2021 Industry Spotlight: Transportation

As transportation technology becomes more connected and reliant on advanced computing – so too grows the level of cyber-threat these organizations face. Self-Learning AI is a vital component of protecting critical infrastructure in today's threat landscape.

At a Glance

- ✔ Darktrace protects over 130 customers across the transportation industry globally
- ✔ Self-Learning AI detects and responds to novel and sophisticated cyber-threats
- ✔ AI provides full visibility across connected, autonomous, shared, and electrified (CASE) technologies

Innovation Expanding the Attack Surface

Recent innovation in the transportation industry has led to significant advancements across connected, autonomous, shared, and electrified (CASE) technologies. For aviation, this has meant a diverse collection of airport IoT, automated checked baggage systems, electronic passports, and user-friendly websites. For logistics companies, this has included a range of technology to support digitized solutions and services, from devices that monitor driver fatigue to warehouse robotics.

For the respective sectors within transportation, these innovations have transformed efficiency and made way for business gains and consumer ease. However, with novel innovation comes a widened and complexified threat landscape. Airlines, airports, logistics companies, and even Formula 1 racing teams have realized the need for sophisticated defense against cyber-criminals who exploit increasingly interconnected digital ecosystems.

> "Darktrace AI is the core of our whole cyber security system."
>
> CTO, OPAIN: El Dorado International Airport

Any kind of interruption, whether from user error or cyber-attacks, could be colossal for aviation, which is already a likely target for malicious attacks, highly costly for logistics providers, and dangerous for the drivers in Formula 1 racing smart vehicles.

For IoT and smart devices, security is often an afterthought to usability and functionality. As ICS and IT converge, attacks that begin on the corporate network and pivot to compromise critical physical environments will only continue to rise. This is where cutting-edge AI security comes in for hundreds of transportation organizations around the globe.

> "We rely purely on Darktrace to highlight changes in behavior that we need to be aware of."
>
> Head of IT and Technology, Birmingham Airport

Self-Learning AI Protects Global and Local Transportation

Major airports, transportation hubs, and logistics organizations around the globe rely on Darktrace's Industrial Immune System to safeguard their IT and OT environments from the full range of cyber-threats. Darktrace AI is a self-learning technology that immediately detects in-progress attacks.

Modeled on the human immune system, Darktrace works by learning what 'normal' looks like across OT, IT, and Industrial IoT. This contextual understanding enables the AI to detect subtle indicators of threat as soon as they arise, with coverage extending over the complete digital infrastructure.

Darktrace's unique Autonomous Response technology takes targeted action to contain cyber-threats in their earliest stages. This is critical in ensuring threats in IT do not pivot to OT environments, and vice versa. With growing convergence of IT and OT systems, a unified and holistic security posture is increasingly critical.

With Cyber AI Analyst, Darktrace automates the threat investigation process, stitching together disparate events across the organization to reveal the full scope of an attack. The technology automatically generates a high-level overview of the incident that even a non-technical team member can review in minutes. Critically, Darktrace Cyber AI Analyst reduces time to meaning by up to 92%.

Identifying a Sophisticated ICS Attack on a Major Airport

At the end of 2020, Darktrace detected an advanced ICS attack targeting a major international airport. The Darktrace Industrial Immune System detected every stage of this sophisticated threat.

The attack, which spanned multiple days, began when a new device was introduced to the network, using ARP spoofing to evade detection by traditional security tools. Next, the attackers managed to hijack their target device. The criminals targeted the Building Management System (BMS) and the Baggage Reclaim network by utilizing two common ICS protocols (BacNet and S7Comm) and leveraging legitimate tools to evade traditional, signature-based security defenses.

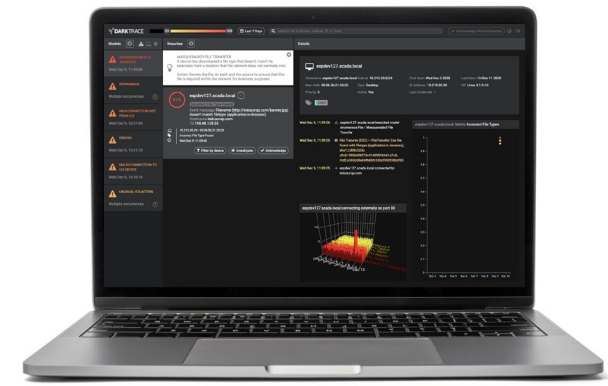
Darktrace's AI technology not only caught the attack but also launched an automated investigation into the incident. Cyber AI Analyst identified all the affected devices and produced summary reports for each, showcasing its ability to not only save crucial time for security teams but bridge the skills gap between IT teams and ICS engineers. Had the attack been allowed to continue, the attackers – potentially an activist group, terrorist organization, or organized crime group – could have caused significant operational disruption to the airport.

Threats by Numbers

of transit agencies do not have an incident response plan.

of transit agencies provide at least annual cyber security training for staff.

of transit agencies have 0 full time employees dedicated to cyber security.



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