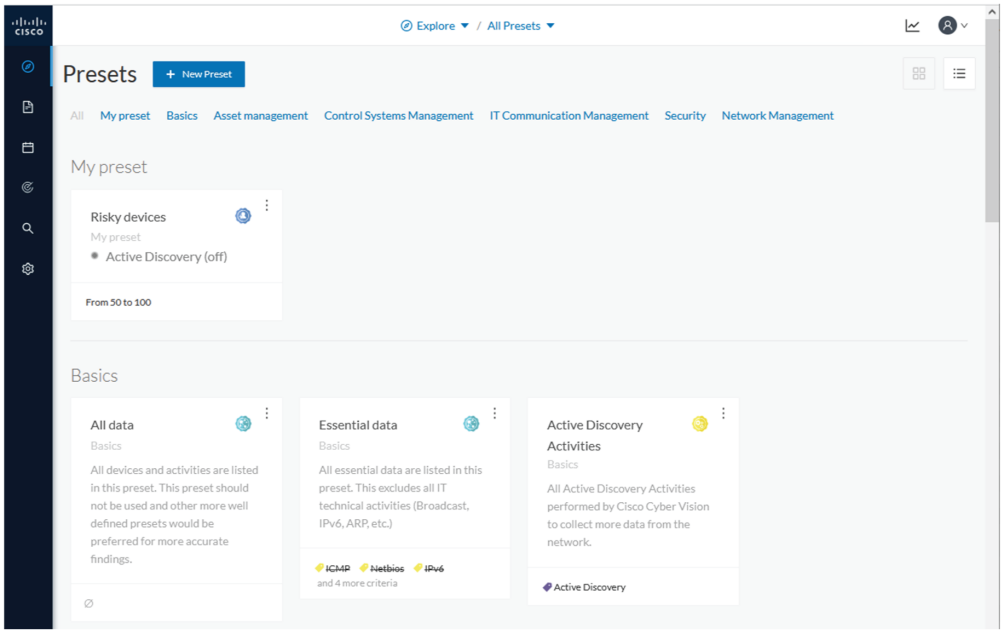
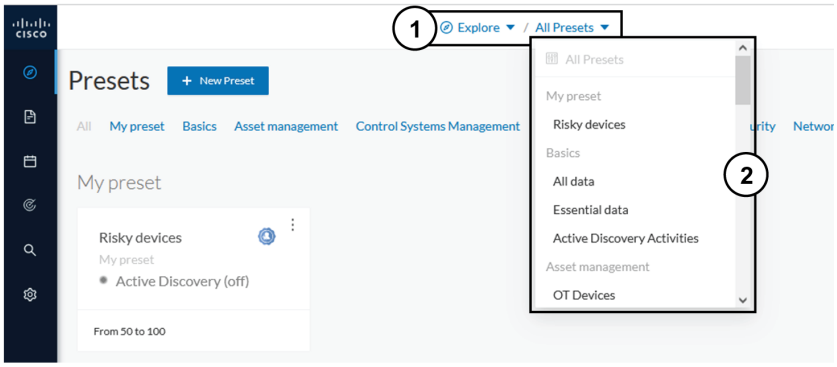
Explore

Presets is a page containing an overview of all presets existing in Cisco Cyber Vision whether they are present by default or part of users' customizations. You can access this page by clicking the Explore button on the left navigation bar.



The top navigation bar **(1)** allows you to access the different presets **(2)** and then reach their different Preset views.



- Preset views, on page 2
- Right side panel, on page 12

Preset views

There are several types of views which relate to different perspectives:

- The dashboard:

  The Dashboard is a unique view which is displayed by default when accessing a preset. It offers an overview of data found by the preset. The fact that it's a tag-oriented view allows you to have a general insight of the network without going into deep and technical details.

- The map:

  The Map is a visual data view of the industrial network that gives you a broad insight of how components are connected to each others.

- Lists:

  Lists are views specialized whether on devices or activities. These views provide classic but powerful data filtering to match what you are looking for. For more information, refer to the Device and activity lists.

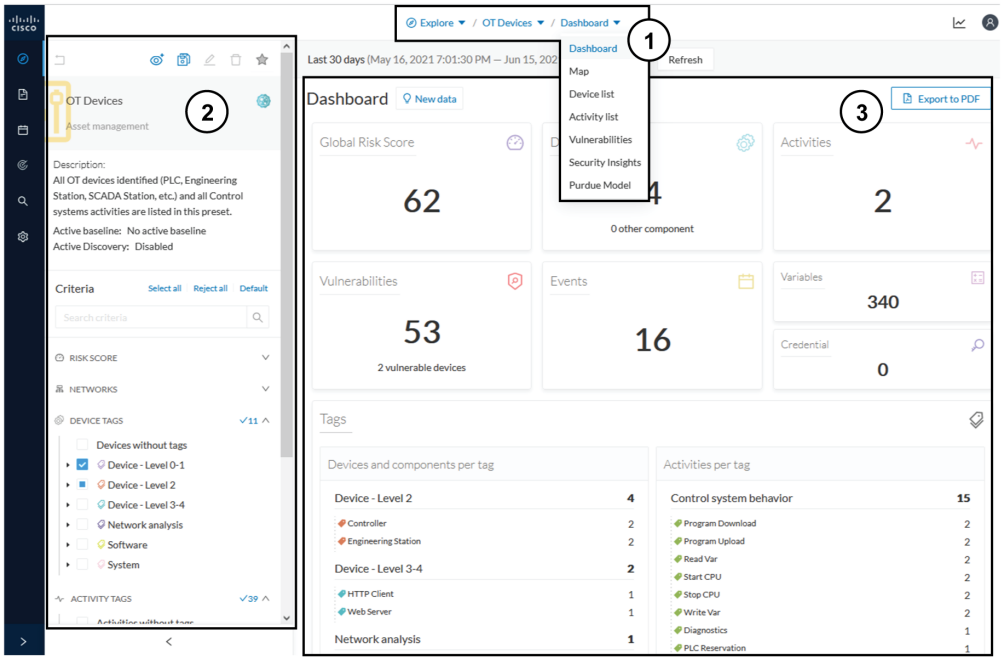
- The Purdue Model:

  In this map, the components of a preset are distributed among the layers of the Purdue Model architecture.

Views are always structured as shown below:

- The top navigation bar **(1)**, which allows you to easily switch between the different views thanks to its menu.
- The filtering area on the left **(2)**, which allows you to modify and manage the preset by adapting criteria and registering changes.
- The view you're on **(3)**, which dynamically evolves as you change and save criteria.

Example of the OT Devices preset on the dashboard view:



Display of preset views has been optimized to avoid lags, solve performance issues and prevent the application from crashing, especially in case of large data flow.

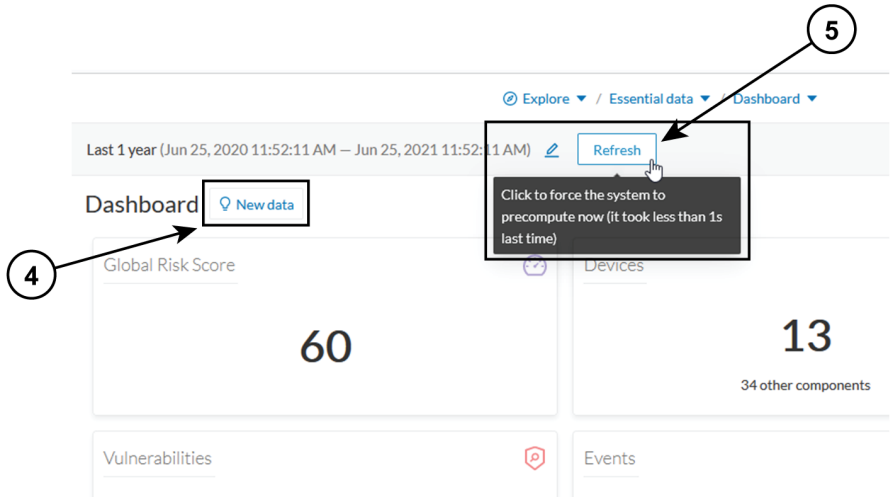
The entire database used to be checked over and over. Elements such as components, tags and activities were counted repeatedly and displayed simultaneously in the preset views, which were continuously refreshed.

As of Cisco Cyber Vision version 4.0.0, data found is stored instead of being directly displayed in the preset views. Preset views refresh occurs only when necessary or requested to not overload the application display. The elements visible in the preset views are actually data from the previous computation, which means that data displayed in the GUI and the data stored in the database, are asynchronous. This actually lighten data load on preset views.

In addition, computation adapts to the preset consultation frequency. That is, a preset often viewed by users will be computed accordingly. Instead, the system will not compute presets that are never used.

When on a preset, data are regularly computed thanks to an automatized data computation running in the background. However, this will 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 and refresh the view as you click on it. The view will be updated to the last computation done in the system, which means that using this button won't necessarily show new data.
- The Refresh button **(5)** forces data computation and refresh the preset view. This task requires more resources and should be used in the following cases:
  - If you expect that new data has been found during the most recent computation (e.g. a new device plugged into the network).
  - If custom data such as groups or names have been changed (e.g. if adding a device into a group).



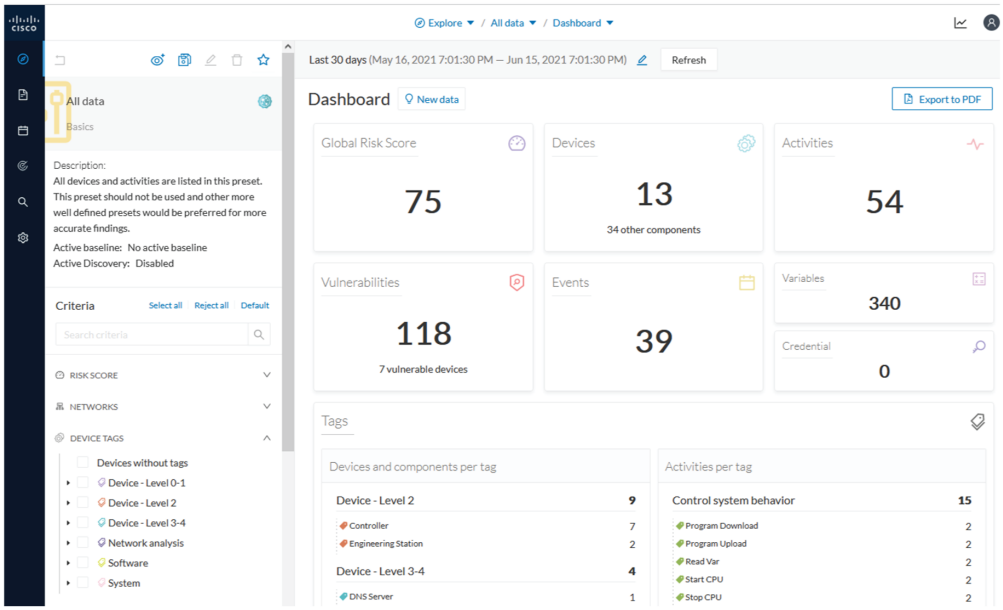
In any cases, the computation is forced and the view is refreshed as you navigate in the application. For example, when accessing another preset or when moving from one view to another.

Note New preset view optimization has also an impact on how criteria are handled in preset views. To be taken into account and thus for the computation to be forced, criteria must be saved as a new preset if acting from a default preset, or saved if in a custom preset.

Dashboard

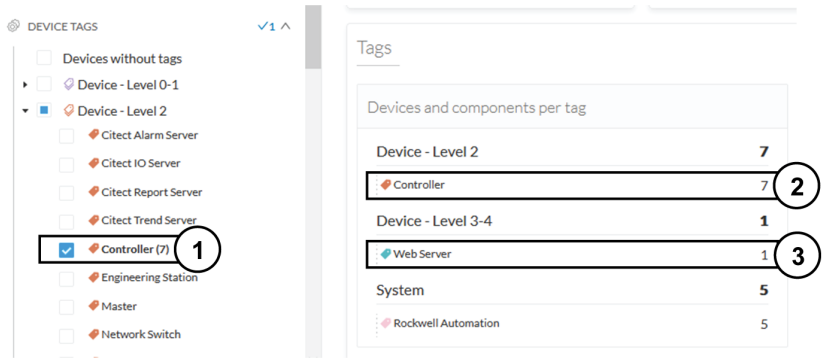
The dashboard is the view by default when opening a preset. It gives you an overview of the preset's global risk score, number of devices, activities, vulnerabilities, events, variables and credentials.

The dashboard is also a tag-oriented view. It's an overview of all tags found -independently of the ones set as criteria- with the number of devices and activities found per tag.



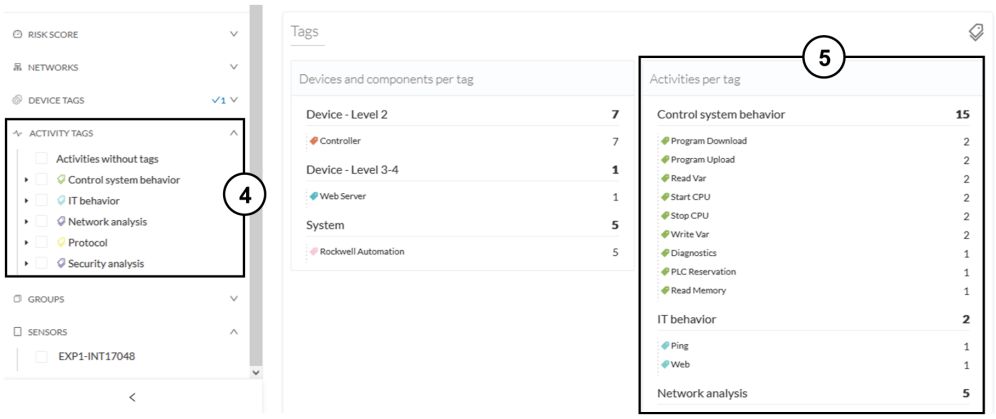
Example: For the purpose of the whole example given below, we access the All data preset, select the Controller tag as criteria (under Device - Level 2), and save the selection as "Example: Controller tag".

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



If you want to know more about one of these devices, switch to the Device and activity lists and reach 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.



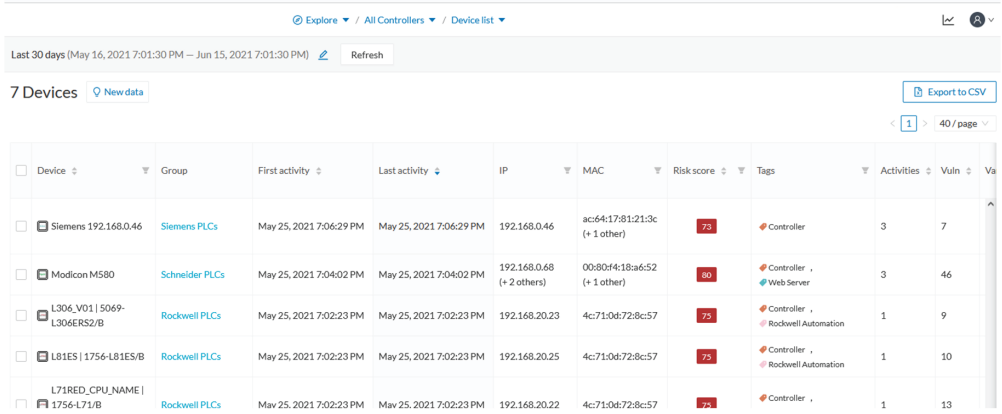
If you want to know more about one of these activities, switch to the Device and activity lists and reach them using the filter available in the tags column.

Device and activity lists

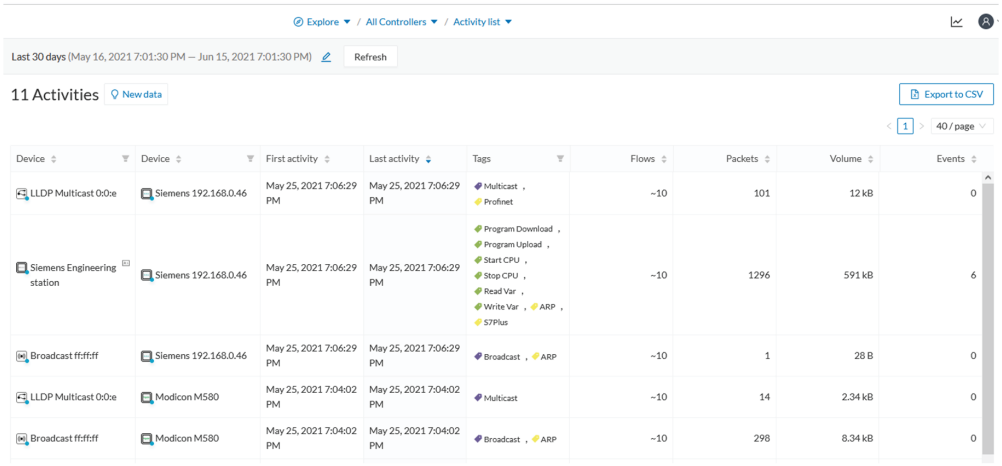
The device and activity lists are two specialized and oriented views. Even though they are legated and share a large number of data, devices and activities are split in two different views to facilitate comprehension and visualization of data.

These views provide general information and advanced technical data about each element found in the preset. Check at the differences between the device and activity views.

The All Controllers preset in the device list view:

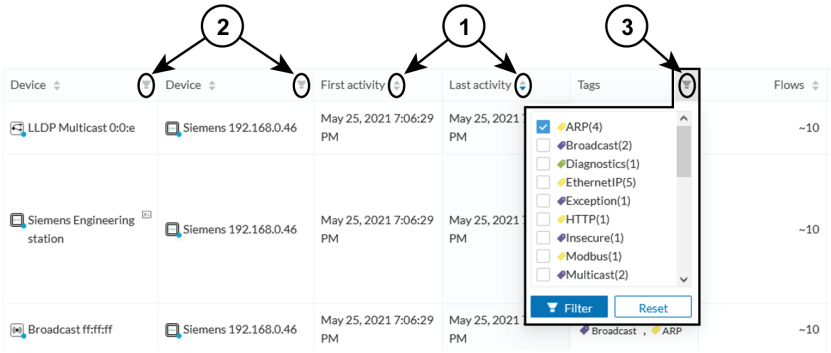


The All Controllers preset in the activity list view:



Lists are meant to perform an in-depth exploration of the network. Using this type of view is especially convenient when searching for a very specific data. To do so, different filters are available inside the lists to sort data:

- The sort icon **(1)** is to sort data by alphabetical order or by ascending/descending order.
- The filter icon **(2)** opens a field to type a specific data in, or a multiple choice menu **(3)** to filter tags.

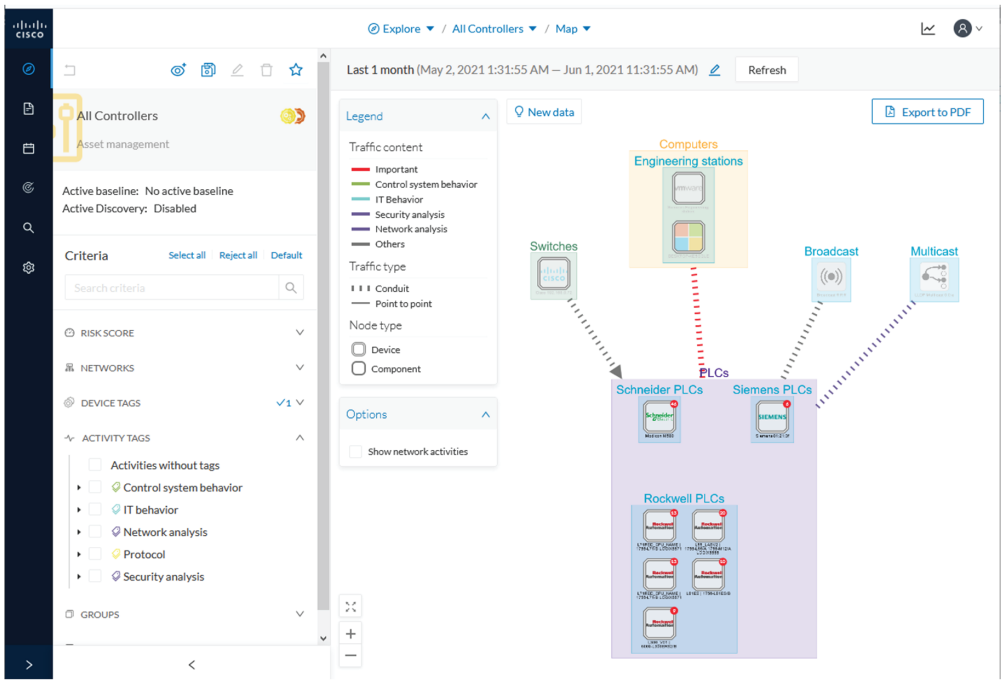


Clicking an element in the lists opens its Right side panel which leads to more advanced data.

Map

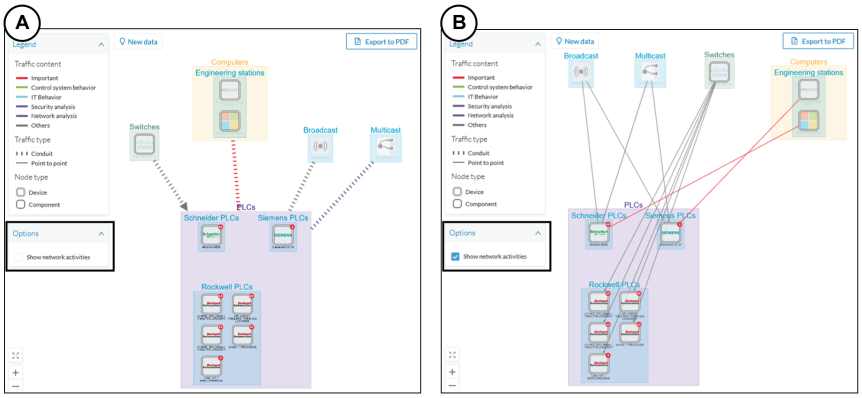
The Map is a visual representation of data of the industrial network that gives you a broad insight on how devices and components are interconnected. It's a good input to get to know how the network is structured. You can start organizing components in a way that makes sense to you by creating groups.

Maps display 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 is **self-organizing**, that is, elements are redistributed as devices, components, conduits and activities appear or disappear, and as groups are created or deleted. Moreover, the map automatically adapts over time and when changing preset. This way, it is guaranteed that the map is always well organized and components never overlap.

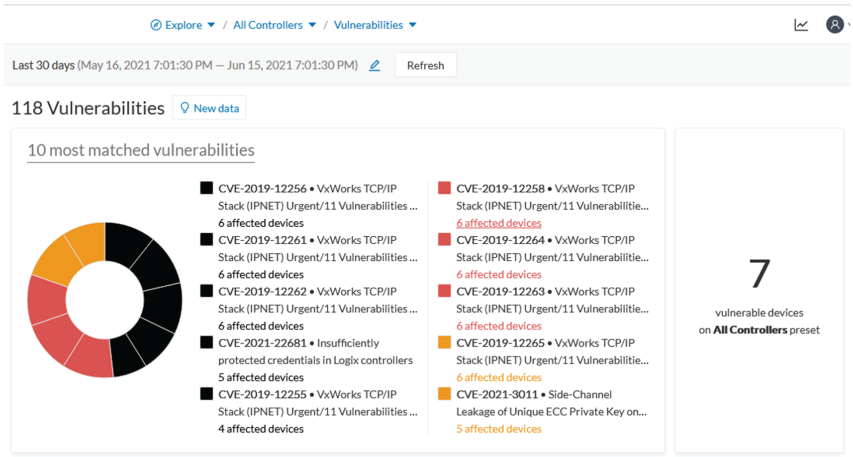
By default, activities between groups are merged and displayed as conduits **(A)**. You can tick the option "Show network activities" to see activities, which gives a more detailed view **(B)**. Elements are here also automatically reorganized in the map to enhance visibility.



Vulnerabilities

The vulnerability dashboard gives you a visual representation and a list of the vulnerabilities detected within a preset.

Important It is important to update the Knowledge DB in Cisco Cyber Vision as soon as possible after notification of a new version to be protected against vulnerabilities. To do so, refer to the corresponding documentation.



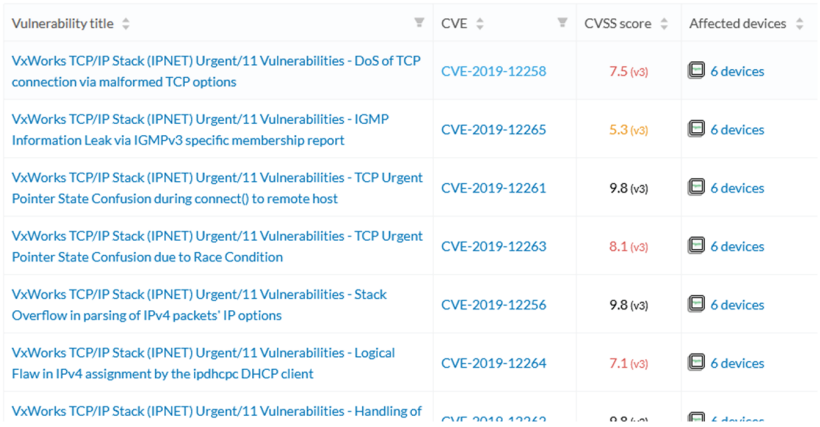
The pie chart presents the 10 most matched vulnerabilities within the preset, that is, the vulnerabilities that have affected more devices. You can click the number of devices detected to see the devices affected.

On the right, you'll see a summary of the total number of devices that are vulnerable in the preset selected.

Below, you have a list of all the vulnerabilities found in the preset with sort icons to sort data by alphabetical order or by ascending/descending order, and filter icons which opens a field to type a specific data.

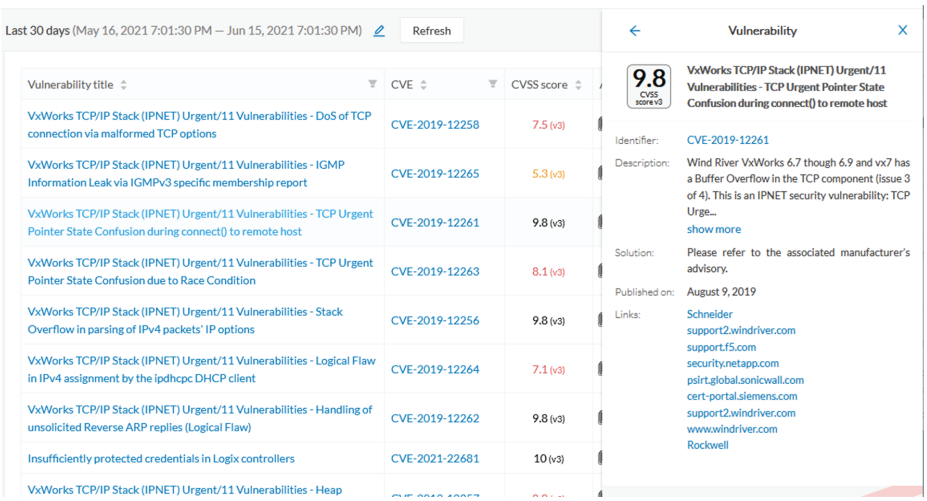
For each vulnerability, the following data are displayed in columns:

- The vulnerability name
- Its CVE ID (world unique identifier for a Common Vulnerability Exposure)
- Its CVSS score (Common Vulnerability Scoring System)
- The devices affected by the vulnerability



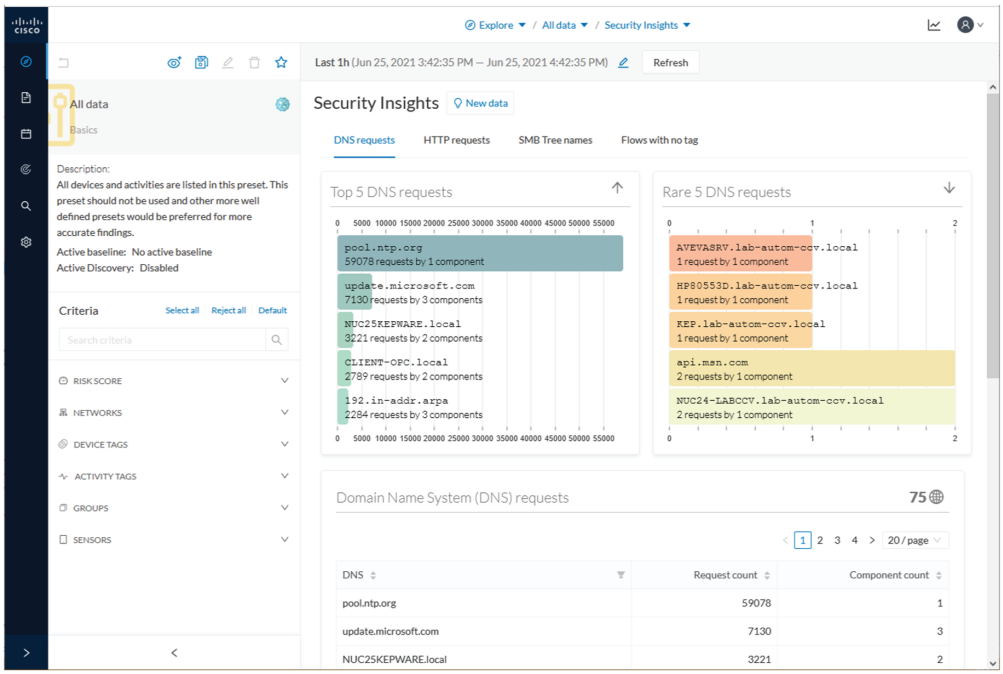
Vulnerability title	CVE	CVSS score	Affected devices
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - DoS of TCP connection via malformed TCP options	CVE-2019-12258	7.5 (v3)	6 devices
VxWorks TCP/IP Stack (IPNET) Urgent/11 Vulnerabilities - IGMP Information Leak via IGMPv3 specific membership 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			

Clicking an element in the lists opens its Right side panel which leads to more details about the vulnerability, including its link to the National Vulnerability Database.



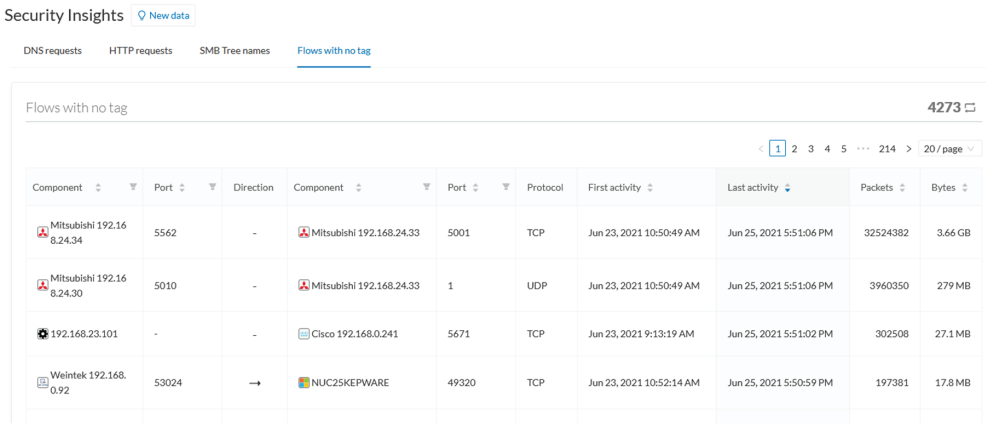
Security Insights

Security Insights is a view that provides statistics for DNS requests, HTTP requests, SMB Tree names and flows with no tag.



For each category, you will find the most frequent and rarest requests, and the list of all these requests.

Flows with no tag:

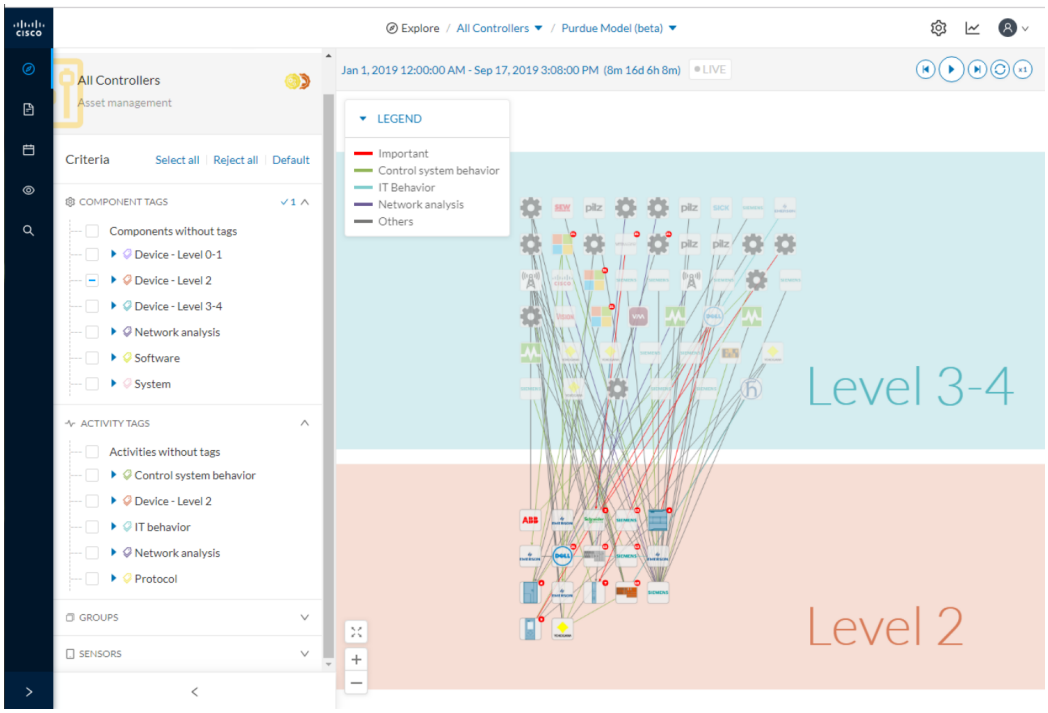


In this category, you will find a list of all flows with no tags, that is, traffic that Cisco Cyber Vision wasn't able to analyze. The reason can be that the protocol is not supported by Cisco Cyber Vision yet. However, this list is interesting from a security standpoint to make sure if such content is really supposed to be on the network and search why it cannot be inspected. A good starting point is to 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.

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

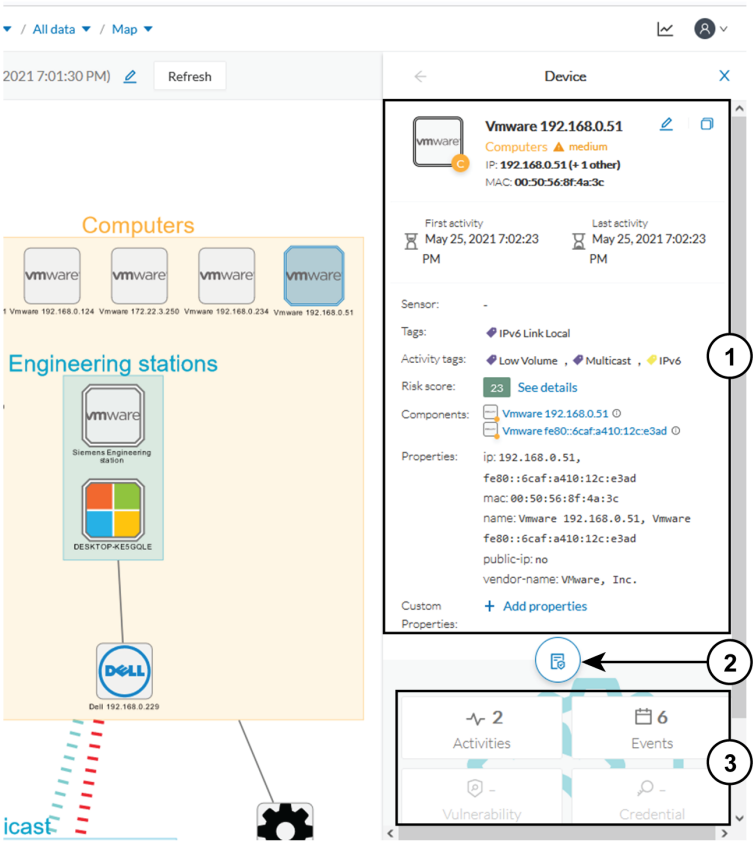


Components are distributed according to the different layers of the Purdue model:

- 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).

Right side panel

A right side panel is a condensed view about a device, a component, a group of components or an activity's information. This view allows you to quickly scan general information about an element meanwhile you're keeping an eye on a broader view such as a device list or a map.



Right side panels differ depending on the type of element consulted. The higher part **(1)** of the right side panel gives you general information about the element. If consulting 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).

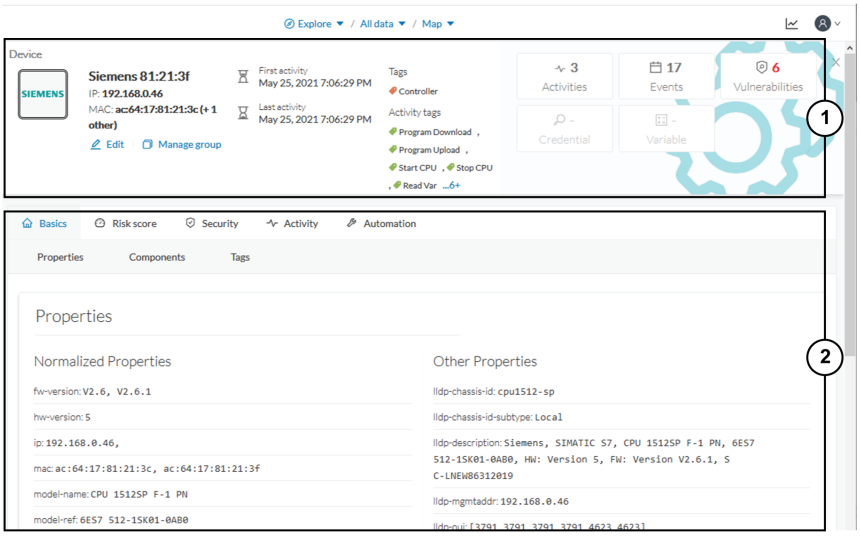
The rectangular buttons below **(3)** redirect to the corresponding information inside the technical sheet.

To access a right side panel you just need to click a device, a component or an activity on the map or a list.

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 consulted.

A device's technical sheet:



A technical sheet is composed of a top bar and of a list of tabs. The higher part **(1)** recaps the information found in the right side 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 lower part **(2)** contains detailed information classified under tabs, displaying or not according to the element you're on:

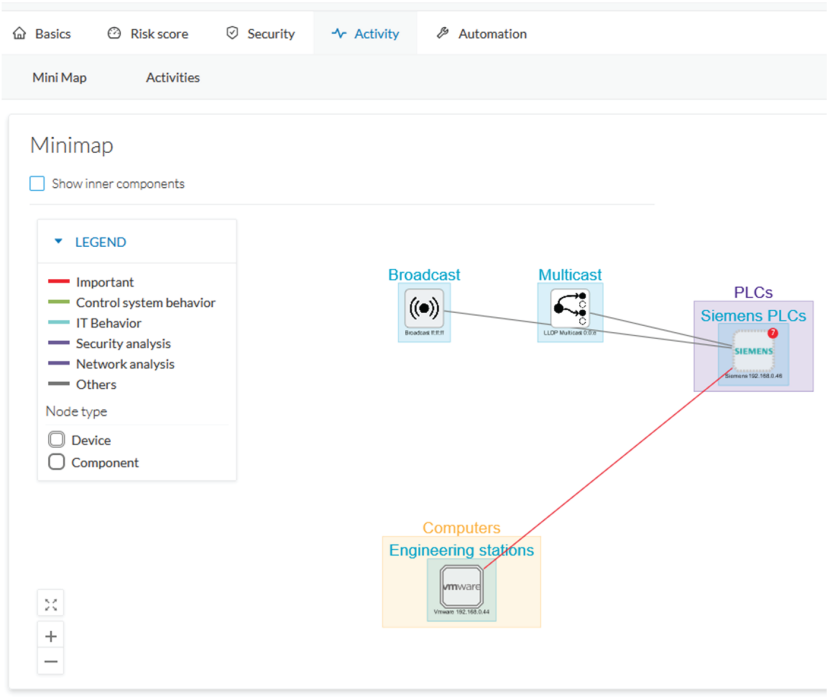
- Basics contains an element's properties and tags that are categorized with their definition. Device's components also appear if applicable.
- Risk score with an overview and a more detailed and focused views.
- Security contains a component's vulnerabilities you can acknowledge and credentials.
- Activity is about an activity's flows and contains a Mini map which is a view that is restricted to a device or a component and its activities.
- Automation contains variable accesses.

You can access technical sheets through a device, component or an activity's Right side panel, clicking the technical sheet button. A flow's technical sheet is visible when clicking on a particular flow.

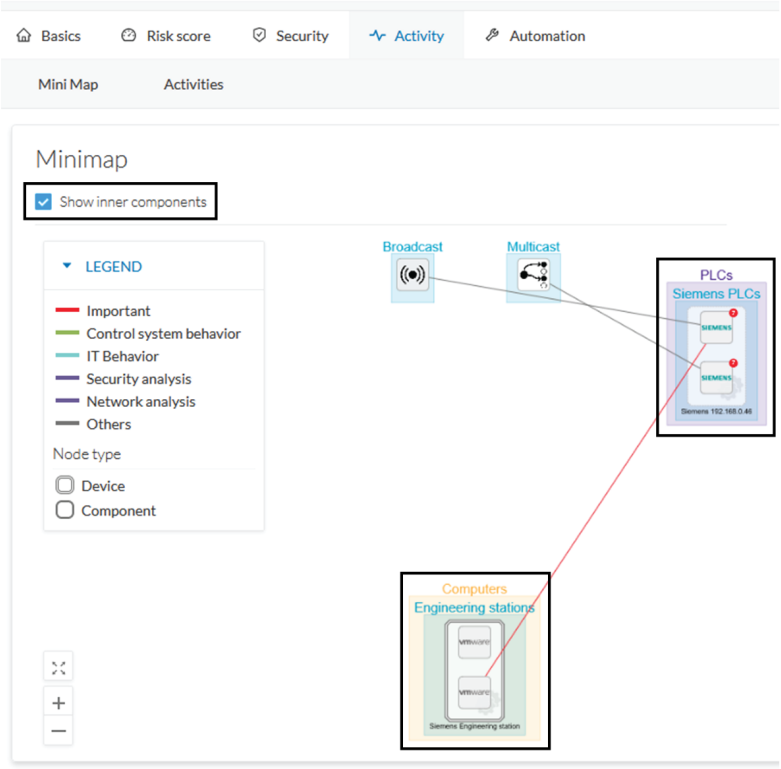
- More information about properties.
- More information about tags.
- More information about the risk score.
- More information about vulnerabilities.
- More information about credentials.
- More information about flows.
- More information about the Mini map.
- More information about variables accesses.

Mini map

The Mini Map is a visual representation restricted to a specific device or component and its activities. This view is accessible through the Activity tab of a Component's Technical sheets.



The option "Show inner components" enables an exploded view of the devices.



Clicking any element in the Mini Map will open its Right side panel so you can have access to further information.