DARKTRACE
INDUSTRIAL

OVERVIEW

Darktrace Industrial Immune System

Key Features

- Self-learning: constantly refines its understanding of normal
- 100% network visibility
- Passively monitors raw network traffic
- Spots threats in real time
- Works from day one & delivers instant value
- Vendor & protocol agnostic: ingests all data sources
- Linearly scalable

> Darktrace helps us stay ahead of emerging threats and better defend our key systems.
>
> **Martin Sloan,**
> **Group Head of Security, Drax**

Darktrace's Industrial Immune System is a fundamental technology platform for OT cyber defense. Based on proprietary machine learning and AI algorithms, the Industrial Immune System is capable of learning what 'normal' activity looks like within industrial networks, and can identify and respond to emerging threats that would otherwise go unnoticed.

By monitoring over 350 dimensions of activity, Darktrace creates 'pattern of life' models for every device, user and controller on your network to detect subtle shifts in behaviors. For example, unusual PLC reprogramming or anomalous trends in protocols may indicate a potentially threatening event: a PLC beaconing to the internet, an IT device with unauthorized access connecting to an HMI, or the actions of a disaffected or negligent employee. Such activities may indicate a compromise or ongoing threat if they represent a significant departure from normal behavior.

Industrial Networks & Protocols

Darktrace's Industrial Immune System works by passively ingesting network data via a SPAN port or network tap. It is able to monitor industrial networks with no disruption to normal functioning of ICS operations, including plants and machinery, and at no point can it interfere with critical control communication.

Using the port mirroring functionality of existing switches or fail-safe network taps, copies of the data are sent to the Darktrace appliance for processing. As Darktrace does not sit in-line, it can easily handle the volume of traffic present in control networks and assess the nature of the communications rather than the content.

Darktrace works very effectively on all forms of network communications, whether encrypted or not. As such, Darktrace is able to cover all ICS protocols that use IP networking technologies and can provide visibility into ICS devices that are not attached to the TCP/IP network, as long as their communications enter the TCP/IP network at some point. Additionally, deep inspection is available for a growing list of protocols.

.

Machine Learning & AI Algorithms

Darktrace's probabilistic approach to network security is based on a Bayesian framework. This allows it to integrate an extensive number of weak indicators of potentially anomalous network behavior to produce a single clear measure of how likely a network device is to be compromised.

This approach accounts for the inevitable ambiguities that exist in data, and distinguishes between the subtly differing levels of evidence that different pieces of data may contain. Instead of generating the simple binary outputs 'malicious' or 'benign,' Darktrace's Industrial Immune System produces outputs that indicate differing degrees of potential compromise. This enables users of the system to triage different alerts in a rigorous manner, and prioritize those which most urgently require action, while simultaneously removing the problem of numerous false positives associated with a rule-based approach.

> Cyber security needs a quantum leap forward. It needs to rely on machine learning-based artificial intelligence.
>
> **James Scott, Senior Fellow, Institute for Critical Infrastructure Technology**

Darktrace Threat Visualizer

Using cutting-edge visualization techniques, the Threat Visualizer user interface automatically alerts users to significant incidents and threats within their OT environment, enabling them to proactively investigate specific areas of the ICS.

The Threat Visualizer provides users with insights into the relationships and data flows across the network, in real time delivering an instant overview of day-to-day network activity. By leveraging the Threat Visualizer, operators can see what is happening in their control systems by visually representing both individual and peer behavior. This works at a high level, identifying diverse threats and anomalies for the operator's attention, and at a more granular level, allowing them to drill down and view specific clusters of activity, zones, and PLCs.

> Darktrace has revolutionized our security. The amount of visibility we achieve from its machine learning approach is unmatched. We are now finding anomalies, in real time, that would have taken us weeks, or even months, to find on our own.
>
> **Terrell Johnson, Manager of Systems and Networks, Sunsweet**

Installation and Configuration

The Darktrace appliance is installed within an hour by a trained Darktrace Cyber Technology Specialist. It works from day one, and immediately begins gathering and analyzing network data.

A single Darktrace appliance can take multiple inputs of network traffic and cover tens of thousands of individual machines, depending on peak traffic volumes. Multiple Darktrace appliances can be federated to cover different ICS zones, or geographically-distributed systems, and deployments can span IT and OT environments securely.

Darktrace consumes raw network traffic collected by either port spanning your existing network equipment or by inserting or re-using an inline network tap or SPAN.

Proof of Value

Darktrace offers organizations the ability to evaluate the power and benefits of the Industrial Immune System, conducting a Proof of Value (POV) or pilot phase. The POV offers a unique opportunity to experience at first hand Darktrace's ability to detect previously unseen threats and anomalous behaviors within your industrial environment.

Contact Us

North America: +1 415 229 9100
Europe: +44 (0) 1223 394 100
Asia Pacific: +65 6804 5010

info@darktraceindustrial.com
darktraceindustrial.com