Risk score

Risk score

What is a risk score?

A risk score is an indicator of the good health and criticality level of a device, on a scale from 0 to 100. It has a color code associated to the level of risk:

Score	Color	Risk level
From 0 to 39	Green	Low
From 40 to 69	Orange	Medium
From 70 to 100	Red	High

The notion of risk scores appears in several parts of Cisco Cyber Vision. For example, you will find them in:

- The filter criteria.
- The device list.
- The device technical sheet.
- The device risk score widget (Home page).
- The preset highlight widget (Home page).

What is a risk score used for?

The risk score is meant to help the user easily identifying which devices are the most critical within the overall network. It provides limited and simple information on the cybersecurity of the monitored system. It is intended as a first step in security management to take actions by showing the causes of high scores and providing solutions to reduce them. The goal is to minimize and keep risk scores as low as possible.

The solutions proposed can be:

- to patch a device to reduce the surface of attack,

- to remove vulnerabilities,
- to update firmware,
- to remove unsafe protocols whenever possible (e.g. FTP, TFTP, Telnet),
- to install a firewall,
- to limit communications with the outside, by removing external IPs.

In addition, it is necessary to define the importance of the devices in your system by grouping devices and setting an industrial impact. Thereby, increasing or decreasing the risk score, which will allow you to focus on most critical devices.

All these actions will reduce the risk score which affect its variables, i.e. the impact and the likelihood.

For example, removing unsafe protocols will affect the likelihood of the risk, but patching a device will act on the impact of the risk.

Risk score represents an opportunity to update usage and maintenance habits. However, it is NOT intended to replace a security audit.

In addition, risk scores are used in Cisco Cyber Vision to sort out information by ordering and filtering criteria in lists and to create presets.

How is the risk score computed?

The risk score is computed as follows:

Risk = Impact x Likelihood

Impact:

The impact answers the question: What is the device “criticality”, that is, what is its impact on the network? Does it control a small, non-significant part of the network, or does it control a large critical part of the network? To do so, the impact depends on:

- The device tags, because some device types are more critical. Each device type (or device tag) or device tag category has been assigned an industrial impact score by Cisco Cyber Vision. For example, is the device a simple IO device that controls a limited portion of the system, or is it a Scada that controls the entire factory? These will obviously not have the same impact if they are compromised.
- The user has the possibility to act on the device impact by moving it into a group and setting the group's industrial impact (from very low to very high).

Likelihood:

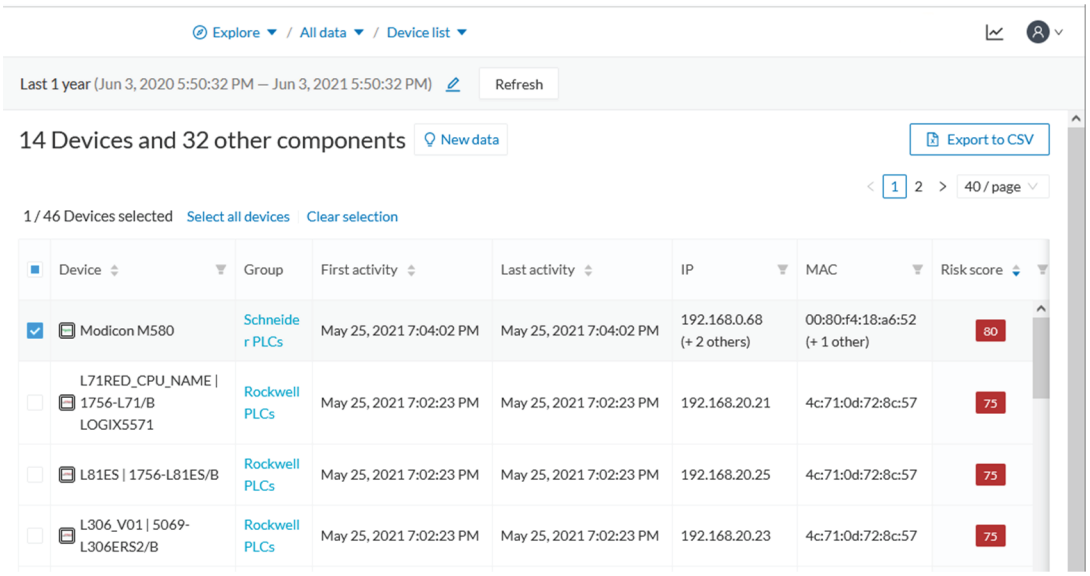
The likelihood answers the question: What is the likelihood of this device being compromised? It depends on:

- Device activies, more precisely on the activity tags. Because some protocols are less secure than others. For example, Telnet is less secure than ssh.
- The exposure of the device communicating with an external subnet.
- Device vulnerabilities, taking into account their CVSS scoring.

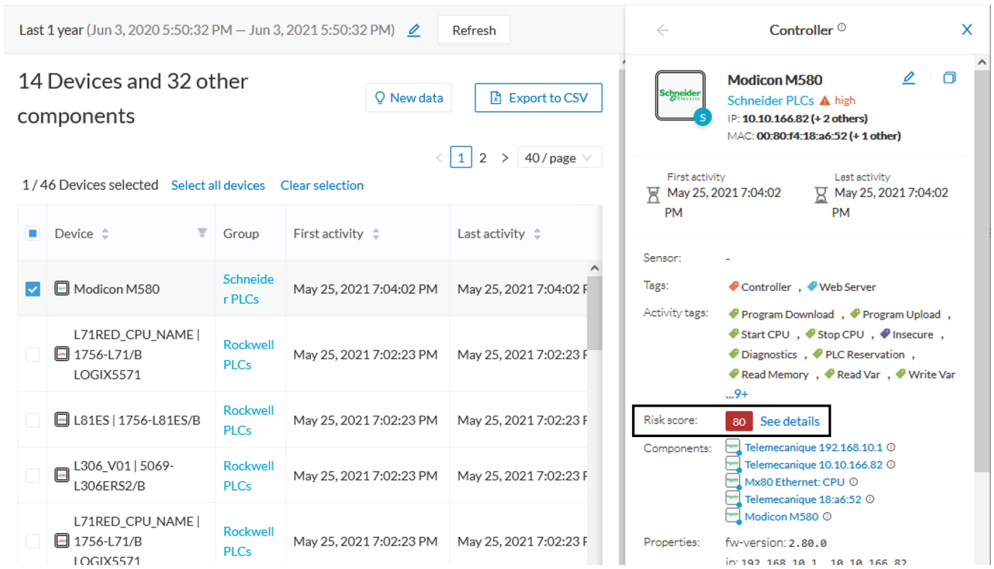
These criteria are visible under Details in the device's technical sheet.

How to take action:

1. In the device list, in the risk score column, click the sort icon to get the highest risk scores.



2. Click a device in the list. Its right side panel opens.
3. Click the risk score's "see details" button.

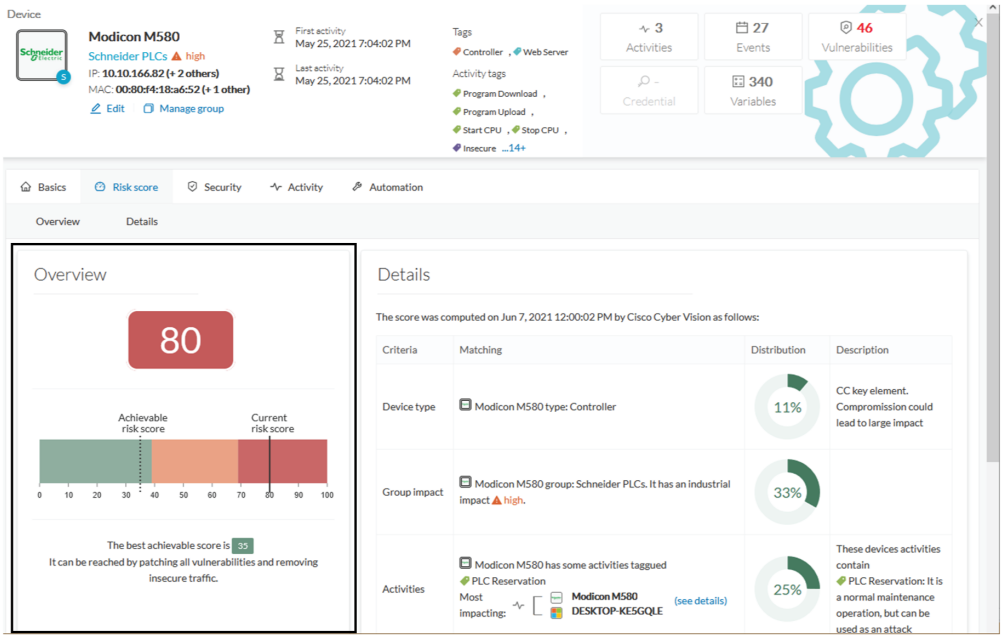


The device's technical sheet opens on the risk score's menu.

Under overview, you can see the current risk score and the achievable risk score.

The achievable risk score is the best score you can reach if you patch all vulnerabilities on the device and remove all potential insecure network activities. The score cannot be zero because devices have intrinsic risks coming from their device type and, if applicable, their group industrial impact.

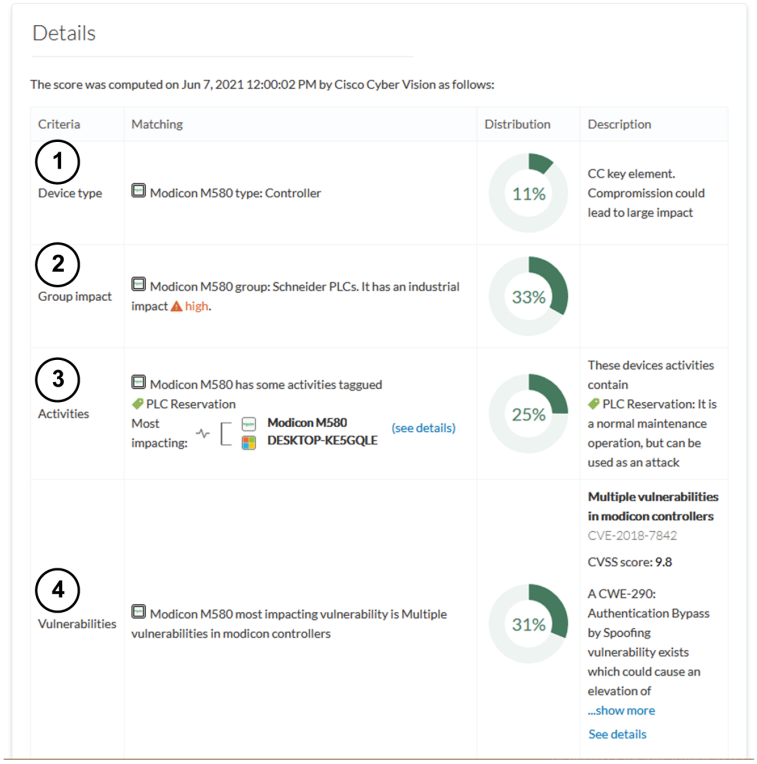
Risk score



Under Details, you have further information about the different risks impacting the device, the percentage of the risk they represent within a total risk score, and the solutions to reduce or even eliminate them.

Device type **(1)** and group impact **(2)** affect the risk impact variable, meanwhile activities **(3)** and vulnerabilities **(4)** affect the risk likelihood.

Risk score



As first information, you have the last time the risk score was computed by Cisco Cyber Vision. Risk score computation occurs once an hour. However, you can force computation by using the following command on the Center shell prompt:

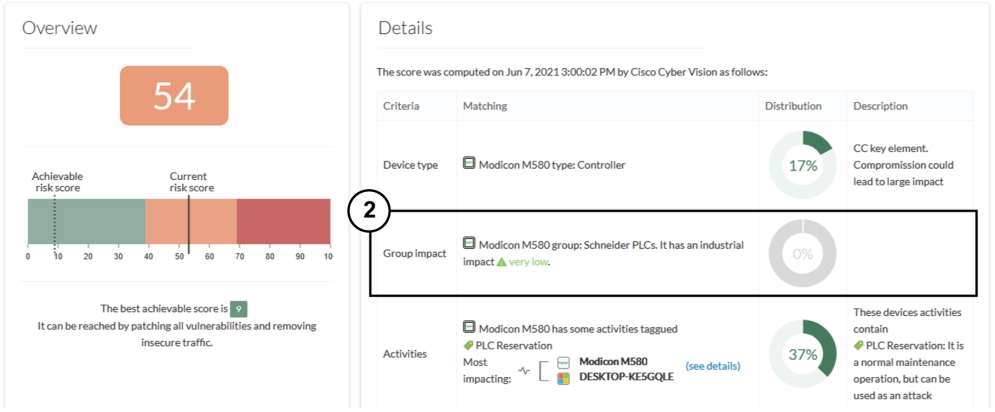
```
sbs-device-engine
```

Below, appears the information retrieved during the last computation.

- Device type **(1)**: Each device type corresponds to a device tag detected by Cisco Cyber Vision. There is no action to be done at the device type level, because each device tag is assigned with a risk score by default in Cisco Cyber Vision.
- The group impact **(2)**: Action is possible if the device belongs to a group. You can decrease the impact by lowering the industrial impact of the group that the device belongs to.

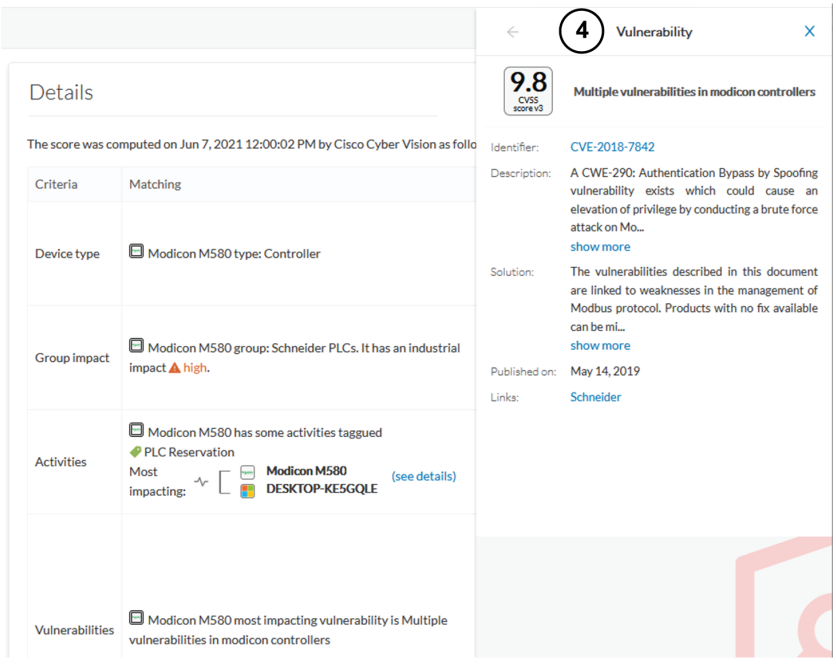
  For example, if I set the group industrial impact to very low (previously high), the overall risk score decreases from 80 to 54:

Risk score



Note The new industrial impact will be taken into account at the next risk score computation (once an hour).

- Activities **(3)**: The most impactful activity tag is displayed. The risk can be lowered if all potential insecure network activities are removed.
- Vulnerabilities **(4)**: Click the "see details" button for more information about how to patch the vulnerabilities and so reduce the device risk score.



By taking these actions, the risk score should decrease considerably.