DARKTRACE
INDUSTRIAL

What Darktrace Industrial Finds

Darktrace Industrial defends some of the most complex industrial control systems in the world against novel and sophisticated cyber-campaigns. Darktrace Industrial's world-leading cyber AI technology has been specifically developed to detect cyber-threats and latent vulnerabilities across both Operational Technology (OT) environments, such as SCADA systems, and IT networks.

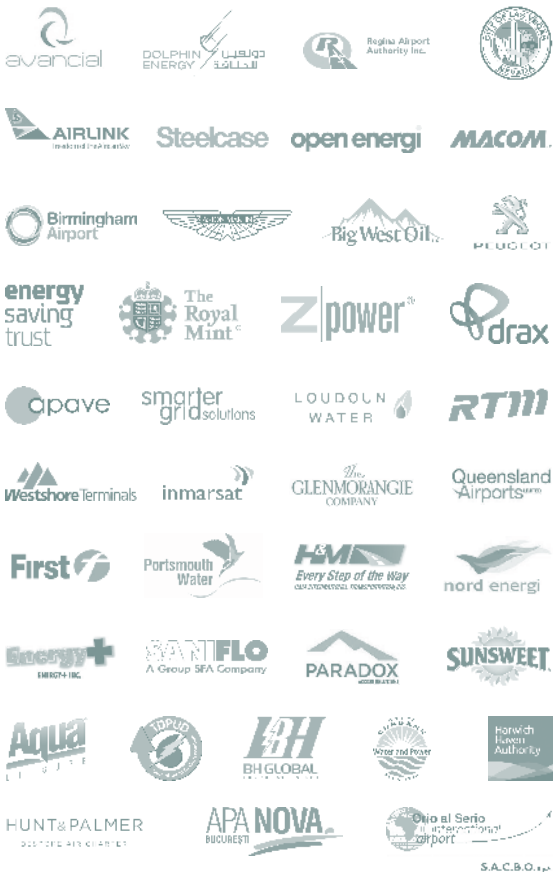
Modeled on the principles of the human immune system, Darktrace Industrial learns the 'pattern of life' of every user, device, and controller, and uses that constantly evolving understanding to detect the earliest signs of an emerging threat. Darktrace Industrial also provides unprecedented visibility across both your industrial and enterprise networks, allowing your security team to gain oversight of the entire distributed infrastructure.

This document features case studies of alerts raised in real industrial networks where Darktrace Industrial was deployed.

Powered by unsupervised machine learning and AI, Darktrace Industrial autonomously learns 'normal' behaviors and can then identify genuine cyber-threats at a very early stage, before they develop into a crisis and cause material harm. This 'immune system' approach is capable of detecting all forms of potentially threatening behavior, including malicious attacks, accidental errors, and malfunction. This allows for a far more comprehensive and risk-based approach to security monitoring than traditional signature tools, which are rigidly programmed to catch only known threats.

Rather than producing a flood of alerts, Darktrace Industrial only surfaces genuine incidents. Threats are scored and ranked by their level of severity, empowering security teams to investigate critical issues, respond rapidly to all forms of threats, and make their systems far more resilient in the long term.

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



Potential Threats

Each example below features a description of the alert and the outcome of the specific investigation. One of the key tasks facing security teams is to quickly examine the immediate context around an alert and eliminate the worst-case scenarios. Darktrace Industrial's powerful and intuitive interface – the Threat Visualizer – enables unprecedented visibility and allows these determinations.

Administrative Activity

of threats detected involve reprogramming, reconfiguration or use of a common administrative tool

- Very rare use within existing control system connections of unrecognized command code sent to PLCs. Proved to be undocumented functionality forming part of vendor-supplied system.
- Unusual RDP connection made from engineering workstation to OT data protection management server, with significant data volume downloaded. Proved to be an unusual access method for an authorized task normally performed locally by the same user.
- Workstation sending logs to a log server makes unusual, direct SQL access connection to it. Proved to be authorized, if unusual, user administration.

Internal Reconnaissance

of alerts reported by Darktrace analysts suggest internal reconnaissance on devices and software

- New device appears on network and broadcasts requests for PLCs to identify themselves. Proved to be an unused cabled second communications module on existing PLC.
- Unusual broadcast behavior of a group of devices. Proved to be an exchange of identity information conducted purely through clear-text broadcasts.
- HMI in production network conducts port scan for the first time. Proved to be triggered by user in breach of policy, such scans against OT devices carry a great deal of risk. Also revealed a surprising amount of success opening connections past firewalls supposed to be preventing them.

New Connectivity

of cyber incidents detected are related to brand new or very rare connection attempts

- Two new failed connections are made between OT devices that do not normally connect, followed by a change in commands sent to PLC in same subnet. Proved to be authorized control system changes taking place.
- New OT protocol connections made between previously inactive devices. Proved to be new part of control system in development long after the new devices were installed.

Malfunction

of threats are malfunctions involving spontaneous connectivity changes and failures

- Sudden drop of multiple connections to a PLC which were otherwise continuous, followed by ten minutes of failed attempts to re-establish them. Proved to be device malfunction corrected by engineers.
- Daily connection from OT workstation to AV update server changes from connecting to failing. Proved to be unintentionally blocked by an authorized firewall change.

> Darktrace's 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**

Incoming Connections From Enterprise

of alerts are triggered by incoming connections to the OT network from elsewhere in the organization

- Failed connection attempt made from enterprise network using dedicated OT protocol. Proved to be accidental trigger of a configuration being tested for intended OT/IT data exchange.
- Unusual SSH connection made from enterprise client to OT application server. Proved to be an authorized administrative user from an unusual source (and a breach of policy).
- Unusual proprietary traffic seen to high port on OT application server. Proved to be authorized deployment of new application connection.

Outbound Connections To Enterprise

of alerts are triggered by outgoing connections from the OT network to elsewhere in the organization

- AV server in OT network begins making new, failing SMB connections towards a server in the enterprise network. Proved to be a software misconfiguration.
- OT device (HMI) makes new, sporadic, failing attempts to contact corporate network over Microsoft Windows protocols. Proved to be misconfiguration that risked radically altering the HMI.
- Workstation behaving unusually compared to otherwise-similar peer devices, making repeated DNS requests that were relayed to enterprise DNS servers. Proved to be a misconfiguration made by the system administrator.

> Darktrace adds another level of sophistication to our defense systems.
>
> **Martin Sloan, Global Head of Security, Drax**

> Darktrace is an effective tool for real-time advanced threat detection.
>
> **Earl Perkins of Gartner, Cool Vendors in Energy and Utilities**

Internet Downloads

of potential threats involve data being downloaded from the public Internet into OT networks

- OT workstation downloaded browser toolbar from rare internet destination. Proved to be user breaching policy, but also that a non-reverted test change had allowed the web proxy to be bypassed.
- An OT device begins attempting to locate a web proxy server. Proved to be a software misconfiguration, which could have resulted in further unauthorized changes to the device.
- Engineering workstation downloads executable from rare internet destination. Proved to be deliberate acquisition of an unauthorized third-party software tool.

Internet Uploads

of potential threats involve data being sent from OT networks out to the public Internet

- Unusual upload to cloud storage provider from engineering subnet. Proved to be a contractor working around a failed proxy server to complete their assigned task.
- Workstation made regular failed connections to an internet destination (foreign Data Centre IP address), unusual compared to its peers. Proved to be a software configuration error not made on peer devices.
- Very large amount of data uploaded by an OT device to its vendor. Proved to be an expected upload as part of the device's function, though this had not been raised to the security team.

Threat Domain

Over time, almost all organizations are converging their OT and IT networks and security responsibilities. There are many factors driving this, from the financial benefits of exchanging data in real-time between production and logistics, to the increased threats to OT systems with IT origins and the skills needed to combat them.

Even where this convergence is slower, OT-focused security teams cannot afford to ignore them. Many parts of control systems are based on IT systems, such as Windows servers and HMIs, engineering workstations, SQL databases, and SMB file shares. The few publicly disclosed major OT threats in recent years have all leveraged IT in order to reach control systems and have also shown that any compromised device that can communicate with the core control system can likely disrupt production. While Darktrace Industrial will highlight unusual activity involving OT protocols between production devices, the majority of potential threats it highlights represent earlier stages of a possible kill chain, and give the security team the ability to investigate and remediate them before key systems are in danger.

OT Vendors & Protocols

Darktrace Industrial's fundamental approach to detecting threats works across all network traffic, including all OT vendor devices and all OT-specific protocols, as it does for all other device types and protocols including IT and IoT.

This is crucial not just in older networks filled with many proprietary or custom protocols, but also in new networks comprising encrypted local connections and IoT devices. Industrial environments are typically highly non-standard and unique, and consequently Darktrace Industrial's detection methodology does not assume or require any specific knowledge of the systems or protocols in use in a given network.

Darktrace Industrial does not rely on having access to Deep Packet Inspection (DPI) of specific protocols as a starting point. Instead it leverages DPI as a bonus, where available, to improve the immediate context around alerts stemming from a particular protocol communication and decreases investigation time. It rarely adds different alerts and those it does are in low-risk areas – the core threat detection capabilities based on machine learning and behavioral modeling work on all forms of network traffic. Darktrace Industrial already performs DPI on many open protocols and others can be added on request.

> Hackers are setting their sights on critical infrastructure. Darktrace's machine learning approach fights the battle before it has begun.
>
> **Michael Sherwood, CIO,**
> **City of Las Vegas**

About Darktrace Industrial

Darktrace is the world's leading cyber AI company and the creator of Autonomous Response technology. Its self-learning AI is modeled on the human immune system and used by over 3,000 organizations to protect against threats to the cloud, email, IoT, networks and industrial systems.

The company has over 900 employees and headquarters in San Francisco and Cambridge, UK. Every 3 seconds, Darktrace AI fights back against a cyber-threat, preventing it from causing damage.

Contact Us

North America: +1 (415) 229 9100
Europe: +44 (0) 1223 394 100
Asia-Pacific: +65 6804 5010
Latin America: +55 11 97242 2011
info@darktraceindustrial.com
darktraceindustrial.com