DARKTRACE
INDUSTRIAL

INDUSTRY SPOTLIGHT

Cyber Defense for Manufacturing

Recent cyber-attacks against manufacturing companies have highlighted the growing threats to this industry. From automated shop floors, to connected supply chains, the modern manufacturing plant benefits from a large degree of interconnectivity between OT and IT systems, allowing operations to run smoothly and enabling real-time analysis of data and processes.

> Yet the convergence of OT and IT has also expanded the attack surface and opened new inroads for sophisticated cyber-attacks and insider threats.

A pertinent example is the 2017 TRITON attack on a petrochemical manufacturer in Saudi Arabia, in which the attackers targeted the facility's safety system. Had there not been an error in the malware's code, the attackers could have caused a extensive damage by overriding the mechanism designed to prevent automated equipment exceeding safe operating conditions.

The continuing sophistication of these attacks highlights the need for manufacturers to protect their critical business operations from well-resourced cyber-criminals who launch novel threats intended to cause widespread disruption and damage.

EPIC GROUP
The GLENMORANGIE COMPANY
BH GLOBAL CORPORATION LTD
PEUGEOT
SANIFLO A Group SFA Company
MACOM
PARADOX ACCESS SOLUTIONS
SUNSWEET
The Royal Mint
SUZUKI
Aqua LEISURE
Z power
ASTON MARTIN
Steelcase

Threats by Numbers

48% of manufacturing companies have experienced a cyber security incident

According to a report commissioned by The Manufacturers' Organisation (EEF), of the 48% of manufacturers who have experienced a cyber security incident, 24% have suffered financial loss or disruption to business as a result. These figures illustrate the varying levels of maturity regarding cyber security in the manufacturing industry, and the need for companies to take action to avoid suffering a similar fate.

45% of manufacturers are not confident they are prepared for a cyber-attack

The report by the EEF also found that 45% of manufacturing companies are not confident they are prepared for a cyber-attack. The manufacturing industry faces complex and diverse cyber security challenges, which can only be addressed by implementing sophisticated cyber security defenses, capable of defending their OT, IT, and IIoT environments.

Manufacturing is the third most attacked sector

After government and finance, The Manufacturers' Organisation states that manufacturing is the third most attacked industry. Attacks focus primarily on obtaining either intellectual property or internal operating information, with cyber-criminals exploiting vulnerabilities in operating systems and industrial control systems.

Darktrace Industrial

Darktrace Industrial is the world's leading cyber AI technology for both OT and IT environments. It implements a real-time 'immune system' to defend networked devices across the entire spectrum of cyber-threat, from machine-speed ransomware to silent and stealthy cyber-campaigns that lie low in industrial control systems.

Powered by enterprise-grade artificial intelligence, Darktrace Industrial learns the 'pattern of life' for every controller and workstation on the control network, and every user and device on the corporate network, developing a rich understanding of 'self' for the entire environment. This evolving understanding of 'normal' enables Darktrace Industrial to detect the earliest indicators of an emerging threat, without relying on rules, signatures, or prior assumptions.

> Darktrace Industrial's unique self-learning technology represents a step-change in defending industrial environments, providing full coverage irrespective of the type of device.

The Industrial Immune System defends some of the most complex manufacturing plants around the world, including FMCG giants and leading pharmaceutical, chemical, and automotive companies.

By deploying software in both the control system and business network, Darktrace Industrial provides a single point of analysis, allowing security personnel to centrally monitor all network activity, from ongoing regular PLC traffic, to distributed IIoT sensor grids.

> 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**

Darktrace Industrial in Action

Compromise of Biometric Control System

At a large manufacturing company with several high priority locations, Darktrace detected a serious threat involving a fingerprint scanner. By exploiting vulnerabilities within the scanner's software, the attackers were able to access the sensitive user information held on the company's network. This information enabled the attackers to gain unauthorized access to the company's facilities and posed a huge threat to the company.

Darktrace detected this threat by identifying suspicious abnormal connections to new devices outside the network and thereby alerted the IT team before any damage was caused.

Data Storage Threatens Intellectual Property

In the network of a major European manufacturer, which stores its intellectual property in the cloud, Darktrace discovered that critical data could be accessed via a simple username and password combination without further restrictions and encryption. This meant that any sensitive information the company possessed could be retrieved by a malicious user with relative ease, by intercepting network communications.

Darktrace detected this vulnerability by finding anomalous activity within the network: the retrieval of an anomalous ZIP file from an external folder. Darktrace was able to highlight the risk to the company as soon as it occurred, meaning the sensitive IP was not leaked and the risk posed to the company's product and revenue was mitigated.

Contact Us

North America: +1 415 229 9100
Europe: +44 (0) 1223 394 100
Asia Pacific: +65 6804 5010
Latin America: +55 11 97 242 2011

info@darktraceindustrial.com
darktraceindustrial.com