Why the Industrial Immune System?

Cyber defense in industrial environments poses a unique set of security challenges.

The constant expansion and evolution of industrial infrastructure makes it difficult to gain visibility into a diverse range of operational technologies (OT). Decades-old ICS and SCADA systems are also often used alongside recently developed technologies, further complicating defense.

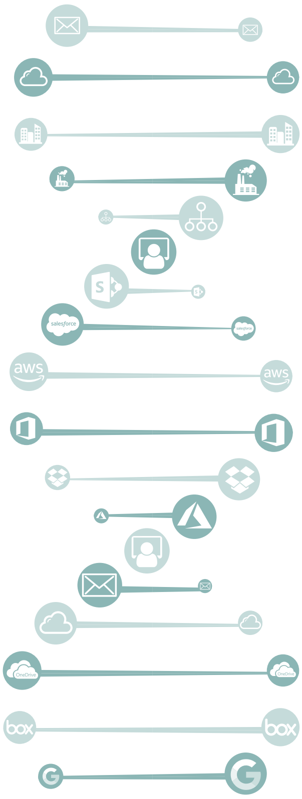
Never-before-seen threats, or 'zero days,' easily bypass whitelists, rules, and signatures. Historically informed methods cannot keep pace with these rapid advances in the techniques of attackers, as well as transformations in industrial infrastructure itself.

Empowering organizations to tackle these challenges, Darktrace's Industrial Immune System leverages advanced AI to catch never-before-seen threats in real time. With its ability to defend OT systems in a technology- and protocol-agnostic capacity, self-learning AI is uniquely able to evolve as your industrial environment changes, staying one step ahead of attackers.

Darktrace's Industrial Immune System illuminates the technology infrastructure of even the most complex cyber-physical ecosystem, supercharging efforts to ensure availability and integrity of industrial technologies.

> "Darktrace helps us **stay ahead** of emerging threats and better defend our key systems."
>
> \- **Drax Power Station**

> "Darktrace is fundamentally **changing the game** of ICS cyber defense."
>
> \- **City of Las Vegas**



Why?

1. AI that continuously learns 'self'–no tuning necessary

- Because Darktrace AI understands the normal 'pattern of life' across unique industrial environments, it can detect sophisticated threats by spotting subtle deviations
- Policy rules and whitelists constantly require 'tuning' to filter out excessive alerts and false positives, and cannot continuously learn as the network expands or evolves, instead requiring manual configuration
- The Industrial Immune System continuously learns as your infrastructure evolves at scale, no maintenance needed
- The Industrial Immune System achieves this all autonomously, contextualizing behavior within the broader OT environment in an entirely self-learning fashion, without any necessary tuning
- The Industrial Immune System analyzes **behavior**, not **content**, which allows it to spot and stop anomalous incidents regardless of the source of the threat or the specific technology compromised, be it PLC, SCADA, HMI, or any novel integration (e.g., IIoT) or workflow innovation (e.g., ICSaaS)

With the constant evolution of OT systems, and their convergence with IT systems, attacks that reach industrial environments by first targeting peripheral systems are becoming increasingly mainstream. It has never been more important than now to move beyond siloed security applications and historically informed defense strategies.

Case Study: Illuminating Copperbelt Energy Corporation Plc's Complex Cyber-Physical Infrastructure

As a leading player in the energy and utilities space, the main concern for the Copperbelt Energy Corporation Plc was safeguarding its complex OT infrastructure. Increasingly connected with the IT network, its operating machinery had become vulnerable to new vectors of attack.

Early in its deployment, Darktrace's AI identified that the controller responsible for Copperbelt's gas turbines was originally managed remotely from a single internet-connected laptop. This represented a significant security risk of which the SOC was previously unaware: by targeting this laptop, attackers could significantly disrupt operations. The Industrial Immune System highlighted the risk, and Darktrace Antigena autonomously responded by neutralizing the risk before any damage could be done.

"Darktrace is always alive, looking at traffic across the entire digital estate. This is something that you would otherwise need several analysts to do," affirmed Choolwe Nalubamba, the Head of Telecommunications and Information Systems at Copperbelt. Darktrace shines a light into every corner of the network, displaying Copperbelt's OT, IT, and IoT networks in a unified view.

2. Detecting 'zero days' and other novel threats

The Industrial Immune system detects threats in a protocol- and technology-agnostic capacity, drawing upon self-learning AI algorithms to identify emerging threats in their nascent stages:

- The Immune System passively learns normal across your bespoke industrial environment, identifying emerging attacks based upon this evolving understanding, rather than prior indicators of threat
- Legacy approaches in OT environments, by contrast, fall into the same pitfalls as historically informed approaches in IT systems, namely, using past attacks to unsuccessfully defend against tomorrow's threats
- Historically informed methods to securing OT are blind to never-before-seen threats, that is, 'zero days'
- Darktrace's AI instead uses unsupervised machine learning to identify all unusual activity, and automatically ranks these by severity in its intelligent presentation of security incidents

Though other technologies may use AI to enhance the speed and scale of their historically informed methods, these fail to detect sophisticated and novel threats. Simply put, the Industrial Immune System learns the DNA of your technology infrastructure, achieving defense to a degree of depth and breadth that legacy methods can't match.

OT Threat Find: Advanced ICS Attack at International Airport

Without a list of known exploits, company assets, or firmware versions, Darktrace's Industrial Immune System recently detected every stage of a simulated state-of-the-art attack at an international airport. Had the attack been allowed to continue, it could have caused significant operational disruption to the airport.

The attack spanned multiple days and targeted the Building Management System (BMS) and the Baggage Reclaim network, with the attackers utilizing two common ICS protocols (BacNet and S7Comm). The attackers also leveraged legitimate tools in order to evade traditional, signature-based security tools.

Legacy security tools failed to pick up on this activity. Darktrace's deep packet inspection, however, was able to identify unusual commands used by the attacker within those 'normal' connections. Darktrace's Cyber AI Analyst was also able to perform a real-time automated investigation and accordingly recommend further steps for action.

3. Unified view across entire industrial environment—PLC, SCADA, HMI, and other emerging infrastructure

Achieving visibility throughout industrial environments has become an incredible challenge.

First, many forms of IT/OT convergence go unnoticed by human teams, often leaving the door open to attackers. The increasing convergence of cloud and OT systems leads to similar security weaknesses, as does the introduction of IoT devices into broader cyber-physical ecosystems, such as IIoT.

The Industrial Immune system provides a unified view by processing all traffic on a granular level in a protocol and technology agnostic capacity. Deployed passively so as to not disrupt critical operations, Darktrace's Industrial Immune System works seamlessly across different technology protocols and types, providing unparalleled visibility.

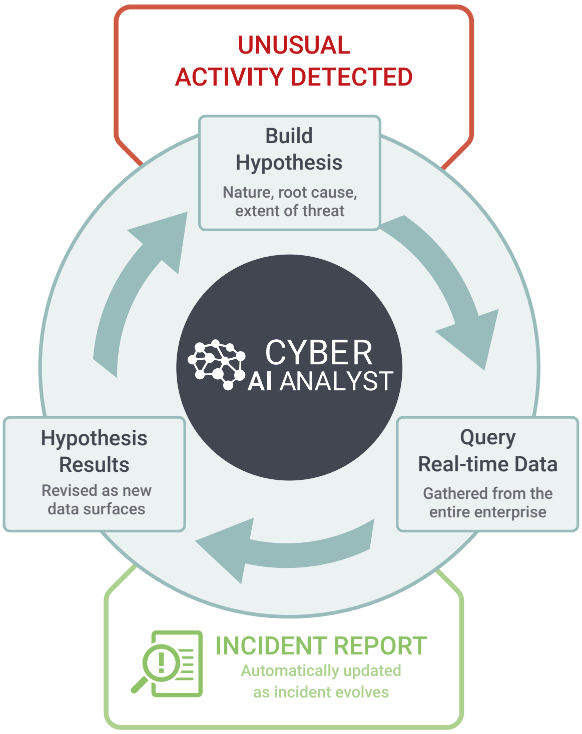
The Threat Visualizer, Darktrace's user interface, intelligently presents a three-dimensional representation of network topology in real time—across PLC, SCADA, HMI, IIoT, and other technologies that comprise many of today's unique industrial environments. Cyber AI Analyst's automated investigations and actionable insights are also available, and seamlessly integrate into the Threat Visualizer alongside other desired integrations.

4. Cyber AI Analyst augments humans, supercharging defense

Combining the precision and flexibility of human expertise with the scalability of AI, Darktrace's Cyber AI Analyst bridges the knowledge gap between specialists in IT and OT security, augmenting humans.

OT engineers are often unfamiliar with cyber security, while IT security experts are often unfamiliar with industrial technologies. Cyber AI leverages supervised machine learning to mimic the human intuition of its leading cyber analysts, including alumni from top intelligence organizations alongside teams of other world-leading experts.

Channeling this wealth of talent with advanced mathematics, Cyber AI analyst continuously investigates all security incidents, reducing time to triage of threats by 92% as it undertakes its automated investigation in order to jumpstart remediation and response.


UNUSUAL ACTIVITY DETECTED
Build Hypothesis
Nature, root cause, extent of threat
CYBER AI ANALYST
Query Real-time Data
Gathered from the entire enterprise
Hypothesis Results
Revised as new data surfaces
INCIDENT REPORT
Automatically updated as incident evolves

Caught in the Wild: Zero-Day APT-41

A world first, Cyber AI Analyst leverages supervised machine learning to mimic the intuition of the leading analysts and intelligence alumni. By conducting automated investigations, the innovation cuts down triage time by 92%, dramatically reducing 'time to meaning.'

Cyber AI Analyst caught a nation-state sponsored advanced persistent threat—zero-day APT-41—without any prior knowledge of the threat. This investigation was fully automated, and, crucially, occurred before any attribution or prior threat intelligence was even available. By stitching together disparate security incidents into an overarching narrative, Cyber AI Analyst was able to escalate this incident and convey the progress of the novel attack in executive friendly one-click reports.