Darktrace/OT: Self-Learning Asset Identification

AT A GLANCE:

- Self-Learning AI helps teams discover what they've never seen before
- Automatically catalogues IP-connected and non-IP ICS devices
- Playback feature pinpoints device connections to rewatch activity in real time

SUMMARY

Asset identification is critical for building robust cyber security in industrial environments. At the same time, due to the diversity of devices and the bespoke protocols often used in industrial control systems (ICS), many organizations still struggle to maintain an accurate and up-to-date catalogue of all assets. Darktrace's self-learning asset identification helps organizations meet this challenge by providing full visibility throughout the entire cyber-physical ecosystem.

Darktrace/OT provides comprehensive asset discovery by understanding communication between assets within a given cyber ecosystem, automatically creating an inventory list from the data points available. Harnessing the power of Self-Learning AI, Darktrace achieves this in an entirely autonomous capacity.

From raw network traffic, Darktrace can detect all IP-connected devices and certain non-IP industrial devices, such as serial-connected PLCs. Using associated information, Darktrace creates a profile for each device and builds a full history for every device that has been seen in the network. As the environment changes, Darktrace's AI can adaptively identify new technologies added to the ecosystem.

Passive Analysis

In its standard configuration, Darktrace uses data with passive analysis interfaces (IP-unconfigured). When active, Darktrace is limited by the content of the network traffic. Crucially, as there is no active interaction with the assets in question, there is no effect on their function.

Based on the behavior of the assets, Darktrace automatically classifies the devices into high-level types. These include ICS device types such as PLC, HMI, and Workstation, as well as IT assets (e.g., desktop, laptop, server), and IoT devices (e.g., printer, mobile, smart devices). The tool does this by looking at a number of metrics, including but not limited to: ports and protocols used, other devices interacted with, and whether the device is providing network services for other devices on the network.

In this way, operating system, device type, hostnames, and network location are identified autonomously. Moreover, device criticality and Purdue model location can be implemented both manually and on the basis of a pre-defined set of criteria. Firmware versions and serial numbers can be identified if they are present in network traffic, but these are not required for Darktrace to perform autonomous threat investigations.



Figure 1: Darktrace Threat Visualizer homepage.

Active Option

Device data can be queried by using Darktrace's Advanced Search function and Elastic Search, by using the API, or by using threat detection models specifically designed for OT environments. Darktrace can also actively 'smart poll' devices for their identities if desired.

Where and when active asset discovery is requested by the system operator, only documented function codes are used to derive the information. Active connections with native identity requests are made from Darktrace to each relevant device, drawing on passively collected knowledge of the protocols and ports where each device operates.

Active identification typically returns the vendor, model, and firmware of a device, although this is protocol- and device-dependent. All possible caution is taken. At the same time, active identification of devices that may have unique operating histories and pre-existing reliability issues does carry inherent risks.

Whether passively or actively identified, model and firmware knowledge allow known vulnerabilities to be mapped to the devices. However, security teams should take great care not to be drawn into thinking that known vulnerabilities represent all risks, as compromises frequently make use of zero-days, which are unknown vulnerabilities and may misuse legitimate operations in ways that cannot be trivially recognized as malicious.

Devices with no or few known vulnerabilities may also just be lacking specific research into them, rather than being more secure. Crucially, Darktrace does not require vulnerability information or use it in detection methods.

Comprehensive Visualization

Device and connection visuals are also available through Darktrace/OT's user interface, the Threat Visualizer, which allows for the 3D presentation of all data flows.

In addition, a mapping of the full network — including all subnets, traffic flows among them, and external endpoints — is available using the Darktrace Explore feature, which allows users to drill down into the subnet and device level. Similarly, traffic between security segmentations is also available. Darktrace's playback feature allows users to view a device of interest at a chosen time to see other devices to which it has connected and also to rewatch activity in real time.



Figure 2: Darktrace Threat Visualizer identifying actioned and breached devices in subnets.

About Darktrace

Darktrace (DARK.L), a global leader in cyber security artificial intelligence, delivers complete AI-powered solutions in its mission to free the world of cyber disruption. Its technology continuously learns and updates its knowledge of 'you' for an organization and applies that understanding to achieve an optimal state of cyber security. Breakthrough innovations from its R&D Centers have resulted in over 135 patent applications filed. Darktrace employs over 2,200 people around the world and protects over 8,400 organizations globally from advanced cyber-threats.

Scan to LEARN MORE

© 2023 Darktrace Holdings Limited. All rights reserved. The Darktrace name, logo, and other trademarks used herein are trademarks of Darktrace Holdings Limited. The names of other companies, products and services are the property of their respective owners.