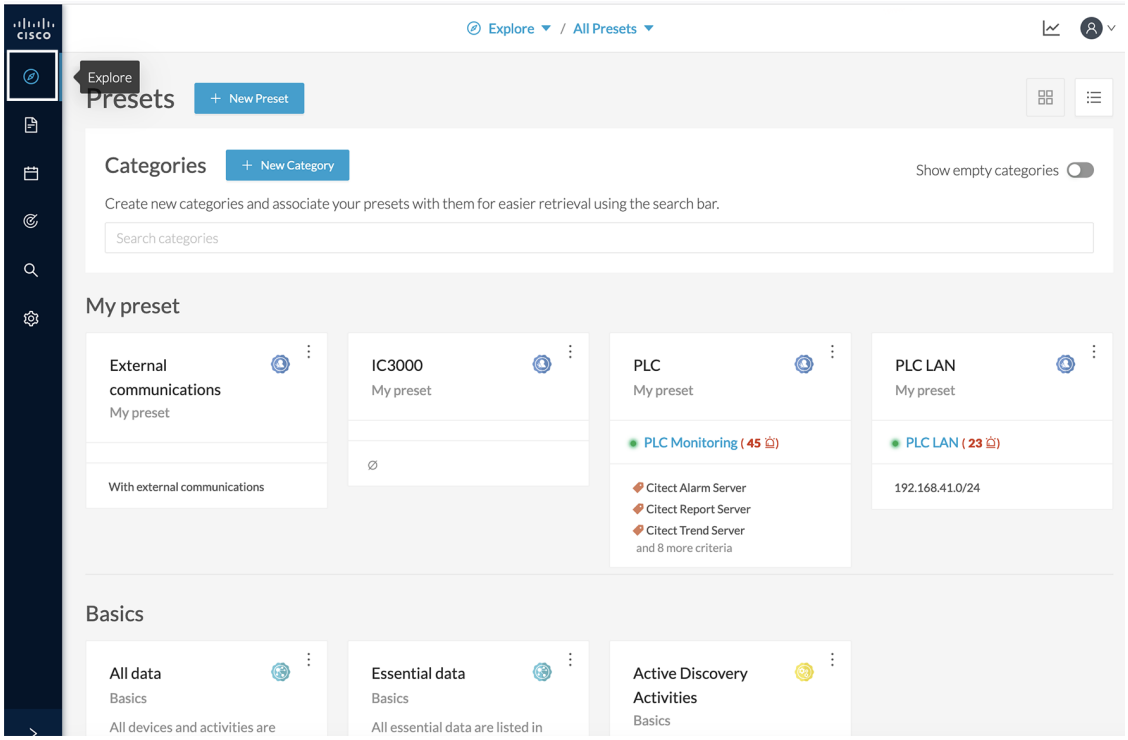
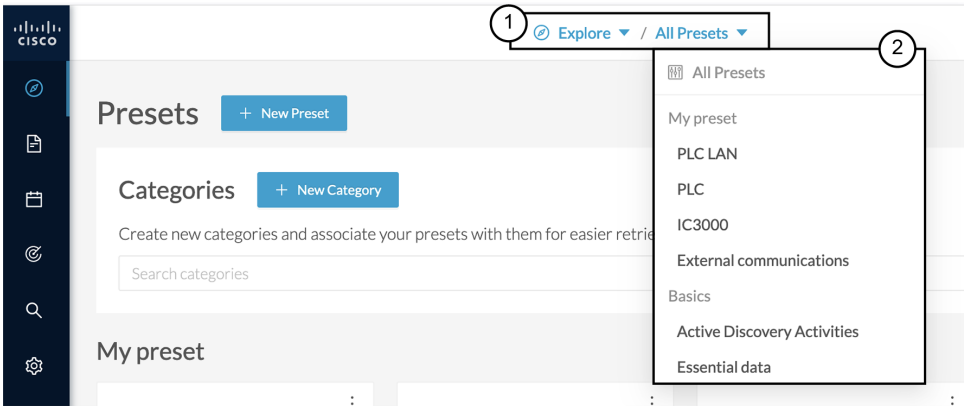
Explore

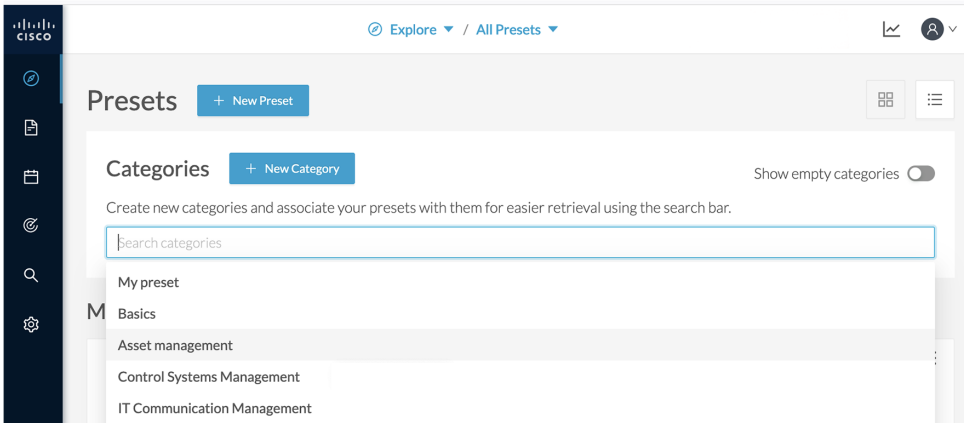
Explore shows an overview of all the Presets in Cisco Cyber Vision, both defaults and custom presets. Click **Explore** on the left navigation bar.



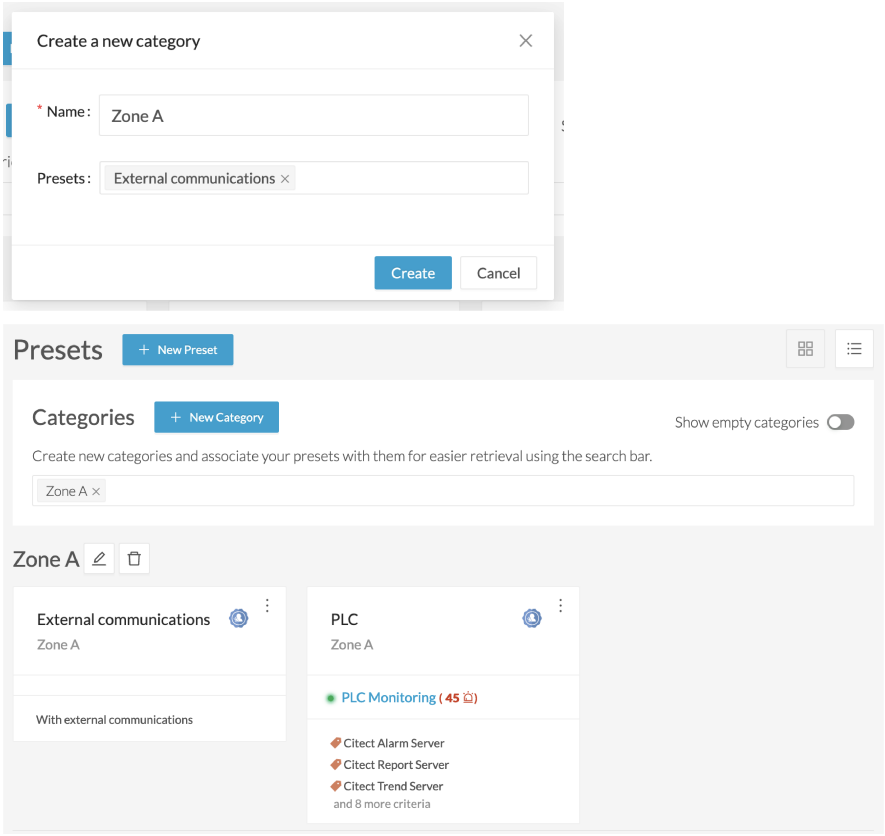
Use the top navigation bar **(1)** to access the different presets **(2)** and Preset views.



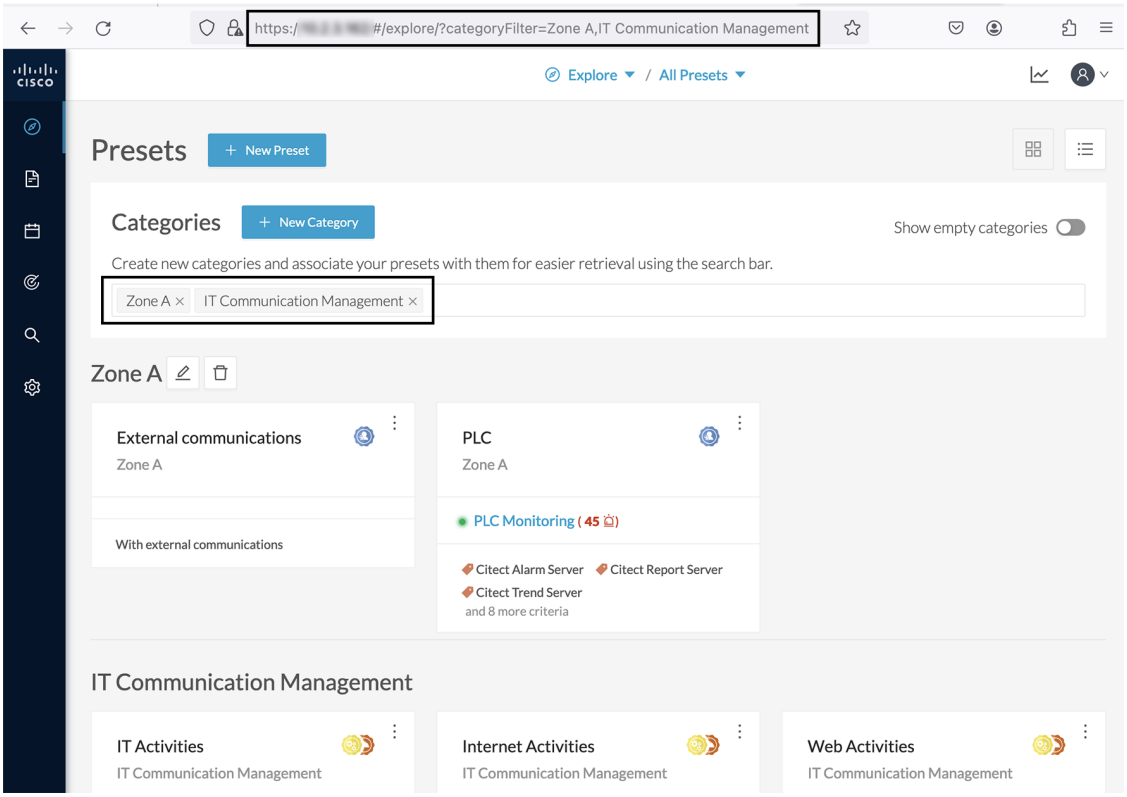
You can also filter presets by categories.



Create new categories to order and search your custom presets.



Filters included in Cisco Cyber Vision Explore page's url allow you to save the selection in your browser's favorites.



- Preset views, on page 4
- Detail panel, on page 15

Preset views

There are several types of views which relate to different perspectives. Using the top navigation bar to access the views, click **Explore > All Data**. The **Dashboard** menu adds.

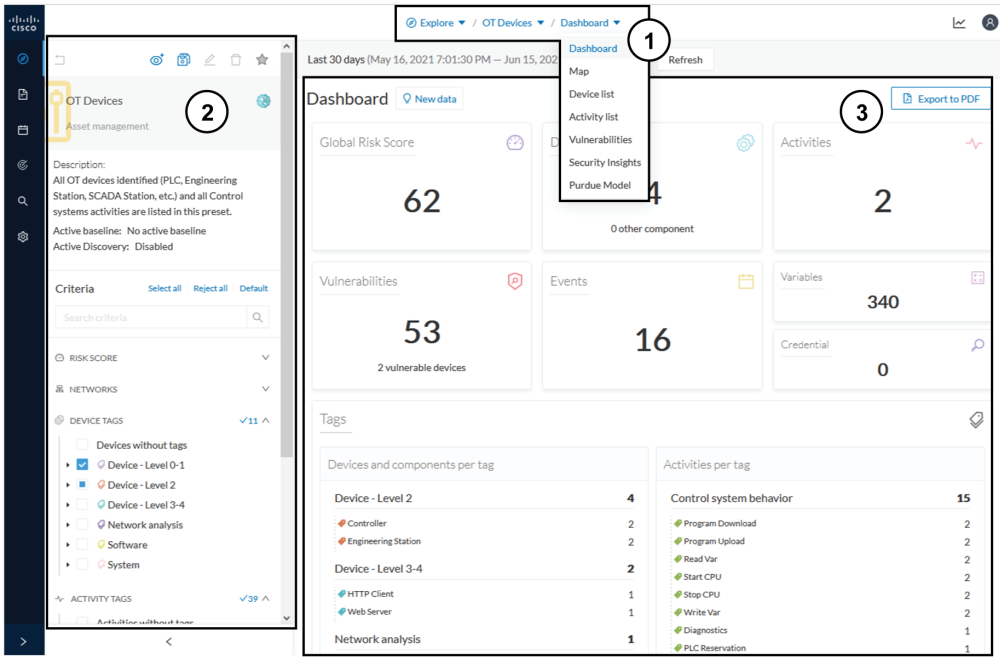
- **Dashboard** view is the default which gives the preset data overview. It is a tag-oriented view showing general insight of the network, without going into deep and technical details.
- **Map** is visual data of the industrial network that gives you a broad insight of how components are connected to each other.
- **Lists**, **Device list** or **Activity list**, show classic but powerful data filtering to match what you are looking for. For more information, refer to the Device and activity lists.
- **Purdue Model** shows how the components of a preset are distributed among the layers of the Purdue Model architecture.

Views are always structured as shown below:

- Use the top navigation bar **(1)** pull-down menus to easily switch between the different views.
- Use the left panel **(2)** to filter, modify, and manage the preset data by adapting criteria and registering changes.

- The center panel **(3)** dynamically changes as you save criteria.

Below is an example of the OT Devices preset on the Dashboard view.

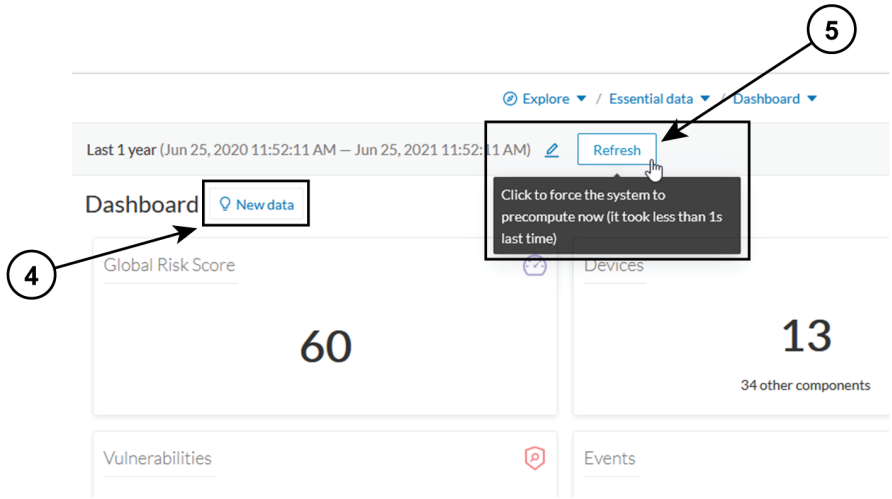


The preset view is optimized to avoid lags, to solve performance issues, and to prevent the application from crashing, especially in case of large data flow. Since Cisco Cyber Vision version 4.0.0, data elements such as components, tags and activities are stored, instead of being directly displayed in the preset views. Preset views refresh occurs only when necessary or requested. This prevents overloading the application display. The elements visible in the preset views are actually data from the *previous* computation. This means that data displayed in the GUI and data stored in the database are asynchronous, which lightens data load on preset views.

In addition, data computation adapts to the frequency of the preset consultations. That is, a preset often viewed by users computes accordingly. Conversely, the system does not compute presets that are *never* used.

When on a preset, data is regularly computed by an automatized data computation running in the background. However, this does not refresh the preset view. Two buttons are available in the preset view to act independently whether on the database or on the preset view to lighten the load on the system:

- The **New data** button **(4)** appears each time a new computation is done. Click it to update the view. *The new view may not show new data*.
- The **Refresh** button **(5)** forces data computation and refreshes the preset view. This task requires more resources. Use **Refresh** for the following cases:
  - If you suspect that new data was found during the most recent computation (e.g., a new device plugged into the network).
  - If custom data such as groups or names has been changed (e.g., if adding a device into a group).



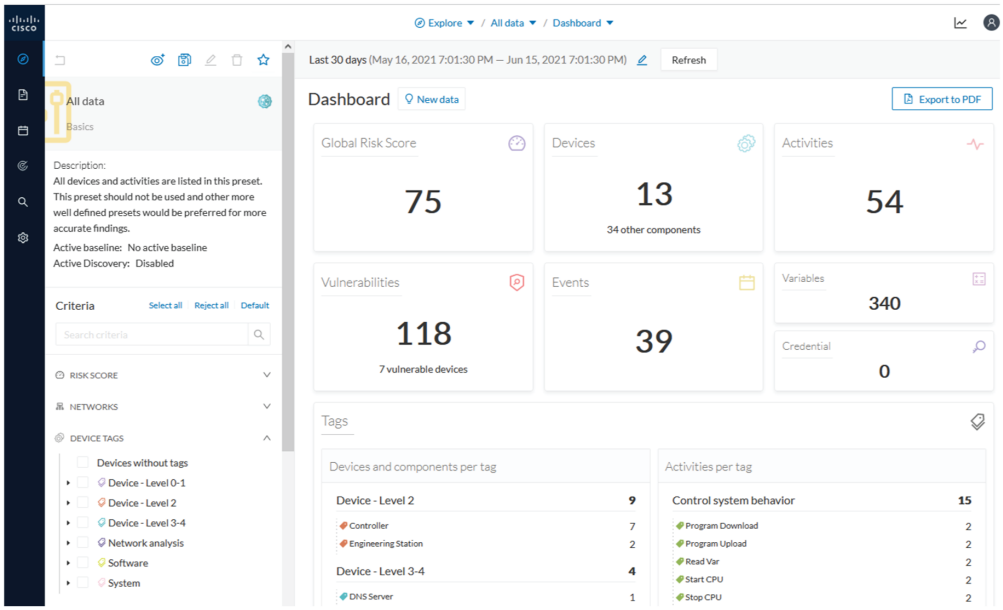
In many cases, computation is forced and the view refreshes as you navigate in the application. For example, refresh happens when you access another preset or move from one view to another.

Note New preset view optimization also has an impact on how criteria are handled in preset views. Save new data in a new or custom preset.

Dashboard

Dashboard is the preset default view. **Dashboard** shows an overview of the preset's global risk score, the number of devices, activities, vulnerabilities, events, variables and credentials.

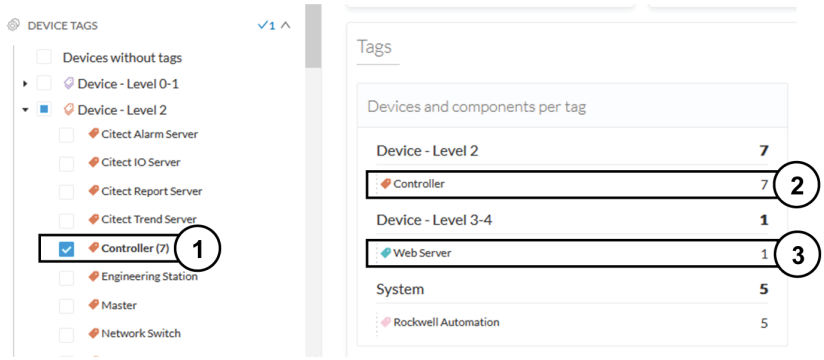
Dashboard also shows **Tags**. The **Tag** pane shows all tags found, including tags set as criteria and shows the number of devices and activities found per tag.



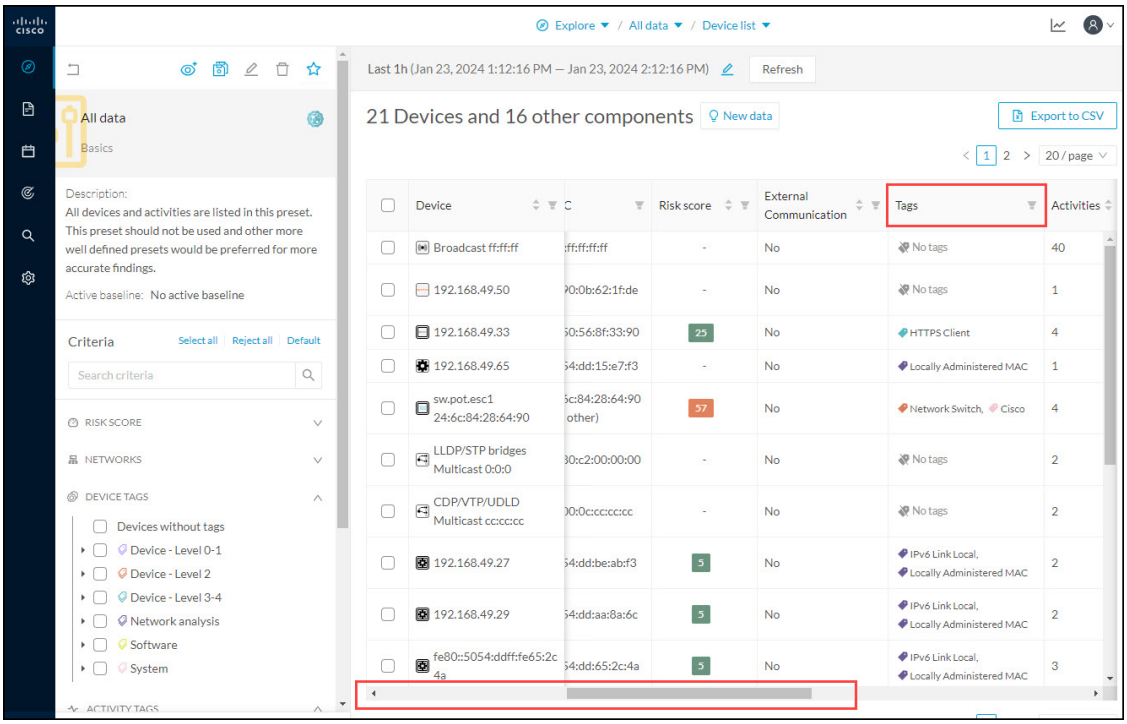
For example:

1. Click **Explore > All Data > Dashboard** from the top navigator menu.
2. Click **Device Tags** from the left panel.
3. Select the **Controller** tag as criteria (under Device - Level 2), and save the selection as "Example: Controller tag."

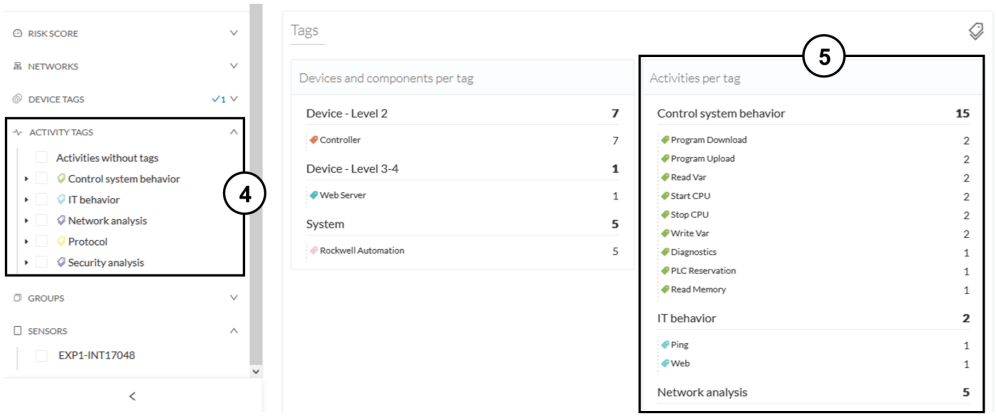
Devices per tag: The number in brackets indicates there are 7 devices tagged as **Controller (1)**. On the **Dashboard**, you see this result **(2)**. One device is tagged as Web Server **(3)**. This means that one of the **Controllers** is a Web Server. Following this logic, we can say that five of the Controllers are Rockwell Automation devices. That leaves one remaining as "unknown."



For more details on these devices, switch to the Device and activity lists and access them using the filter available in the Tags column.



Activities per tag: As for activities, there is no activity tags set as criteria in the example below **(4)**. Yet, you can see that many activities have been found **(5)**. This is because the dashboard view collects all activities involved with the Controller devices found.

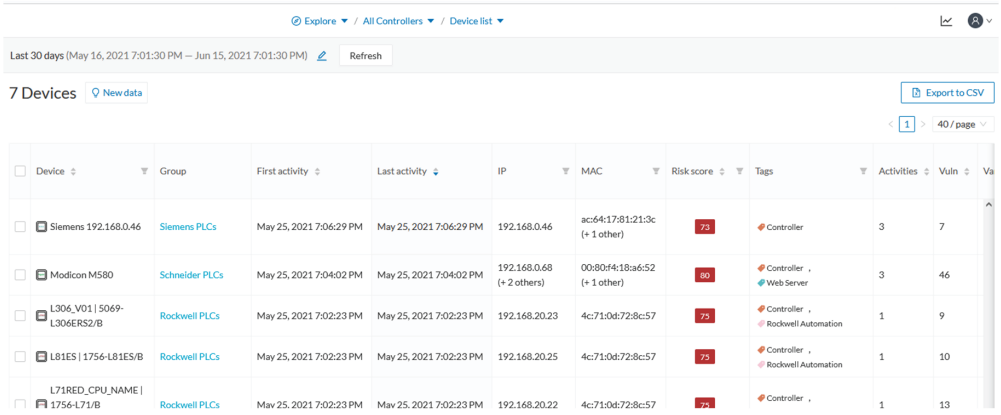


For details on these activities, switch to the Device and activity lists and access them using the filter available in the Tags column.

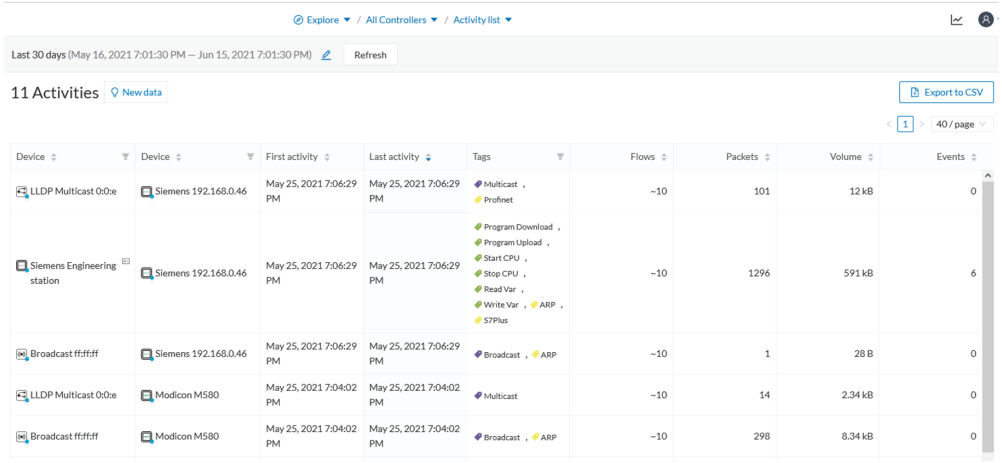
Device and activity lists

The **Device list** and **Activity list** are two specialized views. These views provide general information and advanced technical data about each element in the preset.

Below is an example of the Controllers preset in the Device list view.

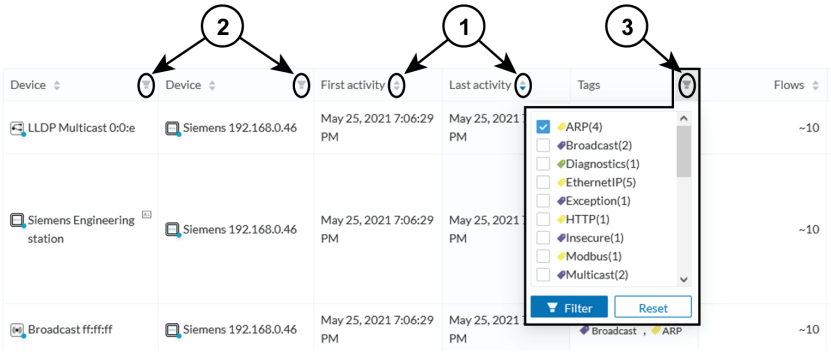


Below is an example of the Controllers preset in the Activity list view.



Lists can provide an in-depth exploration of the network. Use the **Search** function to find very specific data. Use the **Filter** icons in the list columns to sort data.

- The **Sort arrows (1)** list data by alphabetical order or by ascending/descending order. Click again to cancel the **Sort**.
- The **Filter** icon **(2)** opens a field to type specific data in or a multiple-choice menu **(3)** to filter **Tags**.

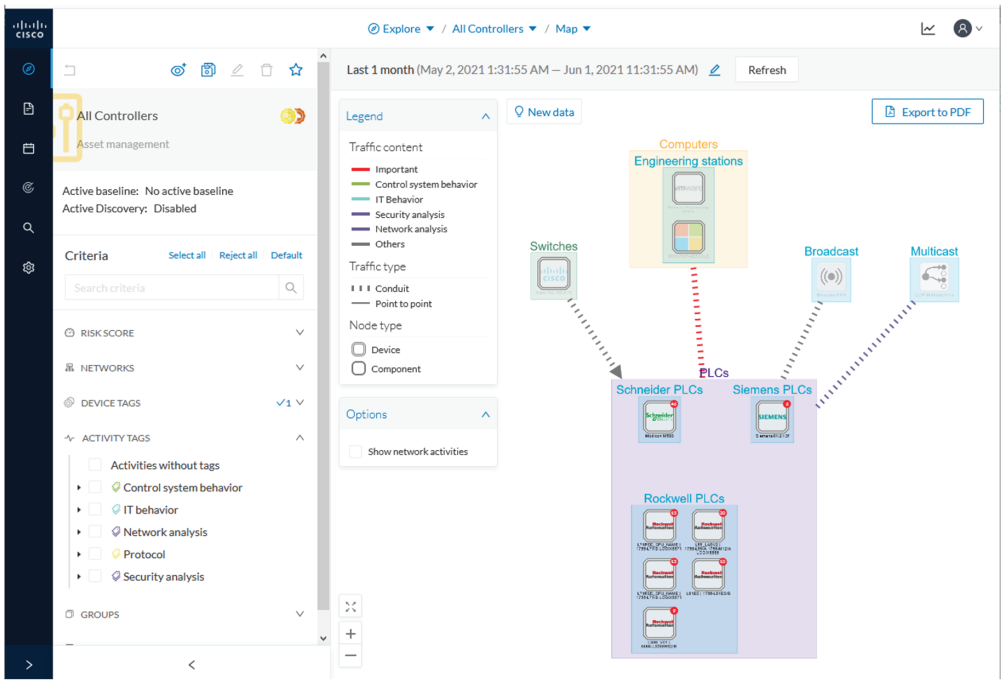


Clicking an element in the lists opens its Detail panel which displays more data.

Map

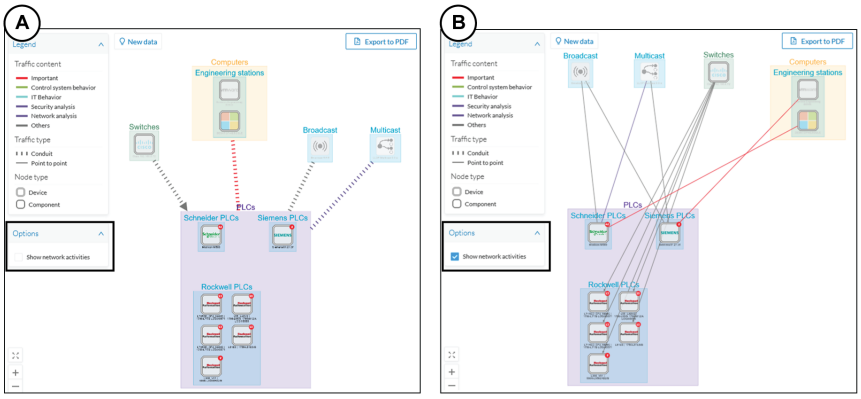
The **Map** view is a visual representation of data of the industrial network that gives you the broadstrokes on how devices and components are interconnected. It shows how the network is structured. **Map** helps you organize components in a way that makes sense to you by creating groups.

Maps displays devices, components, and activities according to criteria set in a preset. **Grayed out devices and components** are displayed because, even if they don't correspond to the preset's criteria, they are necessary to represent the activities of the preset.



Note The **Map** view is ***self-organizing***, that is, elements are redistributed as devices, components, conduits and activities appear or disappear, and as groups are created or deleted. The **Map** automatically adapts over time and when you change a preset. This guarantees that the **Map** is always well organized and components never overlap.

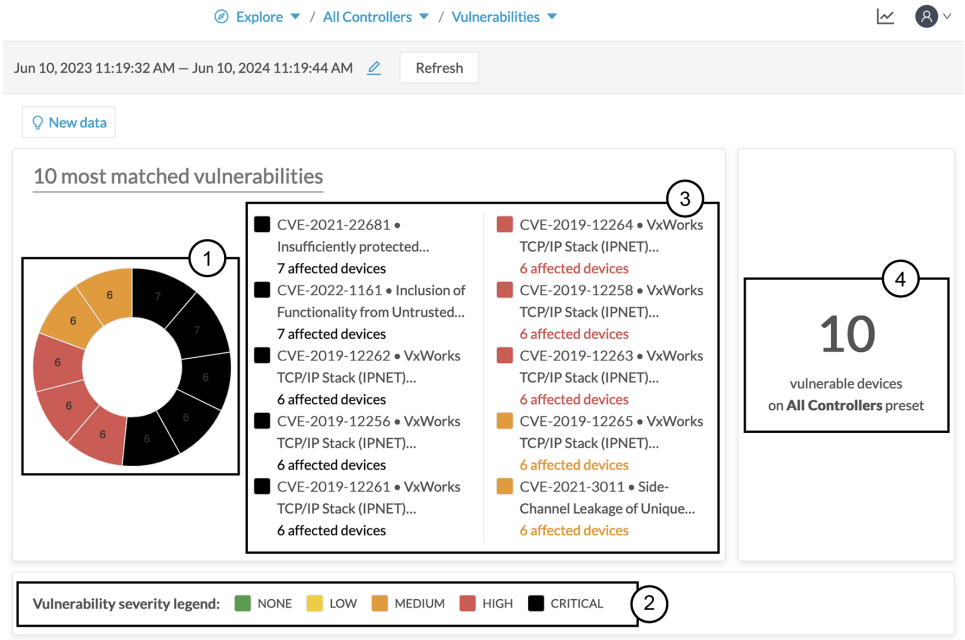
By default, activities between groups are merged and displayed as conduits **(A)**. Select **Show network activities** for a more detailed view **(B)**. To enhance visibility, elements here are also automatically reorganized on the **Map** .



Vulnerabilities

Click **Explore** > **All Data** > **Vulnerabilities** to see a visual representation and a list of the vulnerabilities detected within a preset.

Important If you receive a notification about a new version, update the Knowledge DB in Cisco Cyber Vision as soon as possible. This protects your network against vulnerabilities. Refer to the corresponding documentation.

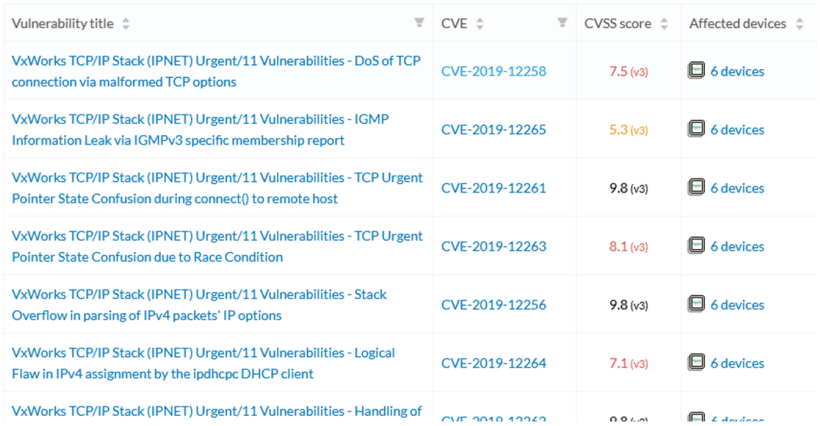


The pie chart shows the 10 most-matched vulnerabilities within the preset and the affected devices **(1)**. The legend below gives you the color code of severity **(2)**. The center panel shows a list of the ten most vulnerabilities **(3)**. Click the hyperlink for an affected device to see the details panel. The right panel shows the total number of devices that are vulnerable in the preset selected **(4)**.

Below is a list of all the vulnerabilities found in the preset. It has **Sort** icons to sort data by alphabetical order or by ascending/descending order, and **Filter** icons, which open a field to type specific data.

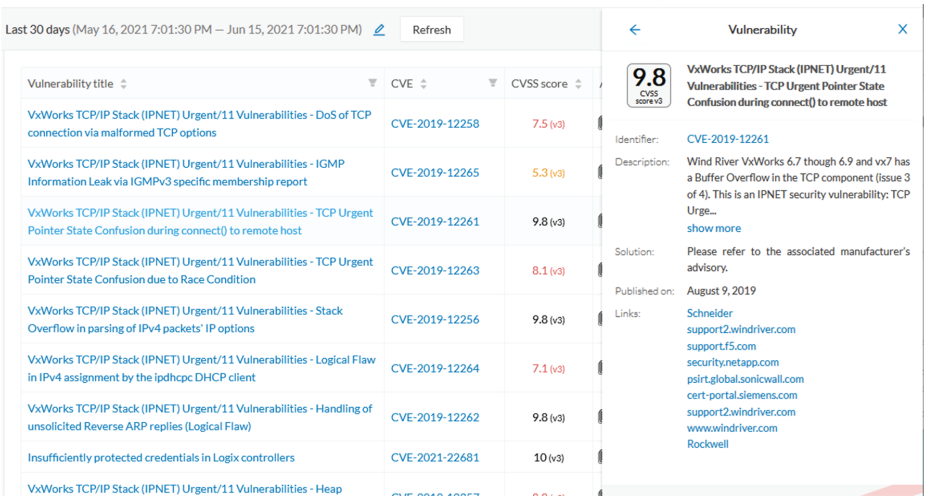
For each vulnerability, the following data is displayed in columns:

- Vulnerability title
- CVE ID (unique identifier for a Common Vulnerability Exposure)
- CVSS score (Common Vulnerability Scoring System)
- Affected devices (by the vulnerability)



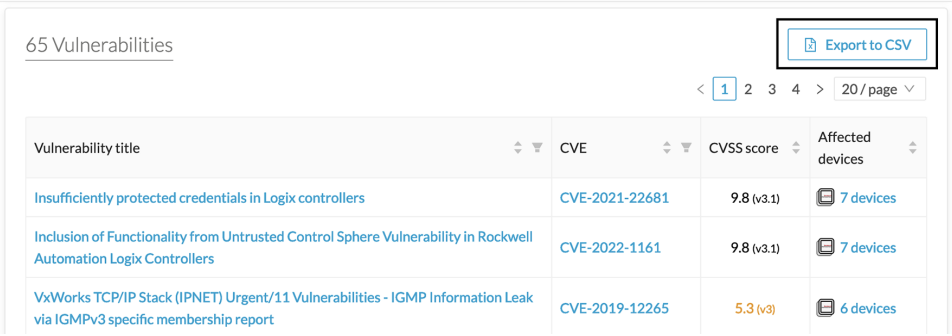
Vulnerability title	CVE	CVSS score	Affected devices
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - DoS of TCP connection via malformed TCP options	CVE-2019-12258	7.5 (v3)	6 devices
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - IGMP Information Leak via IGMPv3 specific membership report	CVE-2019-12265	5.3 (v3)	6 devices
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - TCP Urgent Pointer State Confusion during connect() to remote host	CVE-2019-12261	9.8 (v3)	6 devices
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - TCP Urgent Pointer State Confusion due to Race Condition	CVE-2019-12263	8.1 (v3)	6 devices
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - Stack Overflow in parsing of IPv4 packets' IP options	CVE-2019-12256	9.8 (v3)	6 devices
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - Logical Flaw in IPv4 assignment by the ipdhcpc DHCP client	CVE-2019-12264	7.1 (v3)	6 devices
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - Handling of			

Click an element in the list to open the Detail panel, which includes a link to the National Vulnerability Database.



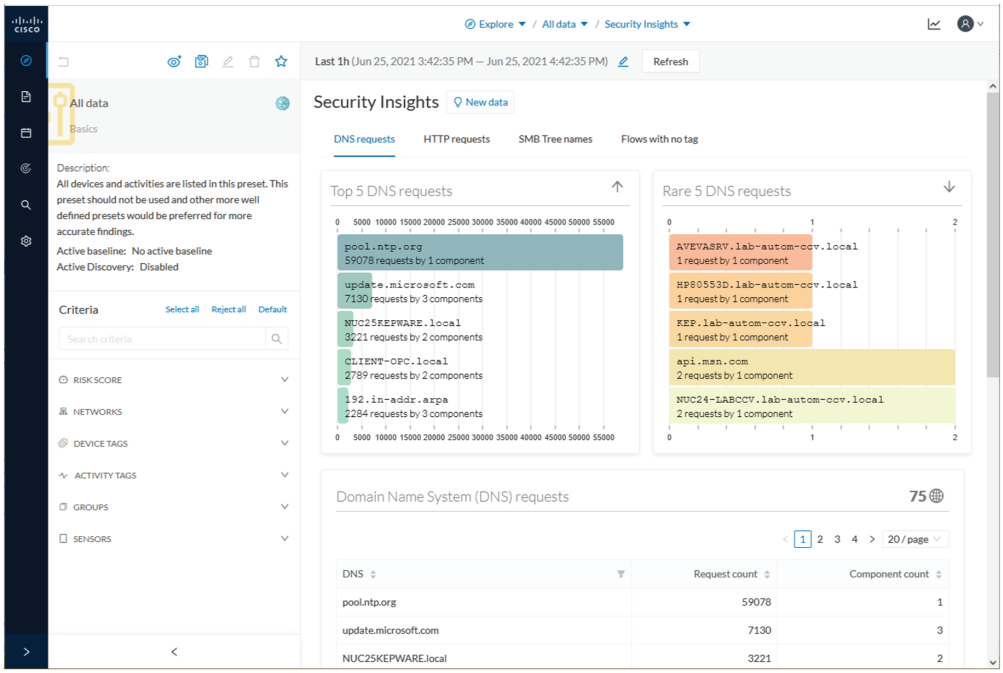
Vulnerability title	CVE	CVSS score
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - DoS of TCP connection via malformed TCP options	CVE-2019-12258	7.5 (v3)
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - IGMP Information Leak via IGMPv3 specific membership report	CVE-2019-12265	5.3 (v3)
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - TCP Urgent Pointer State Confusion during connect() to remote host	CVE-2019-12261	9.8 (v3)
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - TCP Urgent Pointer State Confusion due to Race Condition	CVE-2019-12263	8.1 (v3)
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - Stack Overflow in parsing of IPv4 packets' IP options	CVE-2019-12256	9.8 (v3)
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - Logical Flaw in IPv4 assignment by the ipdhcpc DHCP client	CVE-2019-12264	7.1 (v3)
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - Handling of unsolicited Reverse ARP replies (Logical Flaw)	CVE-2019-12262	9.8 (v3)
Insufficiently protected credentials in Logix controllers	CVE-2021-22681	10 (v3)
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - Heap		

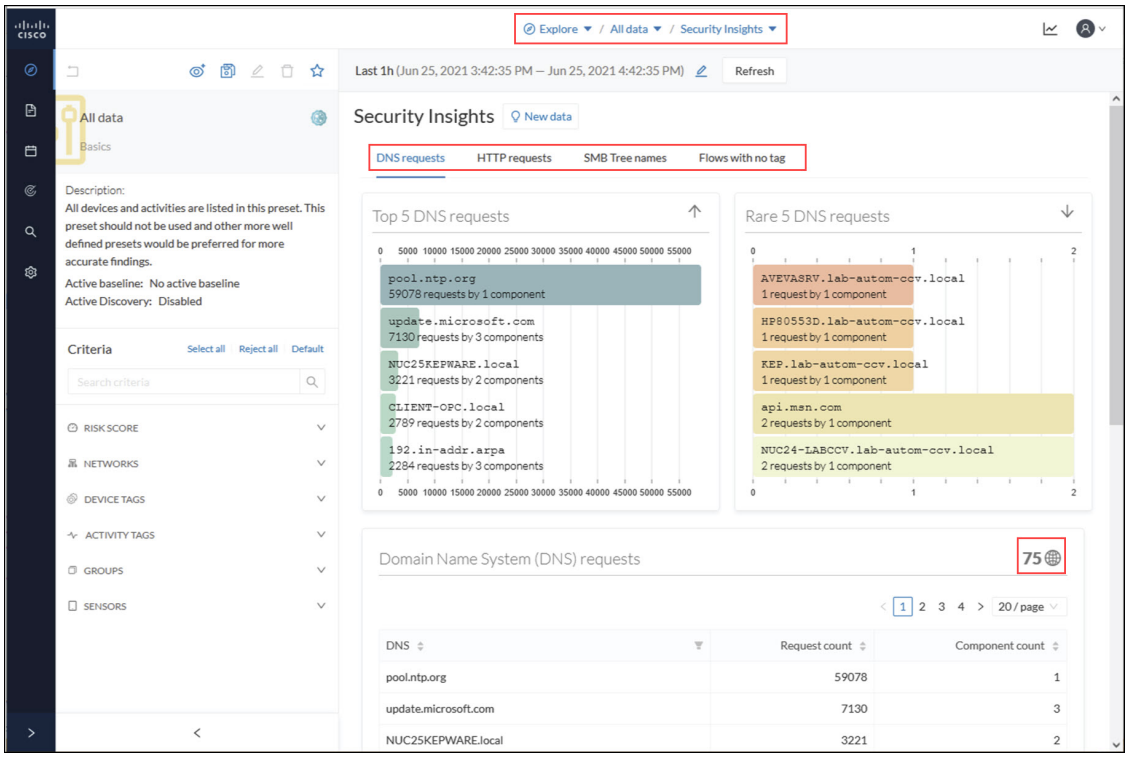
You can **Export to CSV** using the corresponding button on top of the vulnerability list. A report will be generated for the time period defined.



Security Insights

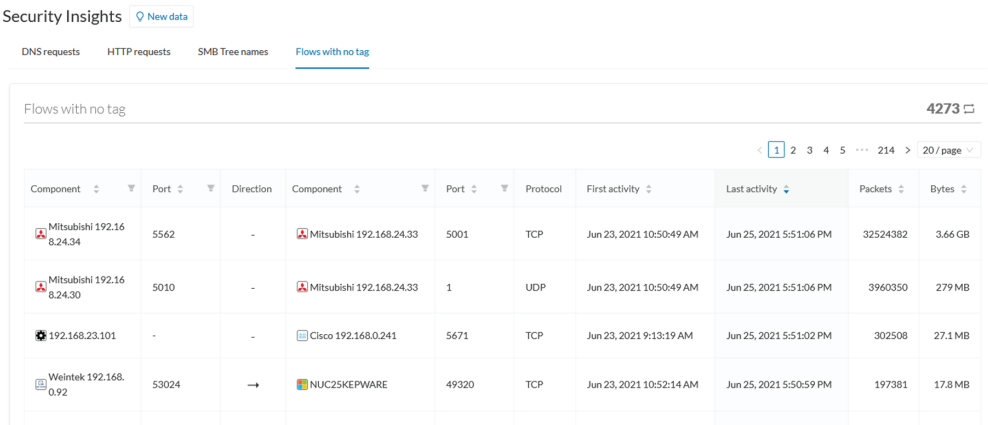
To access **Security Insights**, click **Explore > All data > Dashboard > Security Insights**. **Security Insights** provides statistics for **DNS requests, HTTP requests, SMB Tree names** and **Flows with no tag**.





Each tab shows the top (most frequent), rarest requests, and lists all the requests. In the bottom panel, you can change the number of requests that show per page. You can see how many pages and the current page displaying. The total appears in the top right (75 in this example).

Flows with no tag



This information shows a list of all traffic that Cisco Cyber Vision was not able to analyze. There are various reasons for this, such as the protocol is not supported yet.

Next steps:

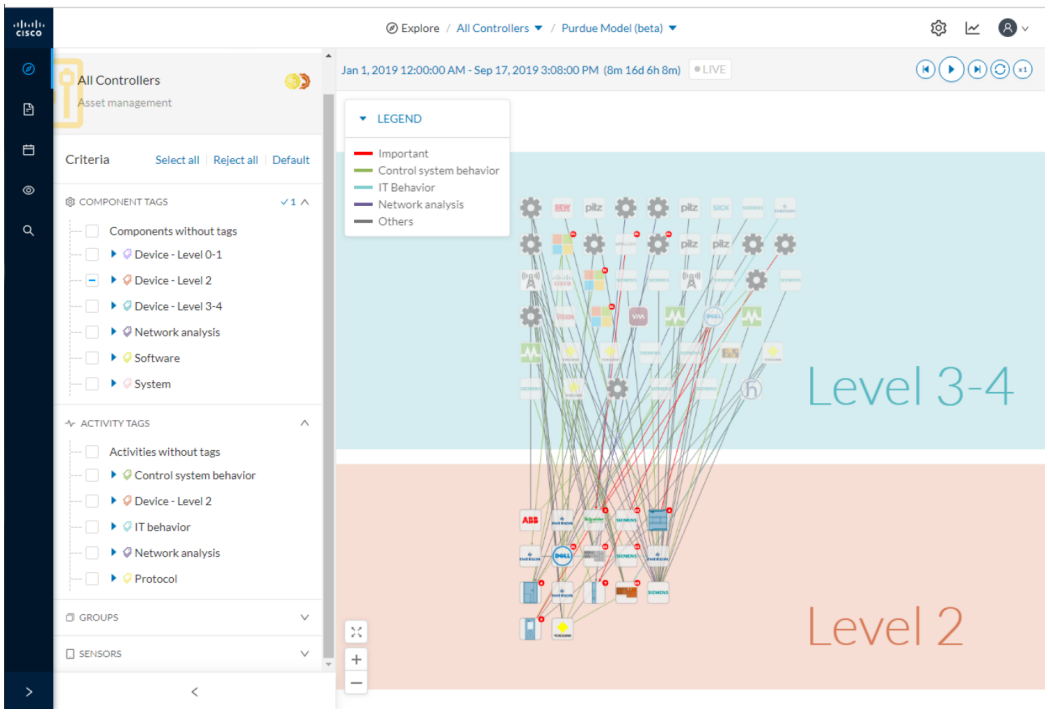
1. Make sure the content is supposed to be on the network.
2. Troubleshoot why it cannot be inspected.

3. Check flows with higher number of packets.

Purdue Model

This map displays the assets of a preset according to the Purdue Model architecture. Components are distributed among the layers by considering their tags. The **Purdue Model** view doesn't undergo any aggregation and is self-organizing. To access **Purdue Model**, click **Explore > All data > Dashboard > Purdue Model**.

Assets of the preset All Controllers distributed among the layers of the Purdue model

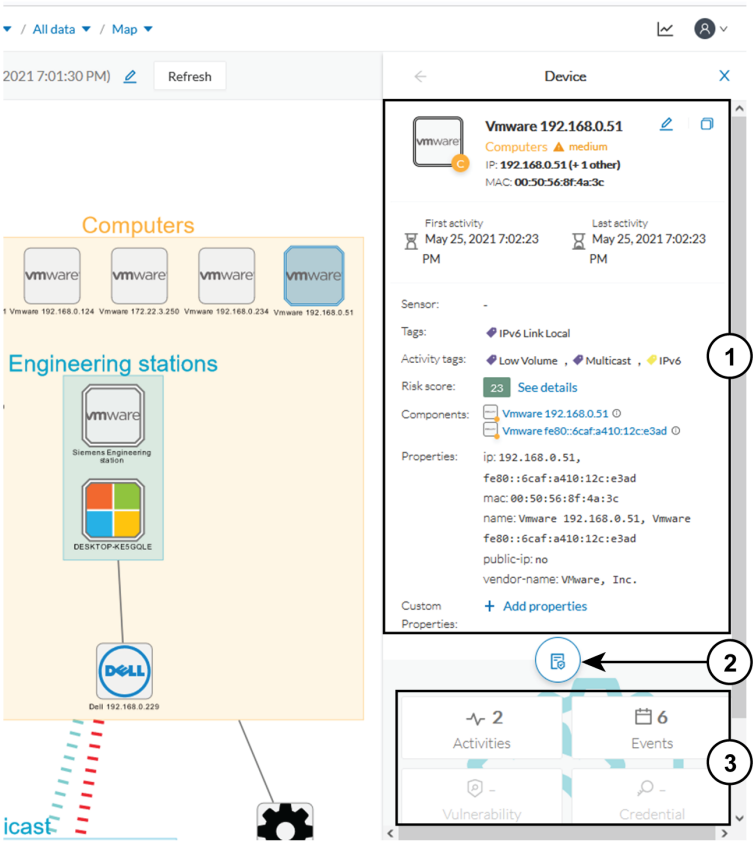


Components are distributed according to the following different layers of the Purdue model:

- Level 0-1: Process and basic control (IO Modules).
- Level 2: Area supervisory control (PLCs, SCADA stations).
- Level 3-4: Manufacturing zone and DMZ (all others).

Detail panel

A Detail panel is a condensed view about a device, a component, a group of components or an activity's information without changing the background device list or a map. To access a detail panel, click a device, a component or an activity on the map or a list.



The detail panel differs depending on the type of element you select. The upper portion **(1)** gives you general information about the element. If you select a device or a component, you can edit its name an add/remove it to/from a group.

The lower part contains a round button **(2)** which opens the element's Technical sheets with all relevant information (available for devices, components and activities).

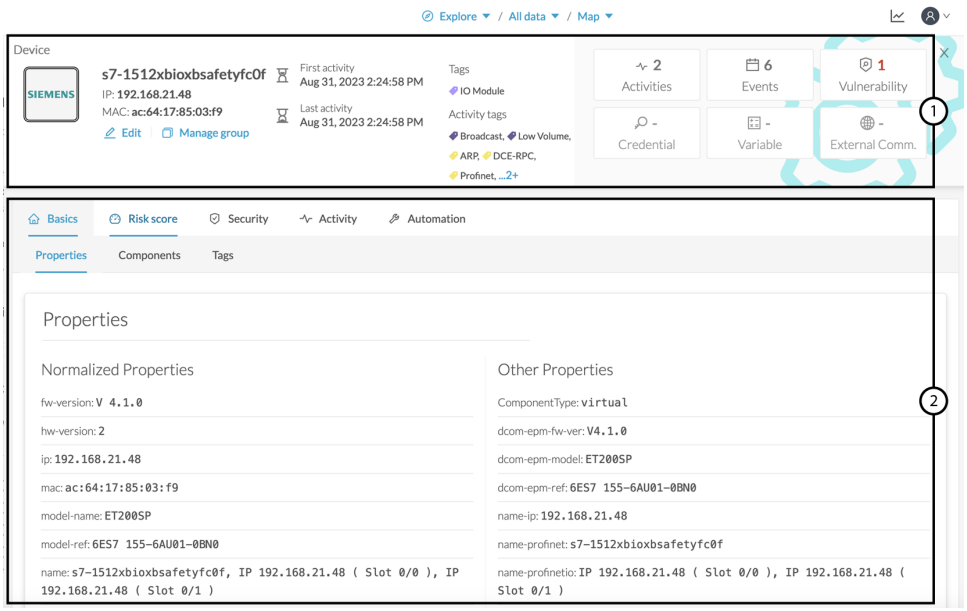
The rectangular buttons below **(3)** redirect to the corresponding information inside the technical sheet.

Technical sheets

A technical sheet is an interactive and complete view of all information related to a device, a component, an activity or a flow. The views differ depending on the type of element selected.

To access the **technical sheet** of a device, component or an activity's Detail panel, click **Explore > All data > Dashboard > Map**. Click the element about which you want more details. The Details panel appears. Click the **Technical sheet** icon.

A technical sheet of a device



The top box of the technical sheet **(1)** recaps the information found in the **Detail** panel. The rectangular buttons on the right redirect to the corresponding information inside the technical sheet. In a device or a component's technical sheet, you can also edit the element's name, add/remove it to/from a group, and add custom properties.

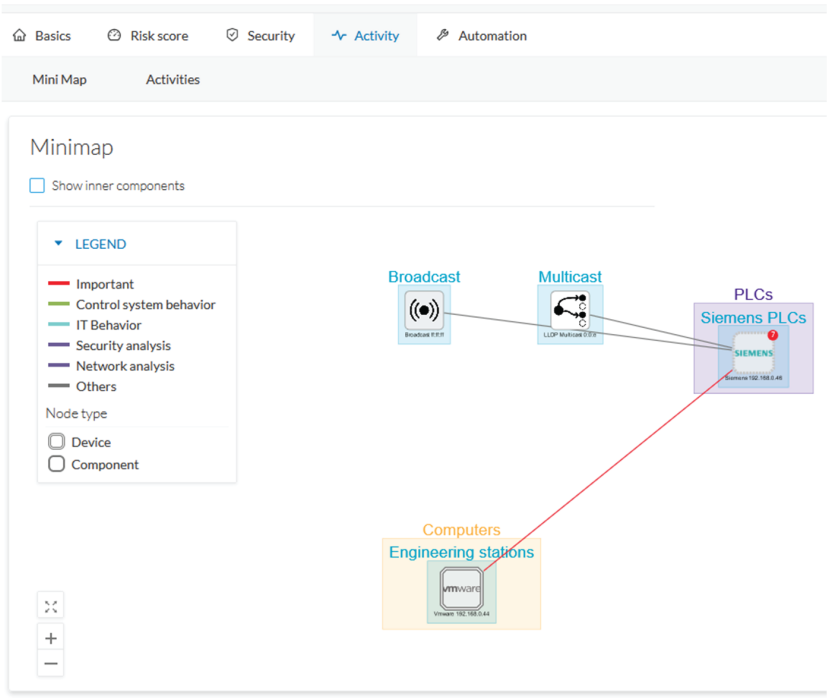
The middle portion **(2)** contains many tabs, depending on the selected element. In the above example, A **Device** detail contains the following tabs:

- **Basics** shows an element's properties and tags that are categorized with their definition. The components of the device also appear, if applicable.
- **Risk score** shows an overview and a more detailed and focused views.
- **Security** shows a component's vulnerabilities and credentials.
- **Activity** shows an activity's flows and contains a Mini map, a view that is restricted to a device or a component and its activities. If applicable, a list of external communications with related information appears under the corresponding tab.
- **Automation** contains variable accesses.

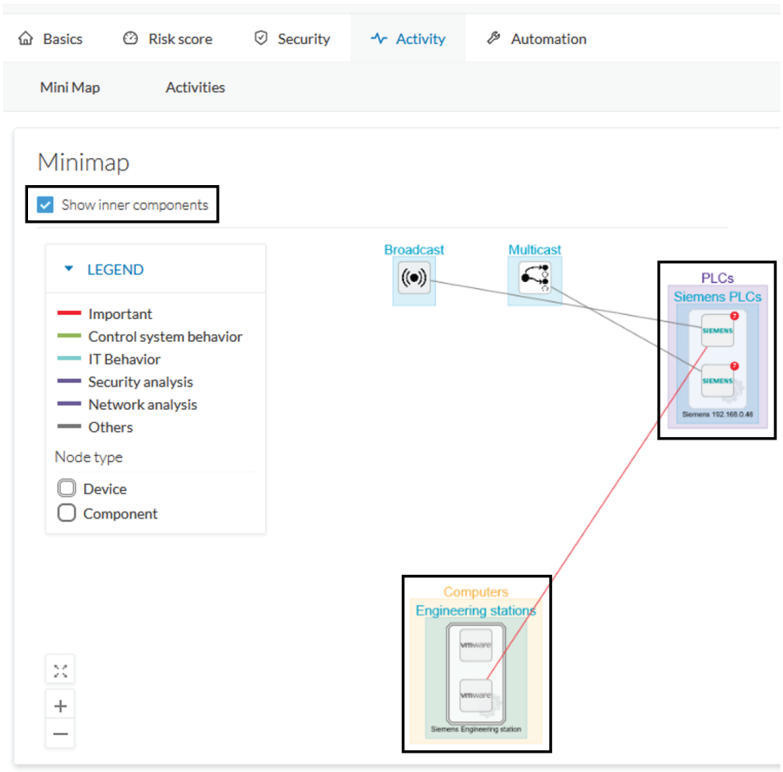
- More information about properties.
- More information about tags.
- More information about the risk score.
- More information about vulnerabilities.
- More information about credentials.
- More information about flows.
- More information about the Mini map.
- More information about external communications.
- More information about variables accesses.

Mini map

The **Mini Map** is a visual representation restricted to a specific device or component and its activities. To access **Mini Map**: click **Explore > All data > Dashboard > Map >** select a device from the map > click **Technical sheet** from the **Details** panel. Click the **Activity** tab.



Click **Show inner components** for an exploded view of the devices.



Click any element in the Mini Map to open its Detail panel for access to more information.