Darktrace/OT

DARKTRACE

Key Benefits:

- Passively learns 'self' in real time, no configuration needed
- Complete visibility across OT, IT, and IIoT
- Protocol and technology agnostic
- Cyber AI Analyst reduces triage time by up to 92%
- Illuminates points of IT/OT convergence
- Identifies assets with a passive and active option

Powered by scalable, Self-Learning AI, Darktrace/OT detects unpredictable attacks in their earliest stages, before the damage is done.

By learning the normal 'patterns of life' for every device and operator in an industrial environment, Darktrace/OT detects known and unknown threats with the same AI-driven methods, as well as granting visibility across all levels of the Purdue model, and into and around the DMZ.

/ Limitations of the Traditional Approach

CISA confirms that "current ICS security technology focuses on reactive defense against known threats with limited capabilities to detect threats based on behavior rather than pre-defined indicators." SANS adds that many advisories for ICS devices have no practical mitigation advice, and over a fifth of reported common vulnerabilities and exposures (CVEs) do not even include a patch, making most vulnerability management workflows a process of diminishing returns.

Static baselines cannot keep pace with changes in the diverse technologies used in ICS ecosystems, where legacy devices are often retrofitted and used alongside IIoT. Siloed security solutions also fail to detect attacks that span the entire organization—for example, malware that enters through a phishing email and then moves laterally, eventually disrupting visibility into OT.

/ Defending Diverse Industrial Environments

By analyzing all traffic and activity on a granular level in a protocol and technology agnostic capacity, Darktrace provides continuous detection, full visibility, actionable insights, and, where appropriate, Autonomous Response for diverse and complex ICS ecosystems. Rather than forming static baselines that need constant tuning and manual configuration, Darktrace harnesses Self-Learning AI to continuously learn 'normal' for all forms of machine and human behavior, identifying deviations indicative of an emerging attack.

Darktrace/OT can be configured to defend all the way down to Level 1 devices in the Purdue model and indirectly into Level 0. It also covers all higher Purdue levels, from supervisory functions, business logistics, and enterprise networks (Level 4&5), and beyond into cloud and SaaS. The technology also provides visibility into and around the DMZ.

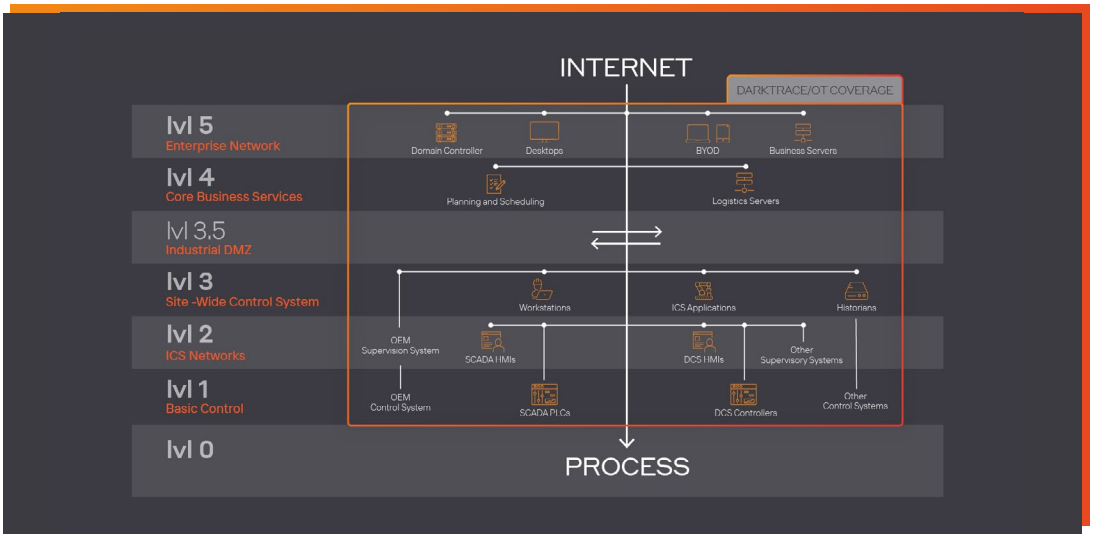


Figure 1: Darktrace coverage directly covers all levels of the Purdue Model and indirectly into level 0

/ Self-Learning AI

Rather than relying on pre-defined indicators of compromise (IoCs) and external threat feeds, Darktrace analyzes an ICS ecosystem's native data through layers of machine learning to detect any unusual behavior, regardless of whether the source is human or machine. This self-learning approach allows Darktrace to detect known and unknown attacks in the same capacity including, but not limited to: zero-day exploits, supply chain attacks, insider threats, ransomware, and devices infected prior to deployment.

/ Adapts to Evolving Environments

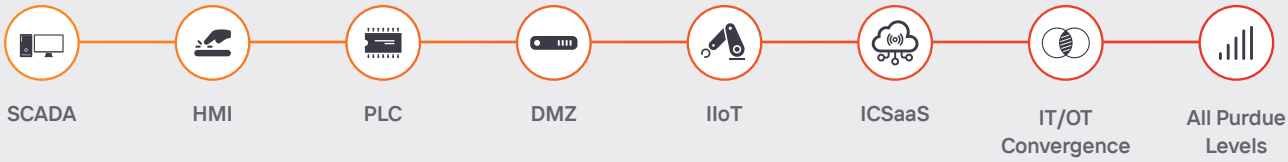
As legacy devices are retrofitted, technologies such as IIoT are being adopted, and remote working is becoming an increasing practice for industrial environments, ICS ecosystems are evolving. Darktrace's Self-Learning AI takes an adaptive approach, with its native ability to learn these changes 'on the job' without human input, removing the need for manual configuration and constant tuning.

/ Comprehensive Visibility

Being protocol and technology agnostic, Darktrace does not need to access specific protocols to perform its threat detection, allowing the AI to identify abnormal activity no matter where it occurs in the digital ecosystem.

At the same time, Darktrace can read into over 50 diverse industrial protocols, including Modbus, IEX-61950, CIP and BACnet.

This allows the technology to grant visibility into a wide range of bespoke industrial environments, regardless of whether they employ decades old devices or the latest IIoT and ICSaaS technologies.



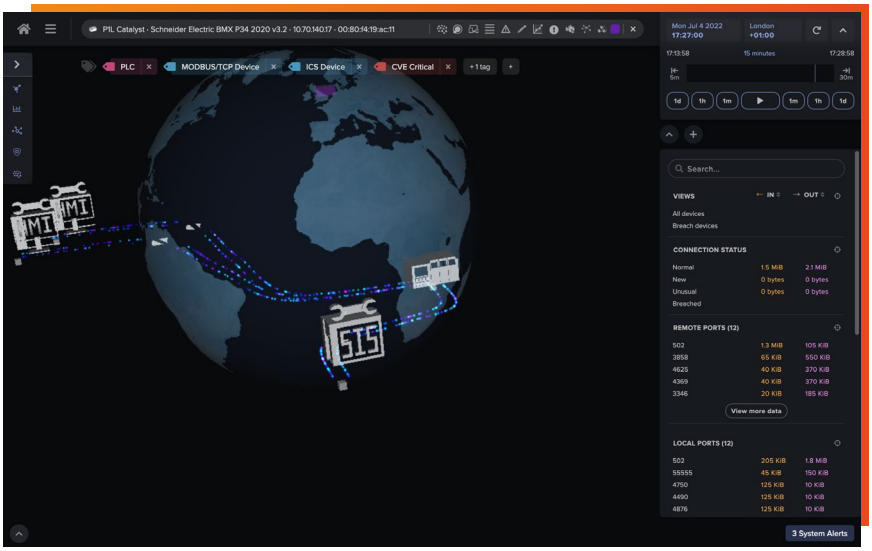


Figure 2: Darktrace/OT detecting anomalous connections to a SCADA ICS workstation

/ Cyber AI Analyst: Augmenting the Human

The barrier to attacking industrial environments is lowering as threat actors expand from nation states to cyber-criminals, as seen with the Colonial Pipeline incident. OT security teams simultaneously are suffering from a skills shortage and tight budgets, remaining perpetually understaffed.

Cyber AI Analyst augments security and operation teams, providing actionable insights and closing knowledge gaps between IT and OT specialists. Autonomously investigating all unusual activity across the whole ecosystem, Cyber AI Analyst connects the dots among disparate events, reducing triage time by up to 92%.

With specialized models for OT, Cyber AI Analyst rapidly cycles through the process of building hypotheses, querying real-time data, and refining its theories. This creates fleshed out Incident Reports that put teams in a position to immediately take action, allowing them to better maintain availability and integrity as an attack emerges.

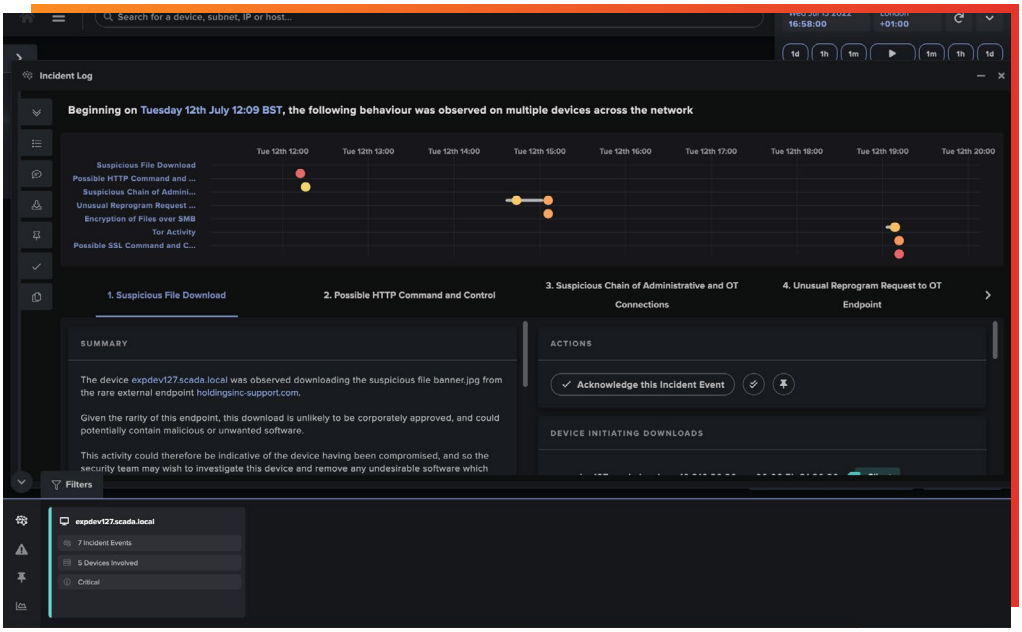


Figure 3: Darktrace's Cyber AI Analyst detecting anomalous encryption an a suspicious chain of ICS administrative credentials

> Darktrace adds another level of sophistication to our defense systems and has already identified threats with the potential to disrupt our networks. It helps us stay ahead of emerging threats and better defend our key systems.
>
> / Group Head of Security, Drax

> Using machine learning, Darktrace detects zero-day threats and suspicious insider behaviors, without having to define the activity in advance.
>
> / Chief Innovation Officer and Director of Technology, City of Las Vegas

/ Capabilities for OT/ICS Specialists

OT Engineer and OT Explore

OT Engineer provides an operations-focused dashboard for control engineers. This includes a subset of alerts with high operational relevance that are suitable for those with typical controls engineer domain knowledge. This feature grants access to immediate information on emerging threats for fast triage, with the aim of minimal interface time. Further, drawing on Darktrace's native ability to evolve alongside changes in the ecosystem, no tuning is necessary.

OT Explore enables a top-down visualization of the OT environment. This provides a time-bounded snapshot of connectivity and also allows users to drill down into the subnet and device level. This can surface unexpected relationships through tags, such as clusters of similar devices not associated prior to exploration.

Passive Asset ID, Active Option

Darktrace's ability to passively identify assets eliminates the risk of operational disruption. Based on the behavior of devices, Darktrace autonomously catalogues IP-connected and non-IP ICS devices. This allows Darktrace/OT to create a profile and full history of all devices seen on network. This device data is fully searchable with Advanced Search, Elastic Search, API, and OT threat detection models.

Additionally, Darktrace provides an active identification module to be used where desired. The active identification module makes requests to known OT devices to identify them using their observed and current protocol and service port combination.

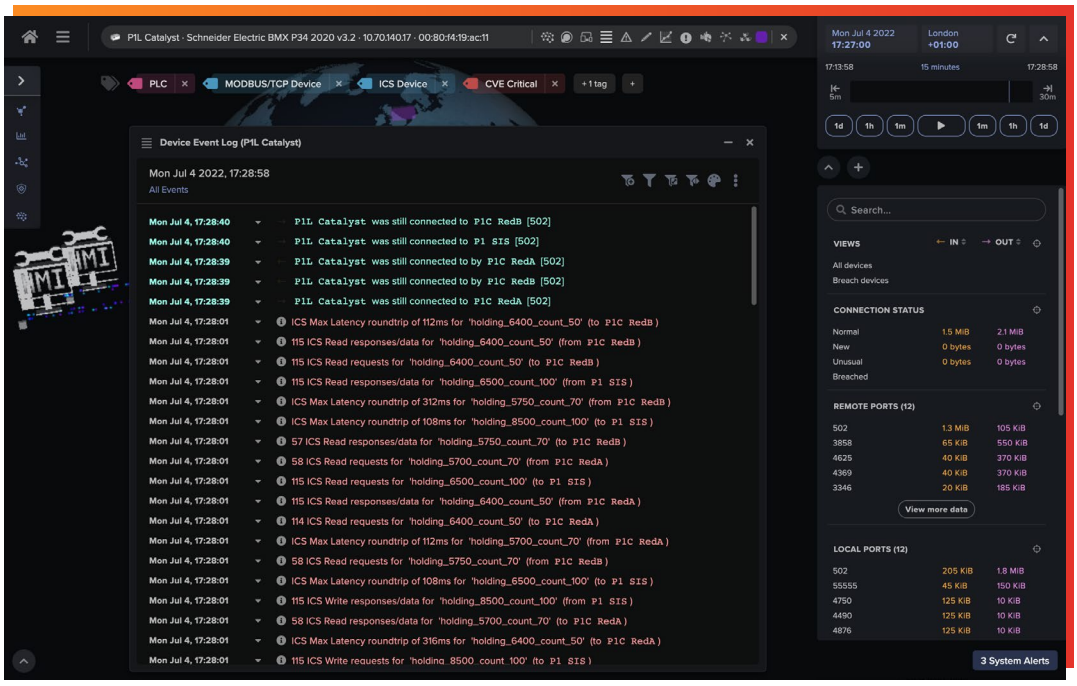


Figure 4: OT Explore provides a top-down visualization of the industrial environment and a time-bounded snapshot of network connectivity.

> Darktrace never keeps you in the dark where threat actors are concerned. This product is awesome and provides exactly what we need to secure and protect our assets.
>
> / Group Head of Security, Drax

/ Illuminating IT/OT Convergence

With the ability to provide a unified view across IT and OT environments, Darktrace is uniquely positioned to highlight any points of IT/OT convergence. In an anonymized study of its client base, Darktrace detected over 6,500 suspected instances of ICS protocol use across 1,000 enterprise environments. The ICS protocol which was detected most in this review was BACNet, seen in approximately 75% of instances. Illuminating these points of convergence is a critical step in preventing attacks from pivoting from virtual infections to disrupting physical processes.

/ Complementing OEM Solutions

Protecting machinery from Original Equipment Manufacturers (OEM) involves a number of challenges, including legacy hardware and software, proprietary protocols, and poorly documented security configurations. With its flexible platform approach, Darktrace easily overcomes these challenges.

When network traffic is not available, for instance, Darktrace can provide coverage at a higher Purdue level, defending traffic into and out of the OEM ICS Network. Darktrace can also ingest log output from OEM security solutions to perform AI analysis. Further, if an OEM is using proprietary protocols, Darktrace can build a 'pattern of life' based on the metadata.

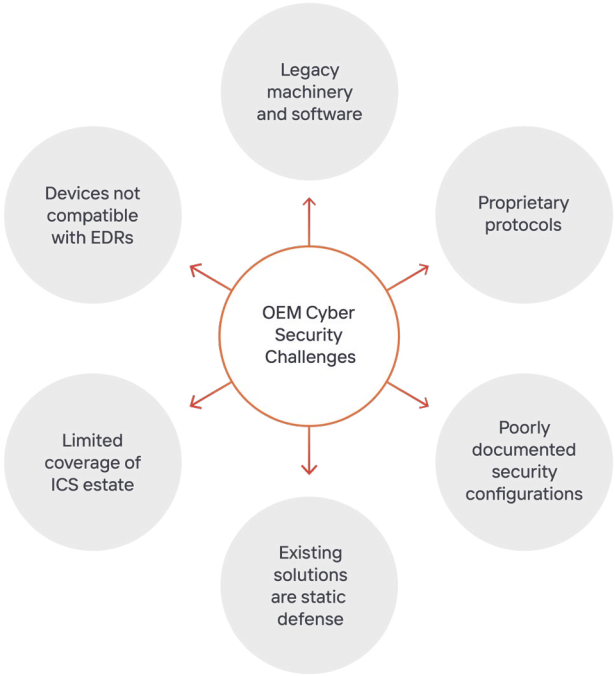


Figure 5: Challenges faced by the cyber security community with OEM networks and devices

> We had connections between our IT and OT environments that we didn't know existed. Darktrace gives us that crucial visibility of both the OT and IT on a single screen.
>
> / Head of Telecommunications and Information Systems, Copperbelt Energy Corporation Plc

> Darktrace's machine-based learning product does all the SOC heavy lifting, filtering out only the most important events. During side-to-side testing with another vendor, Darktrace consistently found potential concerns, where the comparable product missed the same event."
>
> / CIO, Energy and Utilities

/ Defending Against Industrial Ransomware

At an integrated oil refiner and supplier, Darktrace/OT stopped a ransomware attack that originated in the corporate network. Self-Learning AI identified the first signs of a ransomware infection in a desktop device. In addition to writing its own ransom note files, the device made a series of connections to rare external destinations via an internal proxy server and then downloaded potentially malicious files.

The device proceeded to make a number of SMB directory queries. Darktrace/OT instantly detected this activity and highlighted it as likely ransomware, alerting the security team before the infection was able to spread into the OT environment.

/ Protecting Industrial IoT

The mass adoption of IIoT devices has made industrial environments more complex and more vulnerable than ever. Darktrace recently detected a series of pre-existing infections in Industrial IoT (IIoT) devices at a manufacturing firm in the EMEA region.

Self-Learning AI recognized a device exploiting the SMBv1 protocol in order to attempt lateral movement. Darktrace also detected the device abusing default vendor credentials for device enumeration. The device made a large number of unusual connections, including connections to internal endpoints of which the company had previously been unaware. As these occurred, Darktrace illuminated the unusual activity's spread from the infected device across the infrastructure.

In total, Darktrace identified 13 infected production devices. This 'unknown known' threat was detected without any prior knowledge of the devices, their supplier, or patch history, and without using malware signatures or IoCs.

By casting light on this previously unknown threat, Darktrace enabled the customer to perform full incident response and threat investigation before the attack caused any serious damage to the company.

/ Detecting Novel and Never-Before-Seen Attacks

The SolarWinds attack revealed the vulnerability of ICS to exploiting SNMP communications in Building Management Systems (BMS). Without a list of known exploits, company assets, or firmware versions, Darktrace/OT detected every stage of a state-of-the-art attack at an international airport targeting their BMS.

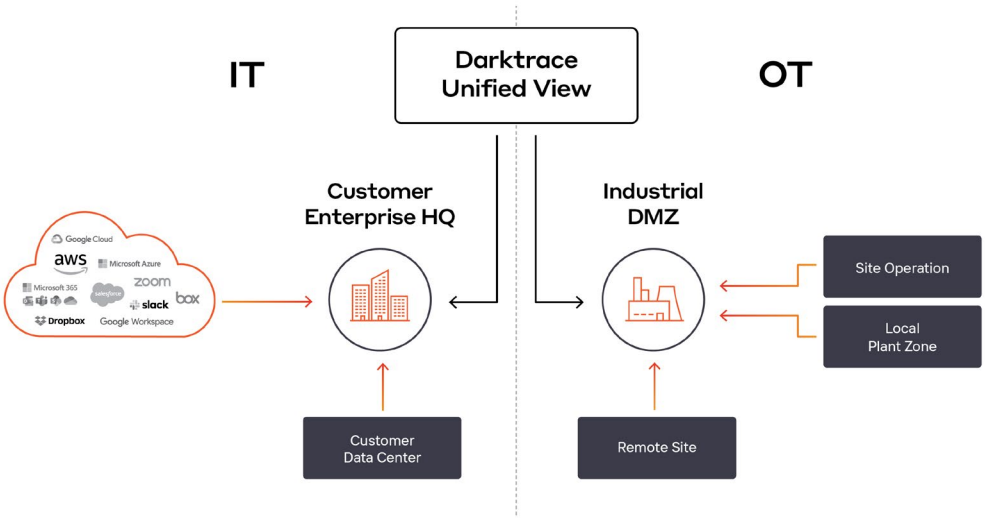
The attack spanned multiple days and targeted not only the BMS but also the baggage reclaim network, with the attackers utilizing two common ICS protocols, BacNet and S7Comm. The attackers also leveraged legitimate tools in order to evade traditional, signature-based security.

Legacy security tools failed to identify the unusual activity. However, Darktrace was able to identify unusual commands used by the attacker within those otherwise 'normal' connections. On top of this, Darktrace's Cyber AI Analyst was able to perform a real-time automated investigation and recommend steps that put the security team in a position to immediately take action.

> Cyber AI can detect cyber-threats before damage is done, whether they arise from an employee or from the industrial systems on our production floor. You need AI in place to quickly identify and respond to threats.
>
> / Director of Infrastructure and Technical Services, King's Hawaiian

/ Unified View

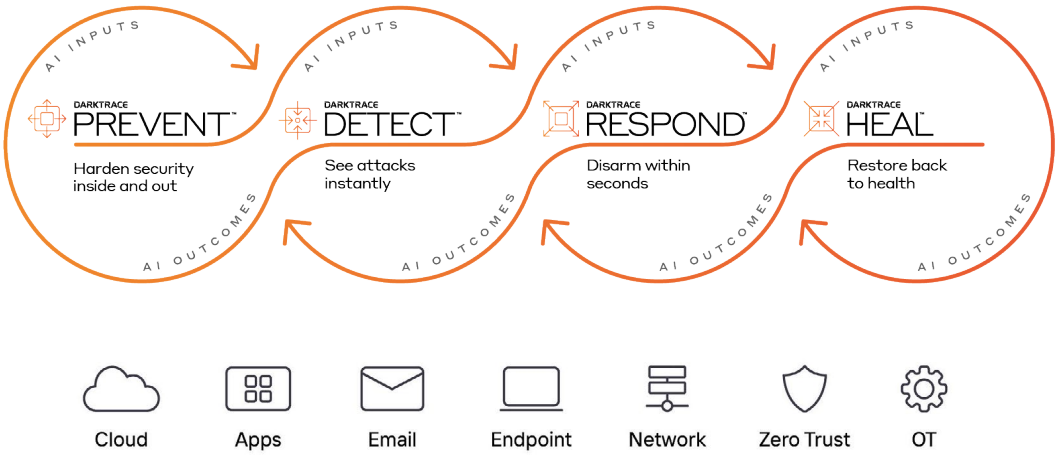
Darktrace/OT provides a unified view across IT and OT systems. In today's threat landscape, where many attacks target OT infrastructure after first pivoting through IT environments, this unified view has become an invaluable tool for detecting and neutralizing threats before the damage is done.



/ Cyber AI Loop™

Darktrace is delivering the first ever always-on feedback system that creates a virtuous cycle in which each capability strengthens and hardens the entire security ecosystem. Darktrace/OT fits into the DETECT and RESPOND components of this ecosystem, sharing its insights with the rest of the security stack – and human teams through Explainable AI.

Cyber AI Loop™



darktrace.com
info@darktrace.com

Scan to LEARN MORE