# Active Device Identification and Vulnerability Tracker for Industrial Control Systems

**Darktrace actively identifies industrial control system (ICS) devices and automatically maps known vulnerabilities alongside them to enhance organizations' visibility into their industrial environments, enabling them to better comply with frameworks, regulations, and government guidance.**

## Key Benefits

- ✔ Provides fullest picture of ICS Devices in your environment
- ✔ Actively requests device ID in narrowest way possible
- ✔ Maps CVEs alongside devices, updating CVEs & mapping automatically

"Once deployed, you will find out that you have not seen anything before."

CIO, Manufacturing

## Self-Learning AI: A Novel Approach

Darktrace's Self-Learning AI takes a fundamentally different approach to cyber defense, learning an organization's 'patterns of life' to understand subtle forms of unusual behavior indicative of threat. This allows the technology to detect both known and unknown threats, including sophisticated attacks that leverage zero-day exploits and novel tactics, techniques, and procedures (TTPs).

Self-Learning AI does not require lists of common vulnerabilities and exposures (CVEs) to detect, investigate, and autonomously respond to threats. Alongside Darktrace's Immune System approach, however, Darktrace does offer Active Device Identification and Vulnerability Tracker modules for organizations who desire these capabilities for their ICS devices.

"It did a great job of identifying 'SCADA' type devices on the network. It works well in a sensitive environment."

CTO, Services

## Active Device Identification

By drawing upon passively obtained information about the protocols and ports already in use on ICS devices, Darktrace can actively request device information in the most specific and narrow way possible. This minimizes the overall risk of an active approach.

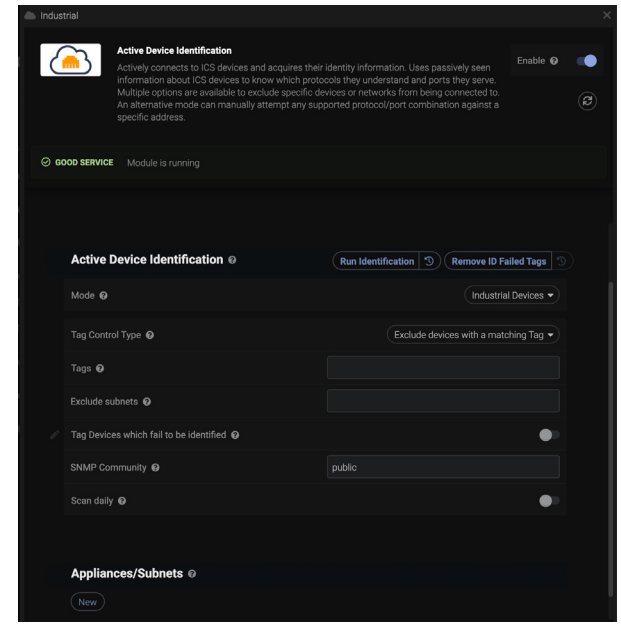


Figure 1: Darktrace's Active Device Identification module

Most Operational Technology (OT) networks do not advertise their device identities in ongoing network traffic. By actively connecting to ICS devices, Darktrace can acquire their full identity information—typically including device type, hostname, model, firmware, and any other miscellaneous data the device may offer such as product code or hardware version.

This module is highly configurable and can be used in a targeted capacity. Multiple means are provided to exclude specific ICS devices or networks of particular concern. It can scan daily or on demand and can also be deliberately aimed at specific devices.

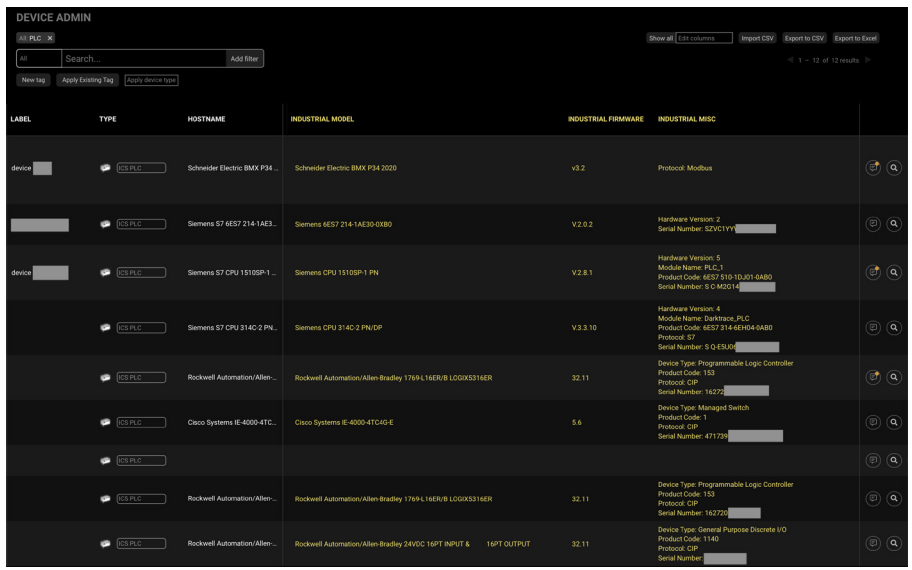


Figure 2: An example of ICS devices in the Device Admin page

## ICS Vulnerability Tracker

Common Vulnerabilities and Exposures (CVEs) only represent known and researched vulnerabilities, of which there are very few investigated in the OT sphere. Their absence does not indicate an absence of risk, a situation and combination that can very easily mislead.

Further, many CVEs have no practical mitigation advice. This foregrounds the strength of Darktrace's Immune System approach, which does not rely upon prior knowledge of flaws in devices and is also able to find threats making misuse of legitimate services.

However, many organizations still desire to track and map known vulnerabilities for their own visibility and also in efforts to comply with frameworks, regulations, or government guidance. Darktrace offers this ICS vulnerability tracking and mapping capability—which is strongly enabled by its Active Device Identification module—as most ICS CVEs can only be mapped successfully when exact device details and firmware versions are known.

The ICS Vulnerability Tracker module tracks and maps CVEs against monitored OT and ICS devices, updating both CVEs and their mapping automatically. It is kept updated from the NVD database or, if unable to contact the internet, from Darktrace software updates.

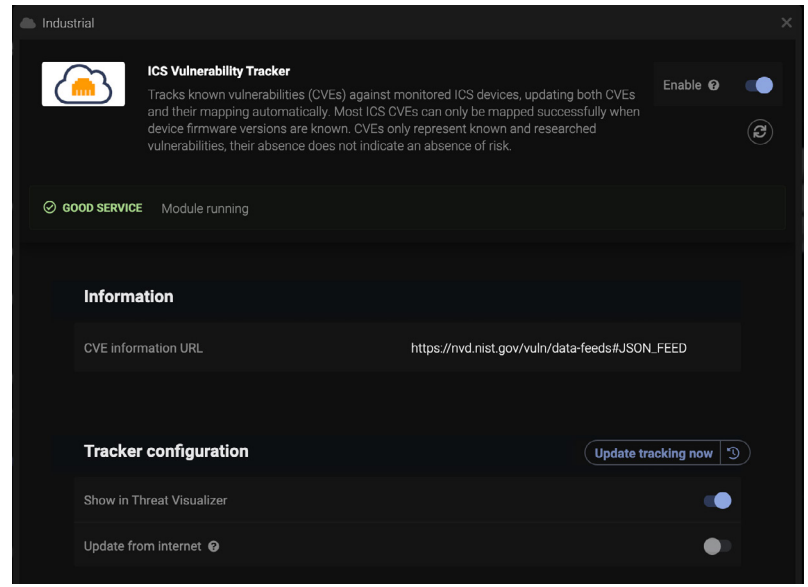


Figure 3: Darktrace's ICS Vulnerability Tracker module

The module shows devices within the network that have known CVEs, with the relevant CVEs listed and described per device. It also shows why each CVE is relevant to the specific device (i.e., CPE mappings).

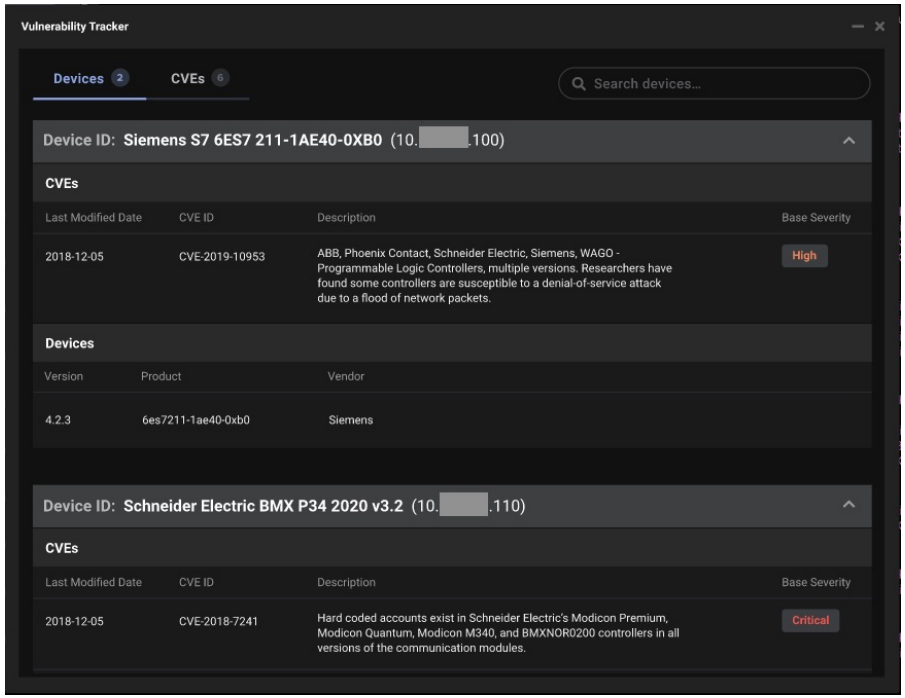


Figure 4: Devices mapped alongside associated CVEs with descriptions

The ICS Vulnerability Tracker module also has the option to show all known OT and ICS CVEs present within the environment, alongside the base severity (e.g., critical or high), the description of the CVE, and the devices on which it is present.

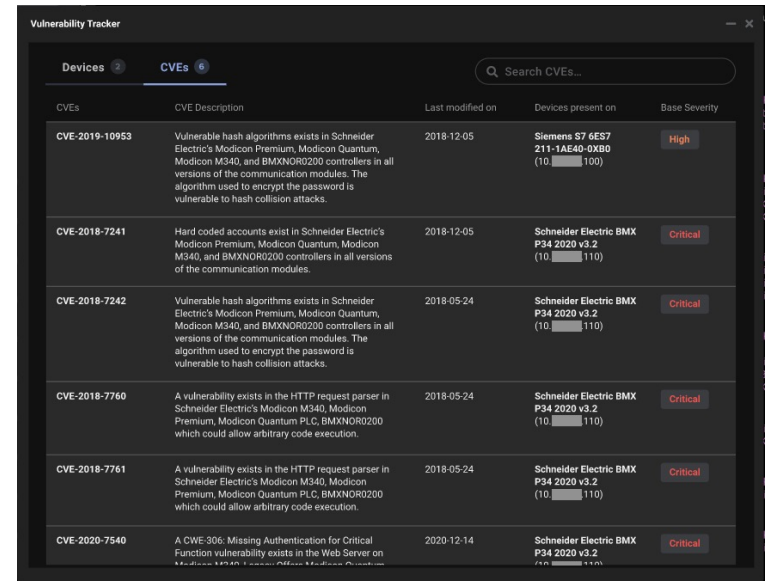


Figure 5: Catalogue of all CVEs present within the environment

To allow users to quickly identify the known vulnerability state of a device of interest, Darktrace tags devices with highest severity rating of any matching CVE. It also tags devices that have a recently discovered CVE for two weeks.

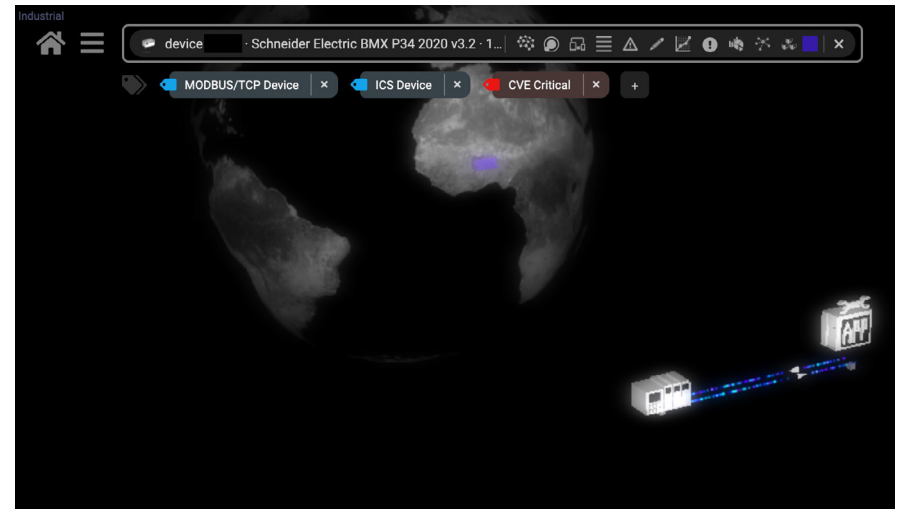


Figure 6: Darktrace tagging devices with highest severity rating