

Industrial Immune System: POV Coverage

The Darktrace Proof of Value (POV) is a free 30-day trial of Darktrace's Industrial Immune System technology. The POV provides you with the opportunity to observe the full capabilities of our Cyber AI in action as it protects your unique industrial environments, including both OT and combined OT/IT ecosystems. Darktrace defends against the full range of cyber-threats, including zero-day exploits, insider threats, supply chain attacks, abuse of legitimate tools, and devices infected prior to deployment.

At a Glance

- ✓ 1-hour 'plug and play' deployment
- ✓ Detects the full range of ICS threats
- ✓ AI-driven investigations
- ✓ Passive and optional active asset identification
- ✓ Specialized features for OT experts

Detects Known and Unknown Threats

The Industrial Immune System performs threat detection without the need for historical training data and lists of CVEs. Rather, Darktrace autonomously builds a dynamic understanding of 'normal' for every device, user, and cluster of similar users and devices, as well as the ICS environment as a whole. This allows Darktrace to spot subtle signs of unusual behavior to detect emerging threats in their earliest stages, before they escalate into a crisis. In this way, Darktrace detects known threats in the exact same fashion as it detects never-before-seen attacks.

Cyber AI Analyst for OT

With specialized models for ICS environments, Darktrace's Cyber AI Analyst automatically investigates all unusual behavior, connecting the dots between disparate events to illuminate fleshed out security incidents. Cyber AI Analyst automatically investigates the scope and severity of threatening activity—generating a natural language report of the incident which includes a timeline of the threat in attack phase terminology.

In ICS environments this proves particularly useful, as it closes the 'knowledge gap' between OT specialists who may lack experience in cyber security and security professionals who may be new to OT security.

Self-Learning Asset Identification

The Industrial Immune System provides comprehensive asset discovery by ingesting all communication between assets within a given cyber ecosystem, automatically creating an inventory list from the data points available. With self-learning Cyber AI, Darktrace adapts to the bespoke nature of your complex infrastructure, identifying legacy devices alongside cutting-edge IIoT technologies and evolving alongside any changes in your operations, as well as advances in your automated processes.

Darktrace achieves this all without the need for human input. Darktrace's asset identification is inherently passive, avoiding any interference with device operations. An active option is also available as desired.

“Using machine learning, Darktrace detects zero-day threats and suspicious insider behaviors, without having to define the activity in advance.”

Director of Innovation and Technology, City of Las Vegas



OT Engineer and OT Explore

Darktrace's OT Engineer and OT Explore capabilities translate the insights of self-learning AI into visuals and text that speak to the particular expertise of OT specialists.

The OT Engineer dashboard provides a subset of alerts that have high operational relevance for those with typical knowledge of the controls engineer domain. These alerts provide immediate information for fast triage, with the aim of minimal interface time. OT Engineer benefits from Darktrace's native ability to evolve alongside network changes, such that it does not need manual operation to keep it up to date.

Darktrace's OT Explore visualizes the network, connections, and data movements from a device and subnet perspective. This allows OT specialists to examine real-time architecture in ways that compare directly with diagrams and also surface unexpected relationships through tags.

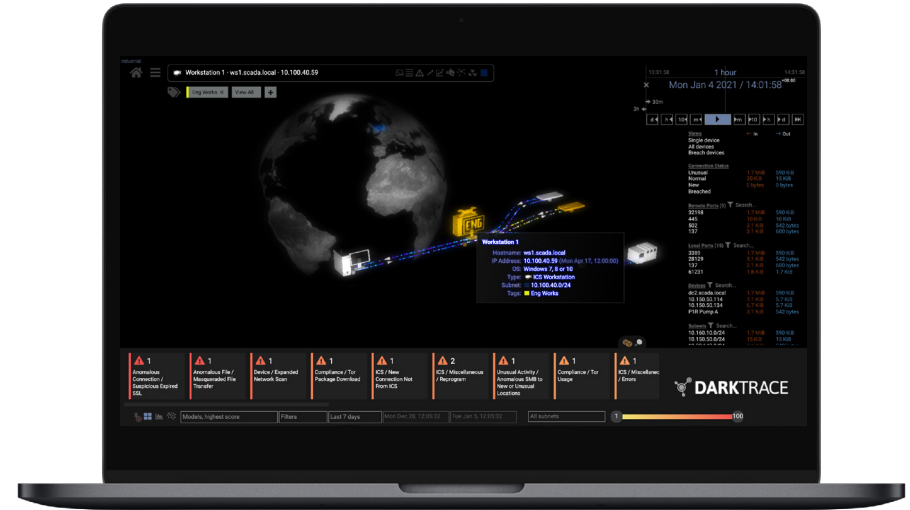
“Enterprises that require a cyber security solution for IT, OT and physical environments will find Darktrace an effective tool for real-time advanced threat detection.”

Earl Perkins, Gartner, 'Cool Vendors in Energy & Utilities'



An Immune System for OT Security

Organizations seeking the most cutting-edge solution for defending their critical ICS environments will find an ideal technology in the Industrial Immune System. It is the only technology that can detect and investigate never-before-seen threats in real time, and also identify all assets and points of IT/OT convergence.



Darktrace's Industrial Immune System detecting unusual activity surrounding an ICS workstation

[See the 'OT Security' section of Darktrace's blog for further use cases and threat finds.](#)






About Darktrace

Darktrace is a leading autonomous cyber security AI company and the creator of Autonomous Response technology. Its self-learning AI is modeled on the human immune system and used by over 4,700 organizations to protect against threats to the cloud, email, SaaS, traditional networks, IoT devices, endpoints, and industrial systems.

The company has over 1,500 employees and is headquartered in Cambridge, UK. Every second, Darktrace AI fights back against a cyber-threat, before it can cause damage.

Darktrace © Copyright 2021 Darktrace Limited. All rights reserved. Darktrace is a registered trademark of Darktrace Limited. Enterprise Immune System, and Threat Visualizer are unregistered trademarks of Darktrace Limited. Other trademarks included herein are the property of their respective owners.

For More Information

-  Visit darktrace.com
-  Book a free trial
-  Visit our YouTube channel
-  Follow us on Twitter
-  Follow us on LinkedIn