DARKTRACE

2020 Industry Spotlight: Manufacturing

With threats to OT environments growing ever-more sophisticated and supply chains under greater pressure than ever before, a unified approach to security across both IT and OT environments has never been more important.

Darktrace Key Benefits

- ✓ 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

2020: A New Era of OT Attacks

In June 2020, a sophisticated, novel strain of ransomware — 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 targets 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, EKANS 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 global 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, 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**

However, these dramatic shifts are risks in themselves. Many systems within an organization's digital and physical supply chain are often older and incompatible with more modern tools and technologies, creating widening vulnerabilities and insecure digital environments. These are in turn being exploited by cyber criminals, who are waging attacks with increasingly tailored and sophisticated methods of exploitation.

The advent of ubiquitous remote work further complicates the security of cyber-physical environments in factories, manufacturing plants, and similar facilities. With hybrid models of working and remote employees shifting to third-party cloud and SaaS applications, security teams are inundated with incidents from both internal employee activity and external threats they encounter every day.

A new era of OT attacks is here, and will only continue to evolve. Cyber-criminals will continue to exploit digital and cyber-physical vulnerabilities, and organizations need a security approach that detects and responds to threats seamlessly across OT and IT environments.

Read more about the EKANS ransomware attack here!

An Immune System for the Manufacturing Industry

The Darktrace Industrial Immune System leverages AI technology to protect the critical and complex cyber-physical environments of hundreds of manufacturers around the globe. Darktrace's Immune System technology scales to cover disparate connected machines, configurations and environments. Using both unsupervised and supervised machine learning, Darktrace AI is not confined to any particular digital format, rather it self-learns at speed and scale.

Modeled on the human body's own immune system, Darktrace's Industrial Immune System learns how connected cyber-physical devices and operational technology, as well as users and IT systems operate and interact across a vast cyber-physical digital infrastructure.

Darktrace AI develops a 'pattern of life' while ingesting digital information 'on the job' – meaning it requires no additional training or added data sets. Thus, Darktrace is able to immediately discern threatening activity wherever and whenever it arises, from the factory floor, to an employee inbox, in real time.

Manufacturing Security Measured

7 Between January and April of 2020, cyberattacks targeting manufacturers increased **sevenfold.**

$ Financial losses caused by data breaches increased 270% on the year in January-March to **$8.4 billion.**

26% **26%** of companies do not have any division overseeing security at factory management systems.

Darktrace detected over **6,500 suspected instances** of ICS protocol use across 1,000 environments in IT networks across its customer network in Summer 2020.

Threat Story: 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, she 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 be exposed to significant risk 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 AI identified the emerging foreign presence.

Darktrace Antigena instantly neutralized the infected device by restricting its activity to fall within its normal 'pattern of life', preventing the spread of the malware and buying back time for the organization to take the infected device off the network.

> "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**

> "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**

For more information

Book a demo now

Immune System Approach

Hear from our customers

Follow us on Twitter

Follow us on LinkedIn

About Darktrace

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 4,000 organizations to protect against threats to the cloud, email, IoT, networks and industrial systems.

The company has over 1,300 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.