INDUSTRY SPOTLIGHT: MANUFACTURING

DARKTRACE

AT A GLANCE:

- Protocol and technology agnostic, with no fixed baselines
- Unified coverage across IT, OT, and IoT
- Detects novel threats in real time as they emerge
- Understands all communication across an environment, from regular PLC traffic, to distributed IIoT sensor grids

With threats to the manufacturing industry growing more sophisticated and supply chains under greater pressure than ever before, a unified approach to security across both IT and OT environments is vital for detecting new threats and vulnerabilities.

/ Ransomware on the Rise: Facing up to Computer-Speed Cyber-Attacks

The manufacturing industry is prey not only to typical cyber-attacks from financially-motivated threat-actors, but also to nation-states, hacktivists, and competitors looking to carry out industrial espionage and seek an advantage. The world saw a 300% increase in cyber-attacks on this sector in 2021, with these attacks getting more sophisticated and hard-to-detect and threat actors develop new tactics and techniques.

Many manufacturing organizations still rely on decades-old bespoke OT systems that were designed without security in mind. Traditionally, decisionmakers in this industry have emphasized performance and physical safety over security, but as OT and IT converge, these concepts are becoming more intertwined.

With cyber-attacks that start in the IT layer increasingly spilling over into industrial systems on the factory floor, the need for a unified system that protects both IT and OT has become more and more evident. The EKANS ransomware strain that disrupted manufacturing facilities around the world in 2020 resulted in a dramatic decline in production and incurred huge costs. This attack directly targeted ICS vulnerabilities, with the ability to attack 64 specific ICS mechanisms in its kill chain.

The growing complexity of manufacturing systems has resulted in extremely bespoke and specialized network infrastructures, and in many cases the systems are being operated and managed by manufacturing specialists rather than the IT function.

As the scale of attacks continues to increase, security teams are becoming more stretched and a skills gap is developing between IT staff and OT engineers. Today's manufacturing organizations need a technology that can illuminate cyber-threats across the entire business, uplifts security teams and bridges that skills gap, providing actionable insights to help remediate the most pressing security incidents.

> Darktrace is a game changer because it takes people from watching a monitor to really starting to work through the trade craft, and reduces the time it takes to triage issues.
>
> / CIO, AmSty

/ Darktrace's Self-Learning AI

Darktrace AI protects the critical and complex cyber-physical ecosystems of hundreds of manufacturers around the globe. Protocol and technology agnostic, the AI detects in-progress attacks across the digital business, instantly alerting security teams to nascent threats.

Darktrace passively learns what 'normal' looks like across connected cyber-physical devices, operational technology, users, and IT systems, and all the interactions between them. By learning 'on the job', Darktrace does not require additional training, added data sets, or tuning; instead, it identifies the subtle signals of emerging attack in real time – no matter how novel or sophisticated the threat.

> Machine learning can detect things that we can't predict and define. It's like finding a needle in an enormous haystack.
>
> / Information Security Architect, Steelcase

With Autonomous Response, Darktrace goes a step further by taking targeted action in real-time to contain an in-progress attack. Because it understands 'normal' for every user and device, the technology knows the precise action to take to contain the threat, without disrupting normal operations. It can be configured to only act on certain devices, with or without human confirmation.

Meanwhile, Darktrace's Cyber AI Analyst autonomously investigates in the background, generating a natural language summary of the incident, reducing time to triage by up to 92% – augmenting human teams and helping to bridge the skills gap between OT and IT with clear, actionable insights.

/ Case Study: IP Targeted by Advanced Malware

At a European medical manufacturing firm, an administrative assistant received a targeted phishing email in relation to payments with an invoice attached. Believing the attachment to be authentic, they clicked on it and unwittingly downloaded a fast-acting malware that had bypassed all other security controls.

The sophisticated malware was specifically targeting the organization's intellectual property, which included highly confidential medical formulas. Should these assets have been compromised, the firm would have experienced significant damage to their competitiveness and reputation.

Once the malware was downloaded, the device rapidly began connecting to a rare external destination while trying to move laterally to other environments. Within two seconds, Darktrace's AI identified the emerging threat and raised a clear alert to the security team, who were able to take the device offline before the malware could spread.

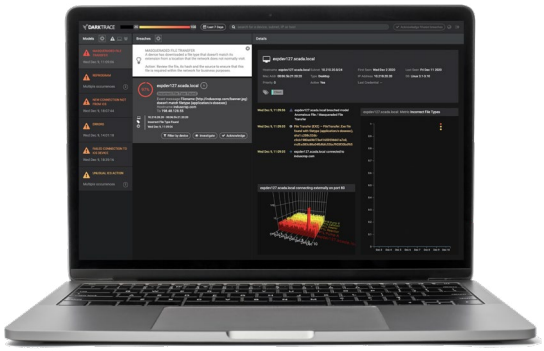

Figure 1: Darktrace's OT Engineer Dashboard surfaces only the most operationally relevant alerts

About Darktrace

Darktrace (DARK.L), a global leader in cyber security AI, delivers complete AI-powered solutions in its mission to free the world of cyber disruption. We protect more than 7,400 customers from the world's most complex threats, including ransomware, cloud, and SaaS attacks. Darktrace is delivering the first-ever Cyber AI Loop, fueling a continuous security capability that can autonomously spot and respond to novel in-progress threats within seconds. Darktrace was named one of TIME magazine's "Most Influential Companies" in 2021.

To learn more, visit darktrace.com

Scan to LEARN MORE