Cyber AI Platform

Industrial Immune System

Powered by Cyber AI, the Industrial Immune System is a self-learning technology that detects cyber-threats and vulnerabilities in industrial environments. The solution works by passively learning what 'normal' looks like across OT, IT and industrial IoT, allowing it to recognize subtle indicators of emerging attacks which would otherwise go unnoticed.

Key Benefits

- Learns on the job
- 100% visibility across OT, IT and IoT
- Automatically tailors itself to your environment
- Technology and protocol agnostic
- Detects subtle signs of emerging threats or vulnerabilities in real time
- Adapts to changing environments

Deep Coverage at Scale

By monitoring network traffic, the Industrial Immune System has direct visibility into and provides self-learning protection across everything from Basic Process (Purdue Model Level 1) through supervisory functions, business logistics and enterprise networks (Levels 4 & 5) and beyond into cloud networks and SaaS services.

Passive Monitoring

Connecting new devices to industrial networks is never straightforward and routine, as for many applications even the slightest interruption in service can be damaging.

The Industrial Immune System is connected passively to an ICS network, receiving copies of as much communication traffic as possible. It ingests copies of raw network data using the built-in port mirroring or 'spanning' capabilities of network switches, or using fail-safe taps, sometimes via an aggregator to bring together numerous connections in one location.

Self-Learning AI

Powered by AI, the Industrial Immune System protects your industrial environment from threats and vulnerabilities of all types, and adapts automatically to your specific networks. Rather than relying on blacklists, the technology works by learning 'on the job' and identifying emerging anomalous activity.

This self-learning capability means that the Industrial Immune System is truly protocol-agnostic and effective in any operational environment, from Modbus, to BACnet, to CIP. The Industrial Immune System works seamlessly with all manner of technologies – without interruption to regular operations.

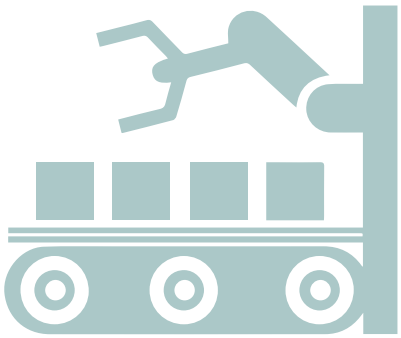
Unified View Across OT, IT, and IoT

Through its intuitive Threat Visualizer interface, Darktrace gives security teams an instant overview of their diverse digital infrastructure, including every user, device, and controller in the network. This enables operators to proactively investigate cyber-threats and specific areas of the ICS.

The Threat Visualizer is usable at operator level as well as from IT Security Operation Centers, enabling collaboration across OT and IT security teams.

The Threat Visualizer displays a graphical, real-time overview of the industrial environment and allows for in-depth investigations.

Real-World Use Case: Compromised Equipment on the Assembly Line



An unknown attacker targeted several industrial IoT devices on a leading food manufacturer's assembly line. Equipment including baggers, slicers, and blenders were attempting to connect to external destinations and move within the corporate network. These devices lacked security approval to connect to the core IT infrastructure.

Correlating these factors in real time, Darktrace AI identified the anomalous behavior as a significant risk to the integrity of both the corporate network and the assembly line. With Darktrace's artificial intelligence, the entire infrastructure was visualized and protected, including Industrial IoT and ICS.

The security team was able to take the compromised devices off the network, preventing the food provider's manufacturing infrastructure from any harm and before the attacker could gain access to the core IT infrastructure.

What Our Customers Say

> Darktrace Industrial is fundamentally changing the game of ICS defense.
>
> **- Chief Information Officer, City of Las Vegas**

> AI is vital to our security posture, as it is flexible enough to defend our entire SCADA environment, including diverse legacy systems.
>
> **- Director of Networking, Utilities Kingston**

> There's no denying the benefit that Darktrace delivers. It is not about being able to shut all the doors, as someone will always leave one open – whether it is an infected USB stick or software drive-by vulnerability. What matters is your ability to identify a breach once it has happened.
>
> **- Group Head of Security, Drax**

For more information

Book a demo now

Download our white paper

Hear from our customers