2021 Industry Spotlight: Manufacturing

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.

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

A New Era of OT Cyber-Attacks

In June 2020, a sophisticated, novel strain of ransomware called EKANS hit several Honda manufacturing facilities around the world. It caused an outage which ground operations in numerous countries to a standstill and resulted in a dramatic loss in production hours and employee salaries, as well as the costs of getting systems up and running without giving in to ransom demands.

What was different about EKANS was that the attack directly targeted ICS vulnerabilities, rather than pivoting through unpatched IT software as a gateway. With the ability to attack 64 specific ICS mechanisms in its kill chain, this strain of ransomware represents a new frontier in the future of OT cyber-attacks.

Further, at a time when there has never been more pressure on manufacturers to meet global demand and maintain the supply chains that connect international commerce, prioritizing the security of OT technology is critical. In the spring of 2020, many manufacturers found themselves suddenly pivoting to produce goods they had never made before in light of the pandemic, overhauling their production lines and implementing new technologies - and many of these transformations look set to remain in place for the long-term.

> "Ten years ago, cyber security was just a firewall. Today, with 5G and remote working, companies are more open to threats. That's where Darktrace comes in."
>
> Frédéric Carricaburu, CIO, Saniflo

> "The Darktrace Cyber AI Analyst is a game changer because it takes people from watching a monitor to really starting to work through the trade craft and reduce the time it takes to triage issues."
>
> Laura Tibodeau, CIO, AmSty

How Cyber AI Protects the Manufacturing Sector

Darktrace's Industrial Immune System leverages AI technology to protect 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.

Modeled on the human body's own immune system, 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.

Once an incident is flagged to security teams, Darktrace's Cyber AI Analyst autonomously triages, interprets, and reports on the in-progress attack. It produces a natural language summary of the event which takes an average of three minutes to read and is able to be reviewed even by a non-technical responder. Cyber AI Analyst reduces time to triage by up to 92% - augmenting human teams and helping to bridge the skills gap between OT and IT.

IP Targeted by Advanced Malware - Medical Manufacturing

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.

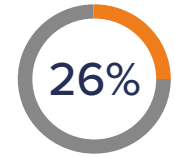
The sophisticated malware was specifically targeting the organization's intellectual property, which included highly confidential medical formulas. Should these assets have been compromised, the firm would have experienced significant damage to their competitiveness and reputation.

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 Cyber AI identified the emerging threat and flagged it to the security team.

> "Machine learning can detect things that we can't predict and define. It's like finding a needle in an enormous haystack."

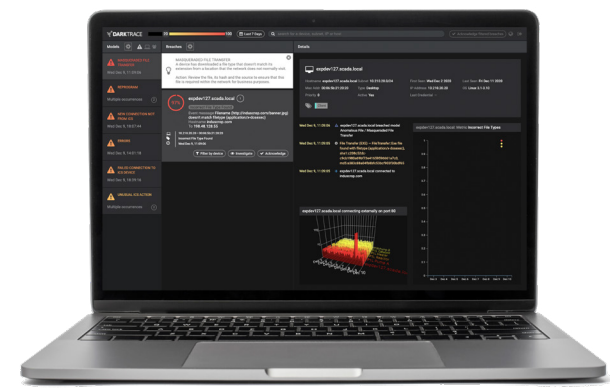
Stuart Berman, Information Security Architect, Steelcase

Threats by Numbers



of companies do not have any division overseeing security at factory management systems.

Darktrace detected over 6,500 suspected incidents of ICS protocol use across 1,000 environments in IT networks in Summer 2020.



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