○ **Set to Industry Benchmark** – Automatically set the target to match the industry benchmark for the data. ○ **Set to Population Benchmark** – Automatically set the target to match the population benchmark for the data.
Category Targets ○ **Computing Resources** ○ **Cloud Resources** ○ **Identities** ○ **Web Applications**	The **Category Targets** section allows you set the target benchmark for each individual category whose data populates the **Lumin Exposure View**. For each category, select the radio button next to one of the following options: ○ **Custom** – Manually select a target benchmark for the category by doing one of the following: ■ In the text box, manually type a target for the category. ■ Click and drag the slider to select a target for the category.

	○ **Set to Industry Benchmark** – Automatically set the target to match the industry benchmark for the data. ○ **Set to Population Benchmark** – Automatically set the target to match the population benchmark for the data.

- ## Trend

Option	Description
Default Timespan Shown	In the drop-down menu, select the timespan to use for the Trend section within the **Lumin Exposure View**.

- ## Remediation SLA

Option	Description
Risk Severity	Do any of the following: ○ Select the check box next to any risk severity you want to include within the Remediation SLA section in the **Lumin Exposure View**. ○ Deselect the check box next to any risk severity you want to include within the Remediation SLA section in the **Lumin Exposure View**.
Data Categories /Remediation (in days)	For each data category, type the number of days within which each risk level of SLA must be addressed. For example, if you have an internal SLA to address critical **Computing Resources** risks within 4 days, in the **Critical** text box for that category, type **4**.
SLA Efficiency Target	For each risk severity, drag the slider to set the SLA efficiency target percentage to use within the **Lumin Exposure View**.

Graph Range	For each risk range, type the date range to use for the graph in the **SLA** section within the Lumin Exposure View.

4. Click **Save** 🖫.

   The **Lumin Exposure View** saves your configuration updates and applies any changes.

Export Lumin Exposure View Data

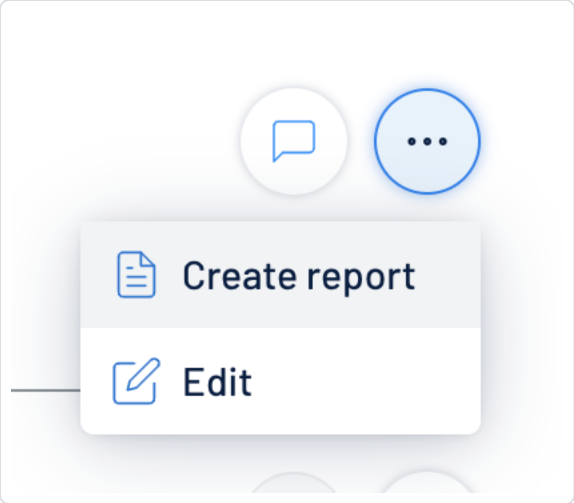
You can export **Lumin Exposure View** data in the following ways:

- Expor the entire **Exposure View** in .pdf format
- Export a single section of the **Lumin Exposure View** in .png format.

To export the entire Lumin Exposure View:

1. Access the **Lumin Exposure View**.
2. In the upper right corner, click the ⋯ button.

   A menu appears.



3. Click **Create Report**.

   The **Lumin Exposure View** downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

To export a single section of the Lumin Exposure View:

1. Access the **Lumin Exposure View**.
2. Scroll to the section of the **Lumin Exposure View** that you want to export.
3. Click the ⤓ button.

The **Lumin Exposure View** downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

Share the Lumin Exposure View

You can share the exposure card data from custom exposure cards with other users within your Tenable One instance. This allows you to forward all data associated with an exposure card for analysis and prioritization.

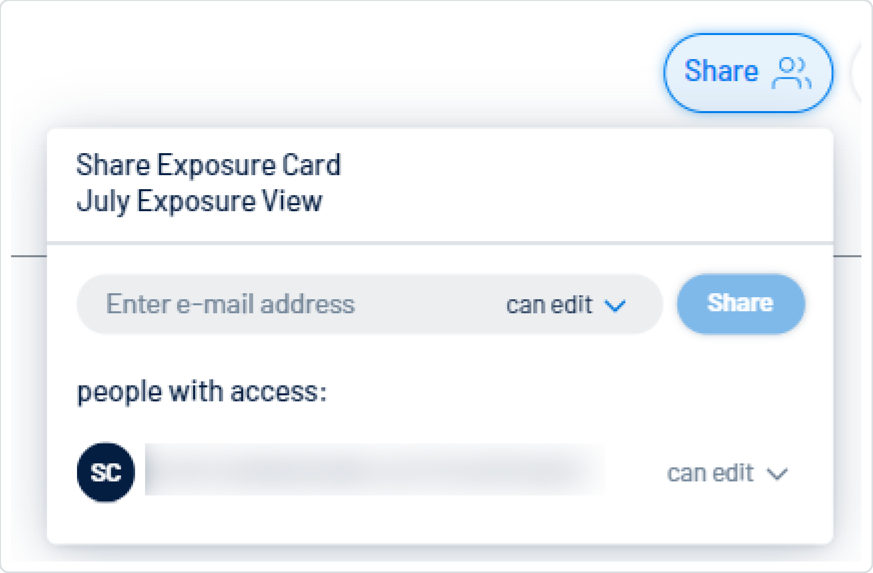
Before you begin:

Ensure the user with which you want to share has the appropriate access.

To share exposure card data:

1. Access the **Lumin Exposure View**.
2. In the **Exposure Cards** library, select the custom exposure card you want to share.
3. Click **Share** 👥.

   The **Share Exposure Card** window appears.

4. In the search box, type the email address of the user or users with which you want to share the exposure card data.

   > **Tip:** Below the search box, in the **People with access** section, you can view which users have access to the data.

5. In the drop-down menu, select the access you want to grant to the user with which you are sharing the exposure card data. For example, if you want to allow the user to comment on the data, select **can comment**.

6. Click **Share**.

   The **Lumin Exposure View** shares the exposure card data with the selected users. Selected users receive notification emails.

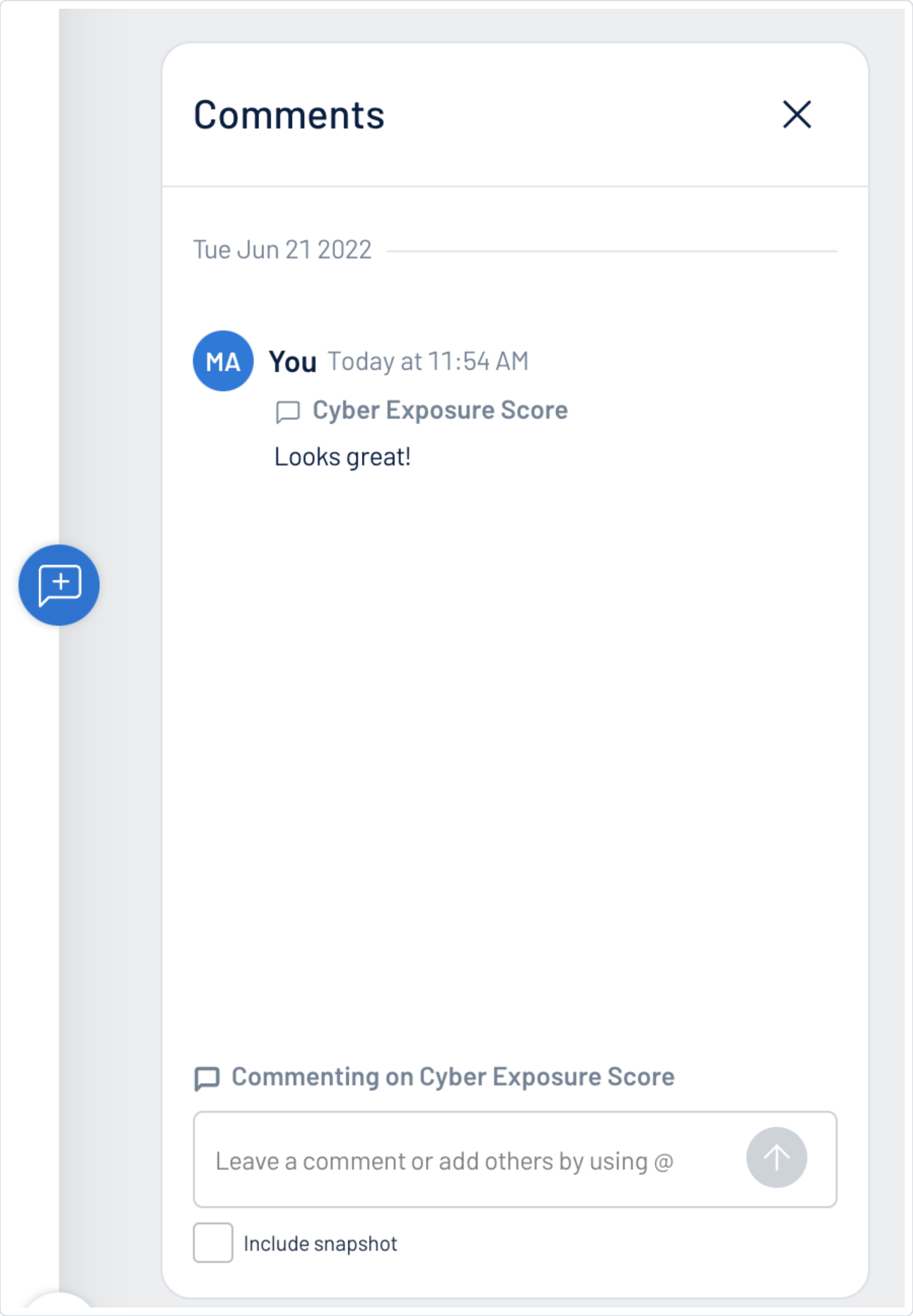
Comment on the Lumin Exposure View

You can comment on any section within the **Exposure View**. Depending on their permissions and notification settings, users within your Tenable One instance can view your comments. For more information, see View Comment Notifications.

To comment on the Lumin Exposure View:

1. Access the **Exposure View**.
2. Do one of the following:
   - In the upper-right corner of the view, click the 🗨 button.
   - Scroll to the section on which you want to comment and click the ⊞ button.

   The **Comments** pane appears.



Comments

Tue Jun 21 2022

MA **You** Today at 11:54 AM

Cyber Exposure Score

Looks great!

Commenting on Cyber Exposure Score

Leave a comment or add others by using @

□ Include snapshot

Tip: If you scroll up or down within the **Lumin Exposure View**, the **Comments** pane automatically adjusts to add the comment to the currently displayed widget.

3. In the text box, type your comment.
4. (Optional) To include a snapshot of the section on which you want to comment, select the **Include snapshot** check box.
5. Click the ↑ button.

   The **Lumin Exposure View** posts your reply. Depending on their permissions and notification settings, the **Lumin Exposure View** notifies other users about your comment. For more information, see View Comment Notifications.

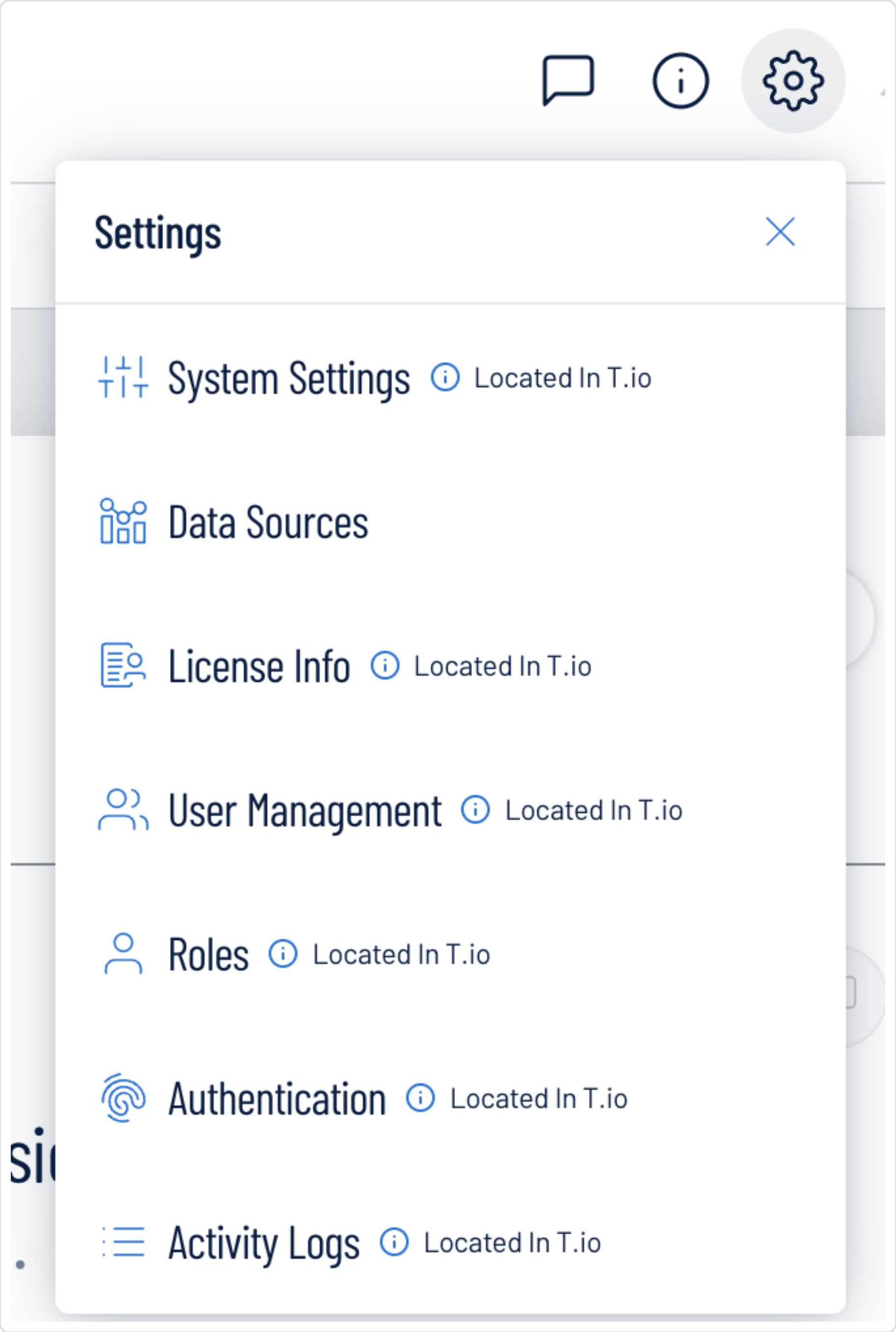
Access the Settings Menu

The **Settings** menu gives you access to user and settings options.

To access the **Settings** menu:

1. In the upper-right corner, click the ⚙ button.

   The **Settings** menu appears.


Settings
System Settings ⓘ Located In T.io
Data Sources
License Info ⓘ Located In T.io
User Management ⓘ Located In T.io
Roles ⓘ Located In T.io
Authentication ⓘ Located In T.io
Activity Logs ⓘ Located In T.io

2. Click one of the following options:

   - System Settings – View and manage settings for your container.
   - Data Sources – View all products feeding data into the Lumin Exposure View interface.
   - License Information – View your license information.

- User Management – View and manage all users, groups, and permissions.
- Roles – View and manage your Lumin Exposure View roles.
- Authentication – View and manage your user authentication settings.
- Activity Logs – View user activity logs.

System Settings

The **System Settings** option in the **Settings** menu directs you to the **Settings** page, where you can interact with all system settings options.

> **Note:** These settings are managed directly within Tenable Vulnerability Management. When you access the this section, you are automatically redirected to the Tenable Vulnerability Management user interface.

To access the Settings page:

1. Access the **Settings** menu.
2. Click **System Settings**.

   The **Settings** page appears. For more information, see Settings within the *Tenable Vulnerability Management User Guide* .

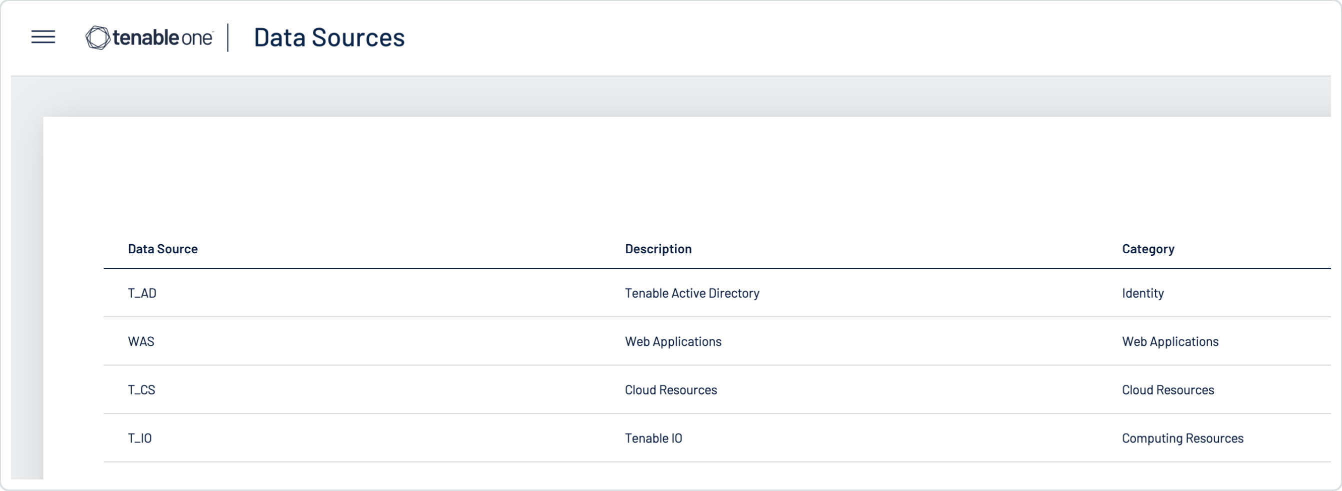
Data Sources

A data source is any product that feeds data into the Lumin Exposure View interface. By default, Lumin Exposure View automatically ingests data from any Tenable product for which you have a license. On the **Data Sources** tab, you can view details for each data source.

To view the **Data Sources** page:

1. Access the **Settings** menu.
2. Click **Data Sources**.

   The **Data Sources** page appears.



Data Source	Description	Category
T_AD	Tenable Active Directory	Identity
WAS	Web Applications	Web Applications
T_CS	Cloud Resources	Cloud Resources
T_IO	Tenable IO	Computing Resources

On the **Data Sources** page, you can view the following information:

Column	Description
Data Source	The product feeding data into the Lumin Exposure View interface.
Description	A description of the data source.
Category	The category to which the data source belongs. For more information, see Lumin Exposure View Metrics.

License Information

The **License Info** option in the **Settings** menu directs you to the **License** page, where you can view license information.

> **Note:** These settings are managed directly within Tenable Vulnerability Management. When you access the this section, you are automatically redirected to the Tenable Vulnerability Management user interface.

To access the License page:

1. Access the **Settings** menu.
2. Click **License Info**.

   The **License** page appears. For more information, see View License Information within the *Tenable Vulnerability Management User Guide* .

User Management

The **User Management** option in the **Settings** menu directs you to the **Users** page, where you can interact with all user management options.

> **Note:** These settings are managed directly within Tenable Vulnerability Management. When you access the this section, you are automatically redirected to the Tenable Vulnerability Management user interface.

To access the Users page:

1. Access the **Settings** menu.
2. Click **User Management**.

   The **Users** page appears. For more information, see Users within the *Tenable Vulnerability Management User Guide* .

Roles

Roles allow you to manage privileges for major functions and control which Lumin Exposure View resources users can access.

> **Note:** These settings are managed directly within Tenable Vulnerability Management. When you access the this section, you are automatically redirected to the Tenable Vulnerability Management user interface.

When you create a user, you must select a role for that user that broadly determines the actions the user can perform. For more information, see Users.

> **Caution:** If you don't have two-factor authentication configured, be sure to disable the **Two-Factor Required** toggle when creating a user. Failure to do so can cause the user interface to display incorrectly for the user.

> **Note**: You can further refine user access to specific resources by assigning permissions to individual users or groups. For more information, see Permissions.

The Lumin Exposure View interface supports the following role types:

- Administrator — Has all permissions and privileges, is responsible for setting up the account, and knows the organization's architecture. They can create groups to organize different business units, and add and manage users on the account.
- Custom — Has custom applied privileges specific to organizational needs. For more information, see the following documentation in the *Tenable Vulnerability Management User Guide*:
    - Custom Roles
        - Create a Custom Role
        - Duplicate a Role
        - Edit a Custom Role
        - Delete a Custom Role
    - Export Roles

Authentication

The **Authentication** option in the **Settings** menu directs you to the **My Account** page, where you can interact with all authentication options.

> **Note:** These settings are managed directly within Tenable Vulnerability Management. When you access the this section, you are automatically redirected to the Tenable Vulnerability Management user interface.

To access the My Account page:

1. Access the **Settings** menu.
2. Click **Authentication**.

   The **My Account** page appears. For more information, see My Account within the *Tenable Vulnerability Management User Guide* .

Activity Logs

The **Activity Logs** option in the **Settings** menu directs you to the **Activity Logs** page, where you can view activity log information.

> **Note:** These settings are managed directly within Tenable Vulnerability Management. When you access the this section, you are automatically redirected to the Tenable Vulnerability Management user interface.

To access the System Settings page:

1. Access the **Settings** menu.

2. Click **Activity Logs**.

   The **Activity Logs** page appears. For more information, see Activity Logs within the *Tenable Vulnerability Management User Guide* .