DARKTRACE

Self-Learning AI for Industrial Control Systems

White Paper

Contents

A New Era of OT Cyber-Threat	**2**
The Industrial Immune System	2
The Challenge of Securing OT	**3**
Convergence with Traditional IT	3
Spillover from Corporate Network Compromises	3
Industrial Internet of Things	4
Threats Facing Industrial Control Systems	**5**
Ransomware	5
Insider Threat	6
Attack Case Studies	6
The Industrial Immune System	**7**
Real-Time Detection of Emerging Threats	7
Cyber AI Analyst: Augmenting Security Teams	8
Deep Coverage at Scale	9
Autonomous Response	9
Passive Observation	9
Asset Identification and Vulnerability Tracking	9
Unified Visibility Across OT, IT, and IoT	10
Darktrace Discoveries: Threat Finds	**11**
Suspicious Downloads and Serpent Ransomware Infection	11
Conti Ransomware	11
Reconnaissance Detected From Blacklisted External Device	11
Internal Reconnaissance Detected Within The OT Network	12
Real-Time Defense With Self-Learning AI	**13**
Darktrace Immune System Platform	**14**
Darktrace Proof of Value	14

A New Era of OT Cyber-Threat

The practice of cyber security has changed dramatically in the past few years, presenting a significant challenge to management teams across all industries and business domains. As IT security teams become accountable for defending Operational Technology (OT) and OT-specialist teams similarly inherit responsibility for traditional IT security, this technical convergence requires the synergy of both specialist skills and working practices.

Compromised OT devices within ICS and SCADA environments can lead to enormous physical damage and danger to human life. Since the widely reported discovery of the Stuxnet attack in 2010, threats to industrial systems have increased in both number and capability.

Today's malware campaigns can actively acquire critical data about control systems, quietly maintain persistent access, and then reprogram them, completing the kill chain. Legacy defenses such as firewalls have become antiquated and inadequate, especially in detecting threatening insiders with privileged access. Increasingly sophisticated machine-speed attacks, alongside ever-rising control system vulnerabilities, have heralded a new era of OT cyber-threat.

"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, Research VP, Gartner

"Darktrace is helping us stay abreast of the changes that are happening in the digital space."

CIO, McLaren Group

The Industrial Immune System

The Industrial Immune System is a cyber defense platform for OT environments which leverages AI to autonomously detect emerging threats, regardless of whether they appear on legacy tool deny lists or are completely novel zero-day attack techniques. Its intelligent understanding of an organization's entire cyber-physical ecosystem allows it to recognize even subtle signals of emerging threats in real time.

The technology provides complete visibility across OT, IT, and industrial IoT in a unified view, giving security teams oversight of its decision-making.

It works by passively analyzing the 'pattern of life' of every user, device, and controller, enabling the technology to recognize dangerous anomalies in behavior. Technology and protocol agnostic, it can be deployed across both OT and IT environments, providing full coverage of an organization without disrupting daily operations.

The Challenge of Securing OT

Convergence with Traditional IT

Even when operating in the same organization, corporate IT systems and Industrial Control Systems will have different objectives. Control engineers have historically been unimpeded by cyber-threats emerging through corporate IT systems, and IT security staff have had little contact with control systems or the physical equipment that those systems manage.

However, intensified competition resulting from globalization has propelled the convergence and synergy of the cyber-physical realm and more general and disparate information networks. Increasingly accountable for both OT and IT security, CISOs have also assumed responsibility for the defense of ICS environments without necessarily possessing the requisite specialized OT skills.

The most likely attack vector for ICS compromise is through the IT network – this has been true for most publicly known OT-targeted malware campaigns, as well as known cases of indiscriminate IT malware affecting OT systems.

The organizational changes that come with the convergence of OT and IT systems present new and significant technological risks but also provide an opportunity for improving OT security and resilience. Sharing a common network architecture will enable monitoring and detection strategies across both domains.

Spillover from Corporate Network Compromises

Industrial control systems are often damaged as an unintended side effect of attacks targeting corporate networks. Standard PCs that now form part of a typical ICS are open to the same compromises as their enterprise counterparts. Several cyber security breaches on major US power stations have been publicly attributed to this method of attack.

Additionally, the 2017 WannaCry ransomware attack that affected the IT systems of organizations across multiple verticals and geographies caused severe disruptions to manufacturing facilities across the world. Such incidents demonstrate that indirect compromises pose as significant a threat to operational environments as successful, targeted attacks against ICS.

Industrial Internet of Things

In addition to developments resulting from converging OT and IT systems, the scope of Operational Technology is broadening with the rise of Industrial Internet of Things (IIoT) devices being integrated into traditional ICS environments. The IoT paradigm presents two challenges – more complex and dynamic networks, and the deployment of new, unique technology.

There has been a dramatic increase in the number of connected devices in industrial environments, bearing significant implications for security teams. As the attack surface has expanded, complete visibility of the digital ecosystem has become increasingly unattainable.

As the shift towards IIoT introduces myriad device classes, there is widespread change across all forms of networked communications. The increasing availability of smart, small, form-factor devices is reorienting computing away from monolithic platforms towards highly distributed nodes. IoT devices are typically connected in wireless topologies, with processing and analytics distributed close to the last mile in ‘edge’ and ‘fog’ computing designs. Particularly in smart grids providing electricity to customers across entire districts, this means a broadened attack surface endangering millions of homes.

While effectively designed to be interoperable and resilient, industrial control systems are not necessarily easy to protect and are typically extremely difficult to update. Cyber security researchers are particularly concerned about the systemic lack of authentication in the design, deployment, and operation of some existing ICS networks. It has become clear that any possible connection to the internet can be exploited, even if it is not direct.

Meanwhile, patching is extremely difficult, as the inbuilt methods for delivering updates in operational environments are unsuited to the requirement of uninterrupted availability. Security support for operating systems at the point of installation has also proven not to last as long as the control systems themselves. Security teams suffer from the inability to retrofit security features into devices with decades of service life remaining.

Threats Facing Industrial Control Systems

ICS environments face numerous cyber security threat vectors with varying degrees of potential loss, ranging from non-compliance to disruption of operations which could result in the destruction of property and loss of human life. Examples of potential ICS-related threats include:

- Advanced Persistent Threats (APTs), including OT-targeted campaigns that bring together leading IT malware and OT control system attack skills
- Insider sabotage
- Supply chain disruption and compromised vendors or contractors
- Human misconfigurations
- Distributed Denial of Service (DDoS) attacks, resulting from increased use of the internet as an OT data transport mechanism

In June 2010, the Stuxnet virus targeted PLCs in Iranian nuclear centrifuges, marking the first revealed instance of targeted malware to cause physical damage and propelling the vulnerability of ICS environments into public consciousness. Since then, several high-profile attacks have hit manufacturers and utilities, including an attack targeting the Ukrainian power grid as well as the closure of a French power plant in the Middle East after malware had compromised its control systems.

Ransomware

Ransomware has become an increasingly prevalent threat for organizations operating ICS, with several high-profile attacks hitting organizations in recent years.

Many of these organizations provide critical infrastructure, meaning any disruption they suffer as a result of ransomware can have broad societal or safety consequences, and place more pressure on the organizations themselves to deliver ransom payments.

Ransomware can target ICS mechanisms directly, as with EKANS ransomware attacks, or can indirectly impact Operational Technology by disrupting the IT systems which provide essential visibility into them. IT/OT convergence has considerably widened the attack surface for OT ransomware, and made it harder to predict where attackers will come from next.

Insider Threat

Over the lifecycles involved with the building and utilization of infrastructure and manufacturing equipment, many individuals will have interacted with a given organization's industrial control systems and supporting physical equipment. Many of them will have had access privileges, allowing them to modify configurations of the underlying software and hardware.

Such increased ICS exposure allows malicious insiders' actions to be well-targeted and effective at disrupting operations. Insiders will not encounter border defenses and will have a greater ability to masquerade as others, making their activities harder to identify and attribute. Where supply chains or contractors are involved, it becomes increasingly impossible to distinguish between the 'inside' and 'outside'.

While vetting and training staff can reduce the risk of insider threat, there is still the possibility of a misconfiguration or a deliberate act of sabotage by a disaffected or ideologically motivated individual.

Monitoring complex cyber-physical ecosystems needs to start from a complete understanding of what is normal for each unique environment. Only then can security teams have the insight to identify the emerging patterns and correlated actions that indicate threat.

Attack Case Studies

Ukrainian Power Grid

In 2015 and 2016, Ukraine experienced the first known instance of an extensive and focused cyber-attack targeting the power grid at scale. These highly sophisticated attacks utilized advanced malware designed to compromise SCADA environments and left thousands of citizens without power for several hours. Since these incidents, the US Department of Homeland Security has issued warnings that long-term attack campaigns against the energy sector are ongoing.

Triton Attacks

In 2017, a multinational corporation was forced to shut down operations in a power plant in the Middle East after malware compromised its industrial control systems. The attackers used sophisticated malware, dubbed 'Triton', to take remote control of safety systems and attempted to reprogram them, causing related processes to shut down. Security researchers reported in 2019 that the same hacking group are targeting the industrial control systems of utility companies in the US, Europe, East Asia, and the Middle East.

Colonial Pipeline

In May, 2021, a ransomware attack struck the IT systems behind one of the largest pipelines in the US, forcing a full operational shutdown. When the 100 million gallons of oil transported daily by the pipeline were brought to a six-day halt, panic ensued and a state of emergency was declared in 17 US states. The attackers, later identified as DarkSide, took advantage of the organization's IT/OT convergence to apply pressure, and extorted a large ransom. Subsequent legislative changes in the US reflected the severity of this attack.

The Industrial Immune System

Organizations providing critical infrastructure must now look to a cyber security technology that delivers continuous insights and provides early warning of both indiscriminate and targeted compromises.

Darktrace's Self-Learning AI technology is a cutting-edge innovation that implements a real-time 'immune system' for operational technologies and enables a fundamental shift from the traditional approach to cyber defense. Built on a foundation of Bayesian mathematics and unsupervised machine learning, the system learns a 'pattern of life' for every network, device, and user.

Rather than relying on knowledge of past attacks, the technology learns what is 'normal' for its environment, discovering previously unknown threats by detecting subtle shifts in behavior. Through identifying these unexpected anomalies, security teams are able to investigate malware compromises and insider risks as they emerge and throughout all stages of the attack lifecycle.

"Darktrace Cyber AI Analyst provides high-fidelity alerts and incidents. I can instantly send that AI intelligence over to our SIEM as well as SOAR for automated actions. It's been a game-changer for the SOC."

Joe Albers, Cyber Security Engineer, Americas Styrenics LLC

Real-Time Detection of Emerging Threats

The traditional approach of blacklisting historical attack types cannot keep up with the pace of emerging vulnerabilities. Darktrace does not require a priori assumptions about environments or threats and can therefore detect the 'unknown unknowns': threats that are as yet unidentified, either because they are novel or have been tailored to a particular defender.

Darktrace continues to adapt and self-learn throughout its entire deployment. It does not require operators to manually maintain or instruct its understanding, allowing them to spend their limited time benefitting from the AI's output.

Whenever an abnormal change of behavior takes place, the Industrial Immune System identifies these deviations from the learned 'pattern of life' and alerts the organization to the possible threat. Because Darktrace's AI builds an evolving understanding of each cyber-physical ecosystem, it is vendor and protocol agnostic and can adapt and evolve to any operational environment.

The advanced mathematics that Darktrace leverages makes it uniquely capable of highlighting significant potential threats without burying them beneath insignificant or repeating alerts. Far more than a set of simple rules applied to network traffic, it can correlate many subtle indicators separated by type or time into strong evidence of a real, emerging threat, meaning that security analysts are not flooded with false positives.

"Artificial intelligence is now vital to our security posture, as it is flexible enough to defend our entire SCADA environment, including diverse legacy systems."

Kevin McCauley, Director of Networking, Utilities Kingston

Cyber AI Analyst: Augmenting Security Teams

While connecting new devices into a corporate network is generally risk-free, straightforward, and routine, the same is not true of industrial networks, where for many applications even the slightest interruption in service could be damaging.

The Industrial Immune System typically runs on a server that is connected passively to an ICS network, receiving copies of as much communication traffic as possible. It receives 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.

For cloud, edge, and physical deployments, Darktrace's lightweight, host-based OS-Sensors are installed on each cloud endpoint and configured to send intelligent copies of network traffic to a local vSensor deployed in the same cloud environment.

Cyber AI Analyst uses AI to automatically triage threats and generate at-a-click Incident Reports, drastically augmenting the capabilities of security analysts.

Powered by supervised machine learning, Cyber AI Analyst replicates expert human decision making, forming hypotheses and reasoning to reach informed and insightful conclusions. Cyber AI Analyst then presents a coherent security narrative of the overall incident in a matter of seconds.

Security teams that oversee both OT and IT as a result of digital transformation projects experience a huge increase in productivity when using Cyber AI Analyst. Both new and unknown threats are automatically investigated and time to triage is reduced by up to 92%.

Cyber AI Analyst can also help critical infrastructure organizations stay compliant in the face of new legislation such as the US Cyber Incident Reporting for Critical Infrastructure Act. This act requires certain cyber incidents to be reported to CISA within 72 hours. AI-generated natural language summaries accelerate the cyber incident reporting process, making it considerably easier for organizations to hit these government deadlines.

"There's no denying the benefit that Darktrace delivers."

Martin Sloan, Group Head of Security, Drax

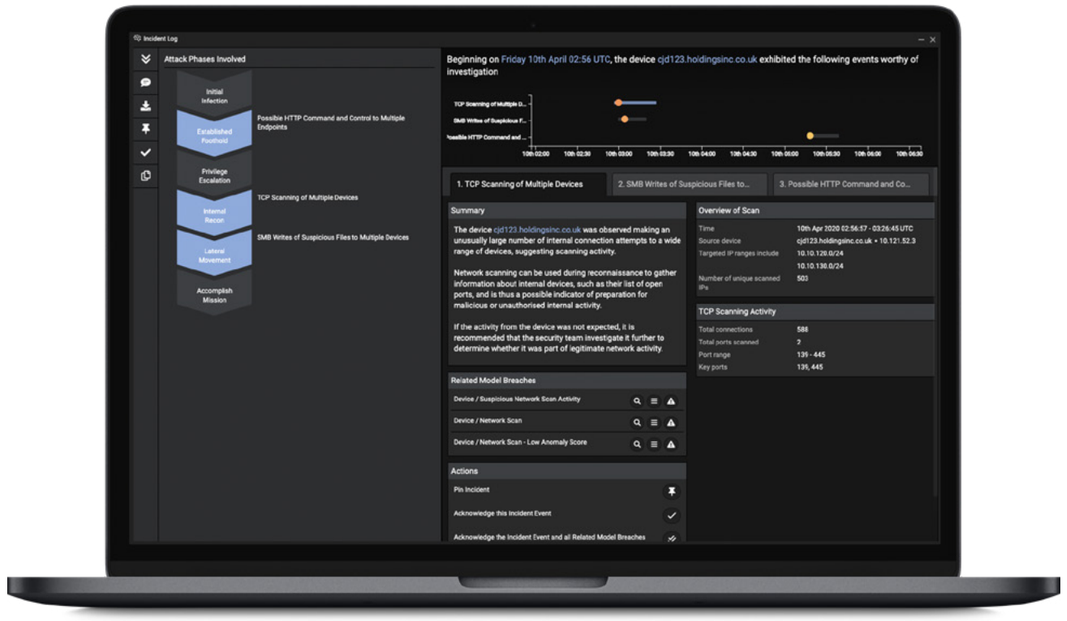


Figure 1: Cyber AI Analyst generates natural language summaries of security incidents

Deep Coverage at Scale

Modern OT networks are deliberately segregated following the principles laid out and refined over time in the Purdue model architecture. Through monitoring network traffic, the Industrial Immune System has direct visibility over and provides cyber security for everything from Level 1 (Basic Process) through to supervisory functions (2, 3), DMZs, business logistics, and enterprise networks (4, 5), and beyond into cloud networks and SaaS services. It also has indirect visibility into Level 0 (Process) as information about it transits the higher Levels.

From single appliances monitoring small localized networks, the Industrial Immune System can be scaled all the way to multinational businesses with millions of devices. Self-Learning AI is the only technology capable of handling threat detection in complex environments. Unlike simpler methods that inherently scale linearly with the number of devices, connections, or bandwidth in the network, Self-Learning AI takes advantage of the increased context available when judging the likelihood of a cyber-threat to scale its alerts far more effectively.

Autonomous Response

Darktrace's Autonomous Response takes action to stop emerging or underway threats in seconds, preventing fast-moving attacks like ransomware from causing damage to organizations. Because of its comprehensive understanding of the 'patterns of life' of organizations and their infrastructure, the actions taken by Autonomous Response are precise and proportionate, preventing further business disruption.

Autonomous Response is fully configurable. It can be set up in human confirmation mode, or tailored to act autonomously only on certain devices or during certain times or threat incidents.

Passive Observation

While connecting new devices into a corporate network is generally risk-free, straightforward, and routine, the same is not true of industrial networks, where for many applications even the slightest interruption in service could be damaging.

The Industrial Immune System typically runs on a server that is connected passively to an ICS network, receiving copies of as much communication traffic as possible. It receives 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.

For cloud, edge, and physical deployments, Darktrace's lightweight, host-based OS-Sensors are installed on each cloud endpoint and configured to send intelligent copies of network traffic to a local vSensor deployed in the same cloud environment.

Asset Identification and Vulnerability Tracking

Gaining visibility into assets in industrial environments is a challenge due to the diversity of devices used in OT and ICS ecosystems, from decades old legacy devices that are retrofitted, to cutting edge IIoT.

Based on the behavior of devices, Darktrace passively catalogues IP-connected and non-IP ICS devices, creating a profile and full history of all devices seen on network.

Darktrace also provides an optional active identification module. The active identification module makes requests to known OT devices to identify them using their observed and current protocol and service port combination.

Unified Visibility Across OT, IT, and IoT

Architectures of ICS and their operational networks are complicated and will typically have undergone many changes by multiple individuals over their lifetime. Darktrace addresses this challenge by observing, analyzing, and capturing communications along with their associated metadata.

Darktrace's unified view technology can be safely implemented as a separate appliance designed to provide a consolidated view into both OT and IT environments. Its user interface, the Threat Visualizer, uniquely displays all this rich information in an intuitive 3D dashboard that gives the operator a comprehensive, real-time overview of their network. This can be used to investigate whether the control system's actual behavior matches its intended design.

In ICS environments, segregation and zoning of the network is a critical security control, especially given the lack of security within endpoint devices themselves. In such environments, understanding the correct flow of data on the network and patterns of communication is essential. The Threat Visualizer allows security teams to view real-time information about data flows across OT, IT, and the Industrial Internet of Things, all while Darktrace's Self-Learning AI continuously compares this activity against expected behavior patterns.

While Cyber AI Analyst can be used to triage and investigate these detections, it is also possible to route the output to an organization's existing Security Information and Event Management (SIEM) systems to integrate with established processes and procedures.

Figure 2: The Threat Visualizer displays a graphical, real-time overview of the industrial environment and allows for in-depth investigations

Darktrace Discoveries: Threat Finds

Suspicious Downloads and Serpent Ransomware Infection

At an integrated oil refiner and supplier, Darktrace's Industrial Immune System identified the first signs of a ransomware infection in the company's network. As well as writing its own ransom note files, a desktop device was found to be making a series of connections to rare external destinations via an internal proxy server and dowloading potentially malicious files.

The device proceeded to make a number of SMB directory queries, amplifying the anomalous series of actions that the Industrial Immune System converted into multiple high-priority alerts relating to the device. Darktrace's Industrial Immune System recognized that this activity closely matched the typical pattern of behavior for ransomware, alerting the customer's security team before the infection was able to spread into their OT environment.

Conti Ransomware

In late 2021, Darktrace identified a Conti ransomware attack targeting an OT R&D investment firm in Europe. A compromised domain controller led to the infection of several devices, which performed network reconnaissance as the attacker began to escalate their privileges within the organization.

The ransomware payload was delivered when infected OT devices used SMB to connect to a folder on the domain controller and read a malicious executable file. This payload stayed dormant for some weeks while cryptomining software was installed elsewhere on the network. The device made successful C2 connections to around 40 unique external endpoints, and Darktrace detected beaconing-type behavior over suspicious TCP/SSL ports including 465, 995, 2078, and 2222.

Darktrace detected every stage of the intrusion, and Cyber AI Analyst stitched together many forms of unusual activity across the compromised devices to give a clear security narrative containing details of the attack. Had the target organization deployed Autonomous Response, or reacted to Darktrace's threat notifications, this ransomware attack would have been stopped in its earliest stages.

Reconnaissance Detected From Blacklisted External Device

Internal reconnaissance was detected at the heart of a US oil and gas production company. A rare internet endpoint that had never interacted with the customer's network before was discovered connecting to several key elements of the network infrastructure using a VPN.

After briefly connecting to the domain controller, it then connected to an employee's computer and the mail server, attempting to gain access via three different entry points. The Industrial Immune System detected this malicious exploration attempt in its earliest stages, giving the security team the ability to reinforce its defenses and ensure no compromises occurred.

> "Darktrace is the most critical tool we leverage to ensure that KOMIPO remains a leading power generation company and a resilient provider of national infrastructure."

Lim Kil-hwan, CISO, Korea Midland Power (KOMIPO)

Internal Reconnaissance Detected Within The OT Network

At a US manufacturing company, the Industrial Immune System highlighted a known but rarely active device within an OT network suddenly broadcasting multiple dedicated OT protocol commands for devices, using that protocol to respond with their identities. While the control system as a whole often used this command in various ways as part of its normal operations, this particular use was found to be unusual for several reasons.

The activity in this case proved to be benign, but most modern OT campaigns that use a specialized protocol payload perform a very similar step as part of their reconnaissance stages.

> "Signature-based malware detection is dead. Cyber security needs a quantum leap forward. It needs to rely on machine learning-based artificial intelligence."

Senior Fellow, Institute for Critical Infrastructure Technology

> "Darktrace is fundamentally transforming how we defend our systems."

Information Systems Manager, Layton Construction

Figure 3: The Threat Visualizer displays all the connections between every device in a cyber-physical ecosystem

Real-Time Defense With Self-Learning AI

Security teams in the OT space increasingly find themselves having to defend against attacks entering through the IT network. This convergence, alongside complex and evolving OT environments, is creating conditions in which cyber-attacks against operational systems are becoming increasingly frequent and effective.

With Darktrace's self-learning Industrial Immune System, organizations are able to detect emerging threats in real time, irrespective of device protocols, operating systems, or other characteristics that make OT networks unique from one another. Its AI autonomously forms an understanding of these diverse environments and also defends the IT network, enabling full visibility and protection across the entire digital business.

Hundreds of critical infrastructure providers across oil and gas, energy and utilities, manufacturing, transportation, and smart cities rely on Darktrace to protect their control environments against all forms of cyber-threat. With years of experience defending highly complex and diverse control systems, the Industrial Immune System has become the leading AI technology for industrial cyber defense that works across all existing OT technologies – and is ready for future ones too.

> "Self-Learning AI can detect cyber-threats before damage is done. You need AI in place to quickly identify and respond to threats – you truly can't put a dollar value on Darktrace."
>
> Qadir Nawaz, Director of Infrastructure and Technical Services, King's Hawaiian

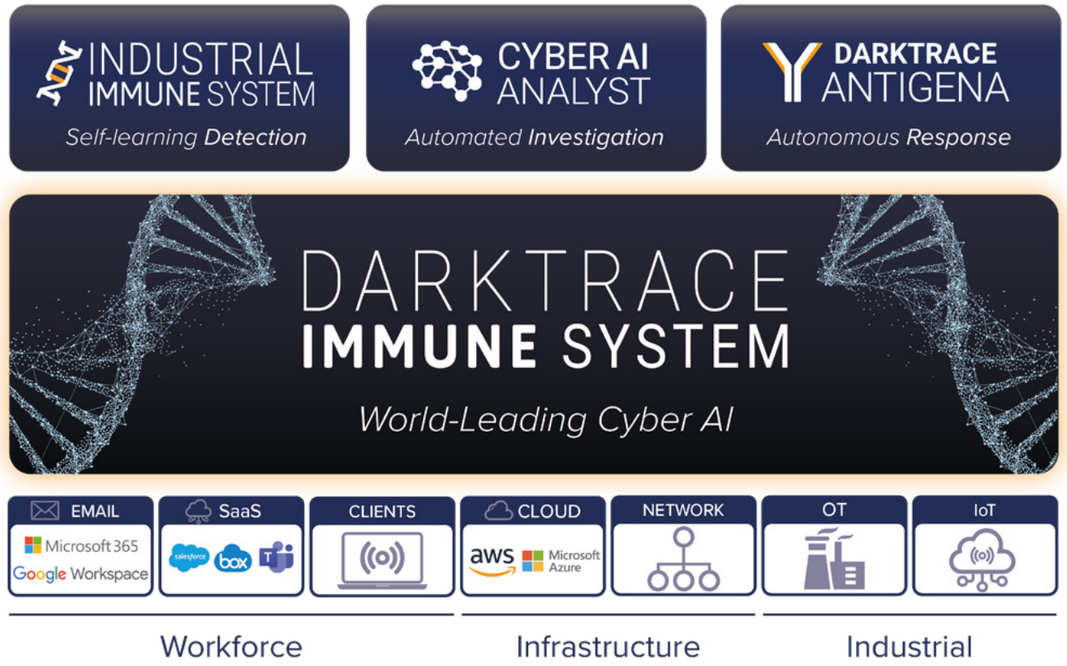
> "Darktrace is fundamentally changing the game of ICS cyber defense."
>
> Michael Sherwood, CIO, City of Las Vegas

Darktrace Immune System Platform

By learning normal patterns and discovering novel threats, the Industrial Immune System represents a core capability of a broader self-learning platform. The product not only interfaces with Cyber AI Analyst to enable autonomous investigations, but also feeds an adaptive Autonomous Response framework via Darktrace Antigena. With Antigena, the platform can respond to self-learning detections and neutralize emerging attacks with dynamic and surgical precision. All three capabilities are grounded in our fundamental Self-Learning AI technology and can be seamlessly extended to protect industrial environments, cyber-physical systems, and email platforms.

Darktrace Proof of Value

Darktrace's Proof of Value (POV) allows organizations to experience first-hand the Industrial Immune System's ability to detect previously unseen threats and anomalous behaviors within their industrial environment. During the POV, Darktrace provides access to the Threat Visualizer as well as weekly, custom-made Threat Intelligence Reports.



About Darktrace

Darktrace (DARK:L), a global leader in cyber security AI, delivers world-class technology that protects over 6,500 customers worldwide from advanced threats, including ransomware and cloud and SaaS attacks. Darktrace's fundamentally different approach applies Self-Learning AI to enable machines to understand the business in order to autonomously defend it. Headquartered in Cambridge, UK, the company has 1,700 employees and over 30 offices worldwide. Darktrace was named one of TIME magazine's 'Most Influential Companies' for 2021.

For More Information

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