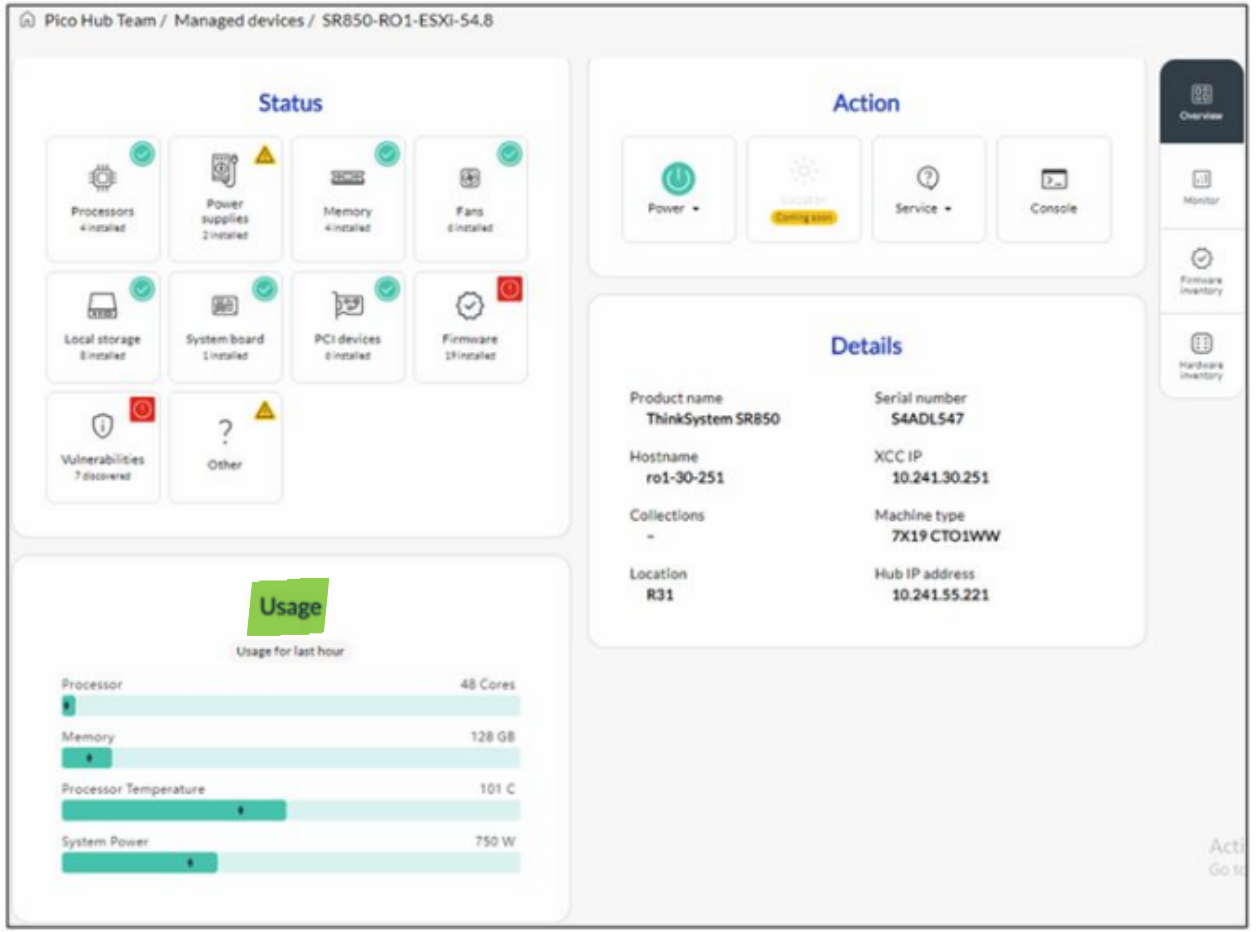
Analytics

Device usage information

Lenovo

Device usage panel

- For the monitoring and analysis of resource usage on a managed system, select a specific device from the **Managed devices** page.
- The **Usage** panel displays a graphical representation of usage data from the past hour and includes information on processor usage, memory usage, CPU temperature, and power utilization by subsystems.
- Hover over any system resource in the usage panel for additional information.
- Usage during the last hour is displayed by default. You can change the time span to show usage during the last 24 hours, 30 days, or 90 days.

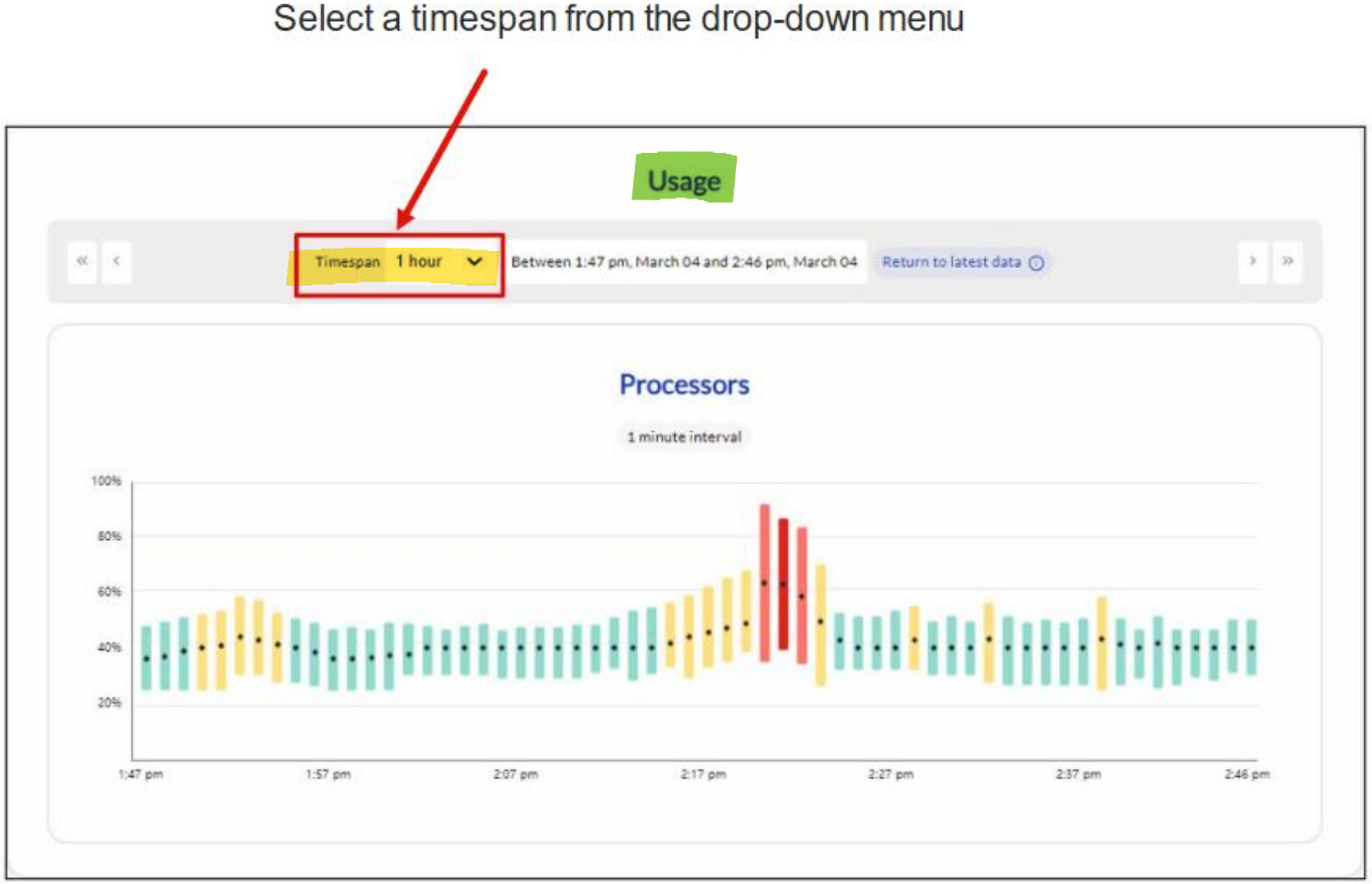


Note: Click the word **Usage** to display a pop-up window that will allow you to manage the information shown in the panel. (Click HERE to see the pop-up window.)

Lenovo

Device usage graph

Click on the usage panel to display graphs showing usage over time. The graphs can be changed by selecting a different timespan from a drop-down menu.



Usage thresholds

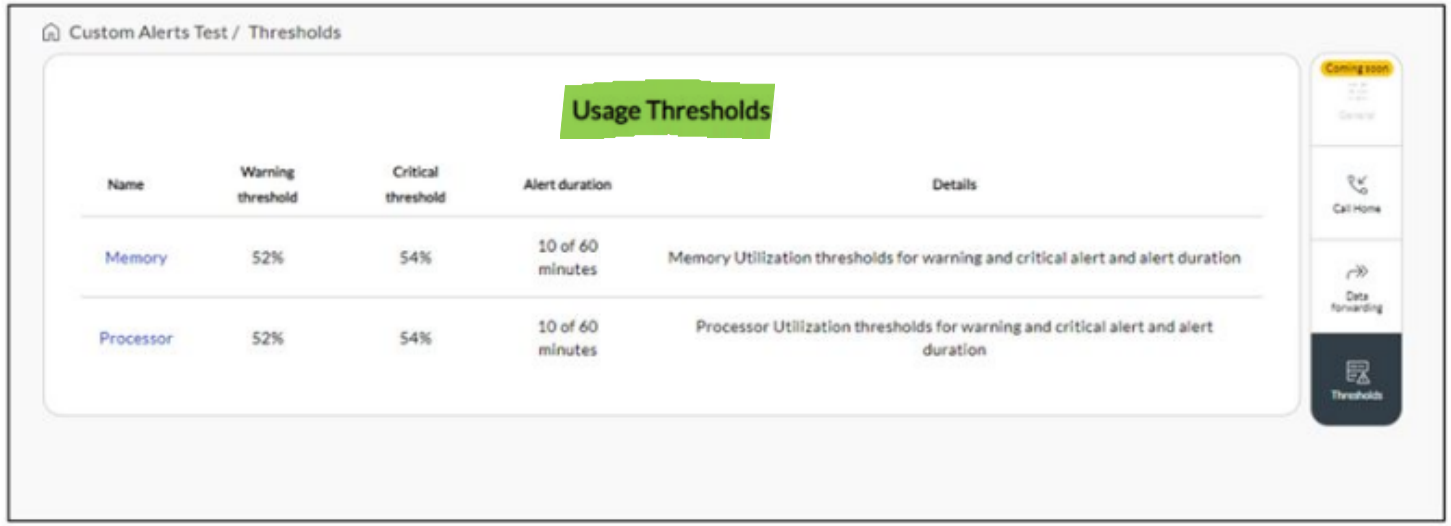
Usage thresholds are enabled by default and have three elements:

- A warning threshold
- A critical threshold
- An alert duration – a specified amount of time within a specified period

An alert will only be raised if the warning or critical threshold is passed and an alert duration is met. For example, if the warning threshold for a processor temperature is 80% and the alert duration is four out of 10 minutes, then an alert will be raised when the processor temperature exceeds 80% for four or more minutes within a 10-minute period.

The minimum alert duration is two minutes in a five-minute period.

Usage thresholds and alert durations can be set for certain components by selecting the **Thresholds** tab from context menu in the **Settings** view and then clicking the row for the component that you want to change.



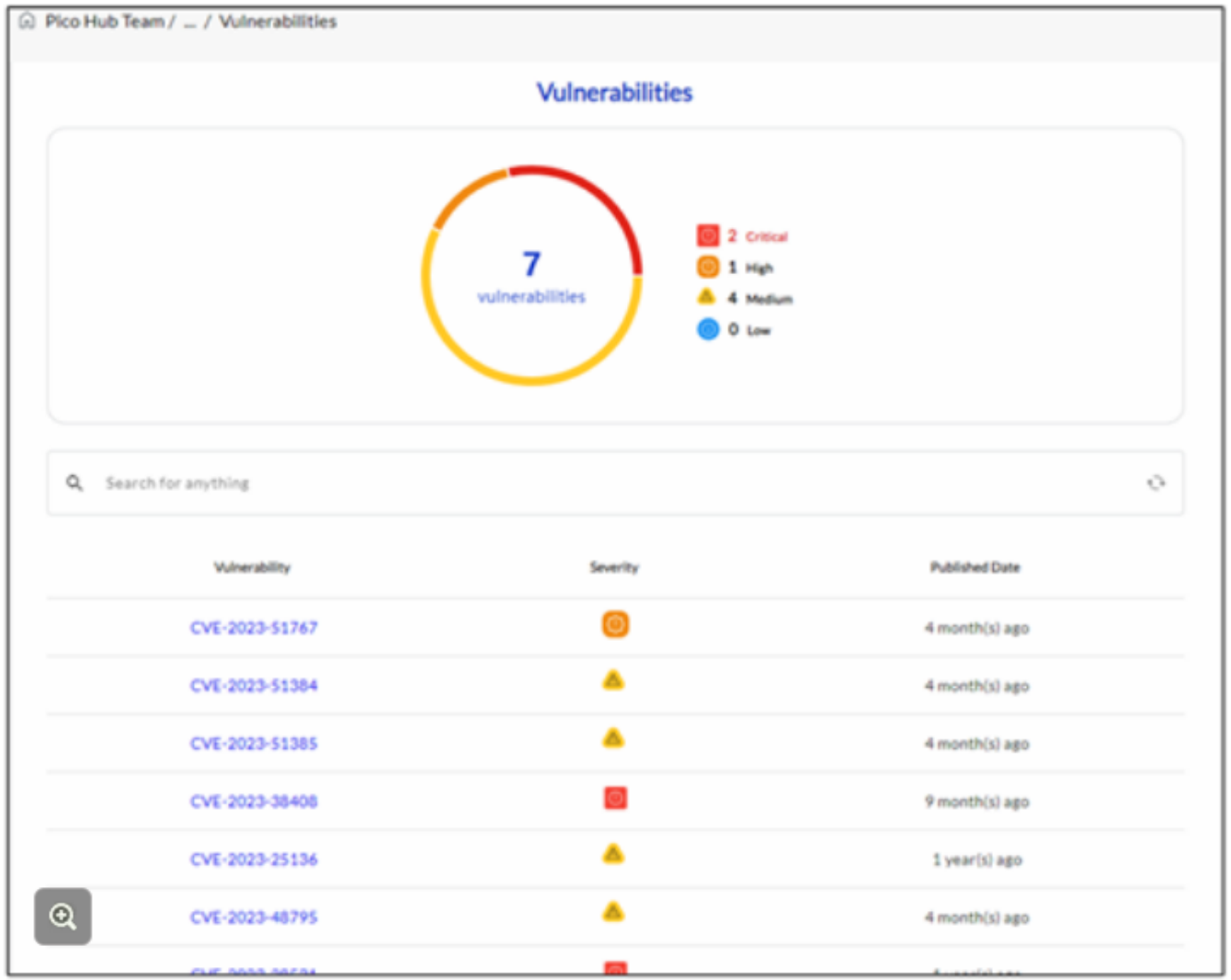
Note: As of Q4 2024, thresholds can only be set for the processor and memory.

CVE analytics

Common vulnerabilities and exposures (CVE) can be analyzed by going to the **Vulnerabilities** panel on the **Monitor** page.
The panel contains a donut chart and a bar chart. The donut chart shows the total number of critical, high-, medium-, and low-level CVEs. The bar chart shows how old the vulnerabilities are.
All information shown in the panels relates to events created in the last 12 months.

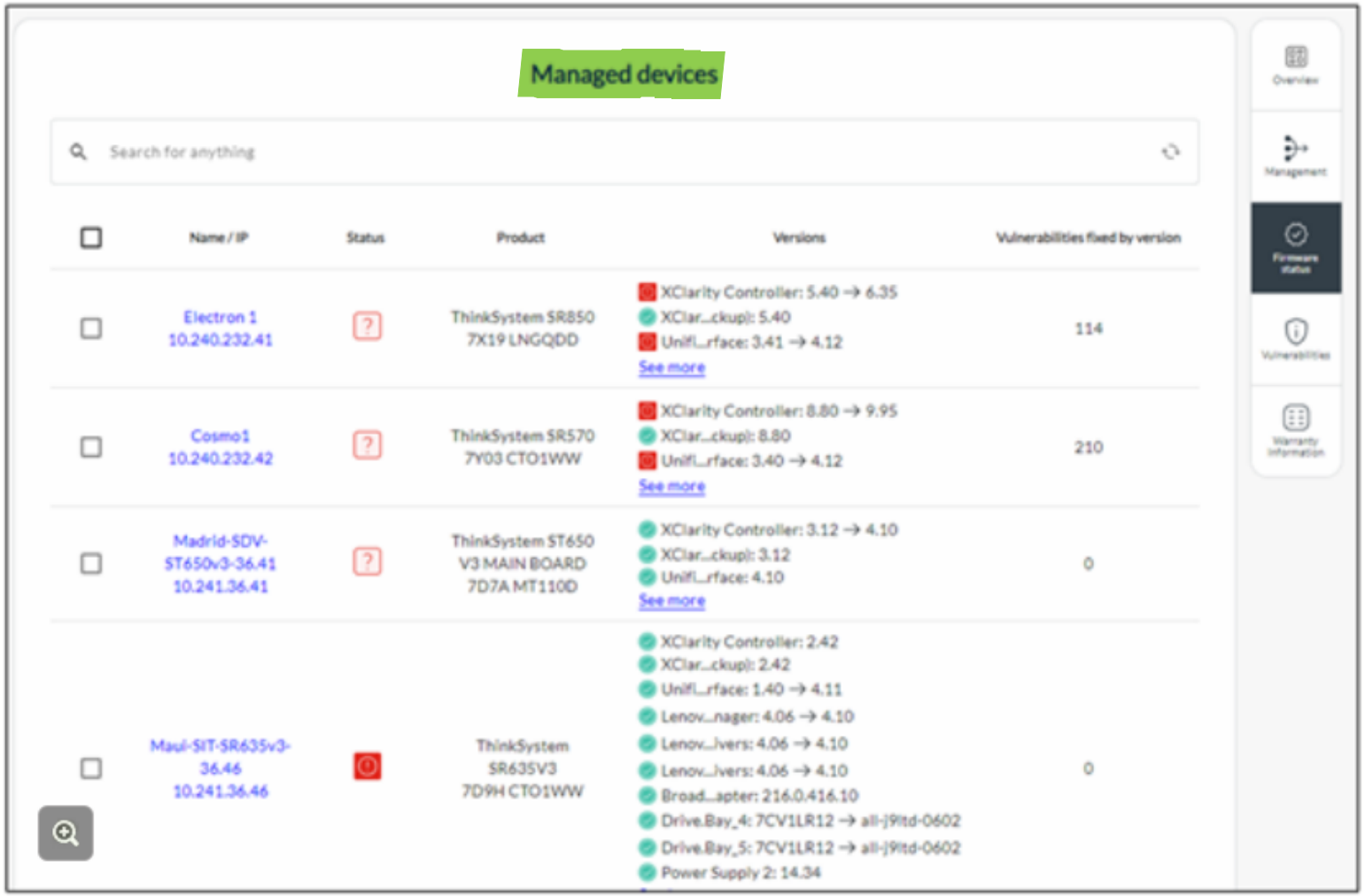
Details of CVE analytics

Click the donut chart to go to the **Vulnerabilities** page where vulnerabilities are listed with a severity level and the date on which they were published. By hovering the cursor over the item, more specific information about the published date will be shown.



Firmware health

- From the **Managed devices** page, select **Firmware status** from the context menu to see firmware health information.
- Along with the health icon there are suggested firmware upgrades.
- More firmware information can be seen in the **Firmware inventory** page. For an overview, refer to the Firmware inventory slide.



Memory Predictive Failure Analysis

XClarity One uses AI to predict potential memory failures. Memory diagnostic logs are collected from managed devices every 24 hours and then refined for analysis. The AI model, which is trained on real-time data, generates accurate prediction outputs to suggest preventive actions. While the AI's predictive capabilities are reliable, more validation is required before taking actions like shipping replacement parts.

Memory Predictive Failure Analysis (MPFA) will be available with version 24.3. To use the feature, customers must enable the **Call Home** feature. All data collected is anonymized for model training.