2021 Industry Spotlight: Maritime

As the maritime industry becomes increasingly digitized and adopts new technologies, safeguarding IT and OT systems across vessels, ports, and offices is a top priority. Darktrace's Self-Learning AI provides a safe harbor for companies around the world, offering 24/7 autonomous cyber security.

At a Glance

- ✔ Self-Learning AI installs natively on ships, protecting vessels even if they lose connection
- ✔ Autonomously detects and stops cyber-attacks without interrupting business operations
- ✔ Provides security teams with high-fidelity alerts, allowing them to prioritize pressing threats

The Challenge of IT and OT Convergence

The shipping and navigation industry is exposed to a wide range of cyber-attack vectors, with businesses relying on a complex web of systems - from smart devices on remote vessels to IT systems onshore. This includes OT systems used to steer ships and load cargo, with Industrial Control Systems (ICS) involved in the engine control room and navigation lights.

To fuel efficiency, many maritime organizations have integrated their OT and IT systems. But, the sector's fast-moving digitization and robotization has exponentially increased the number of entry points for cyber-criminals. Not only does this make maritime organizations more vulnerable to threats but successful attacks can cause disruption both on land and at sea.

Yet cyber security is not only about defending data and cargo. The Vople Institute of National Transportation Systems found that "commercial merchant ships rely upon hundreds of ICS to manage propulsion, support navigation and communications, provide fire protection, operate safety systems, and manage cargo loading and discharge." As such, attacks have the potential to jeopardize human safety as well as schedules.

However, while IT and OT convergence opens the door to new risks, it also represents an opportunity to begin approaching security with a holistic mindset in which the entire digital business can be defended in a coordinated capacity – meaning threats are less likely to slip through.

Threats by Numbers

900% increase in maritime cyber-attacks since 2017.

92% of the estimated costs arising from cyber-attacks are uninsured.

74% of world trade is transported on the sea.

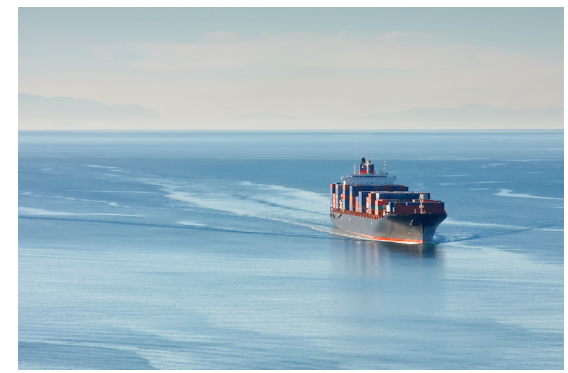

Figure 1: Self-Learning AI protects companies at all times, both onshore and offshore

Industrial Immune System: Autonomous Defense

Darktrace's Industrial Immune System leverages Self-Learning AI to safeguard OT and ICS environments, as well as Industrial IoT (IIoT) and cyber-physical systems. The Immune System can also be deployed in IT environments, including email, endpoints, cloud, SaaS, and the traditional network, providing a unified view across IT and OT infrastructure, and illuminating points of convergence.

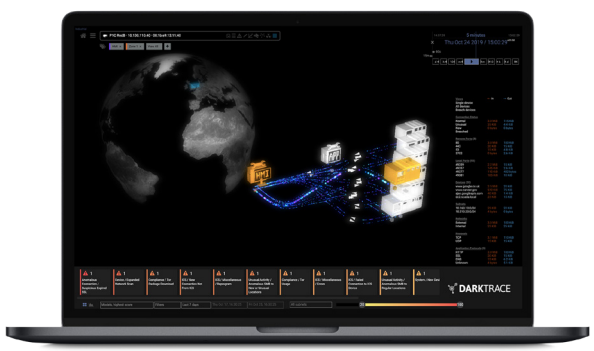

Figure 2: Darktrace's OT Engineer Dashboard surfaces only the most operationally relevant alerts and high-fidelity threats

By learning the normal 'patterns of life' for all devices and users in an organization, the Industrial Immune System detects novel and sophisticated attacks in their earliest stages. Darktrace detects both known and unknown threats before they do damage, without relying on rules, signatures, or lists of CVEs.

Powered by Self-Learning AI, Darktrace achieves this all autonomously, adapting to changes in a vessel or port's OT and IT ecosystems without the need for configuration or fine tuning. Protocol and technology agnostic, Darktrace spots threats regardless of their source or the specific technology affected — including PLCs, SCADA, HMI, IIoT, and the range of bespoke ICS employed in the maritime industry.

With Cyber AI Analyst, Darktrace automatically triages, interprets, and reports on the full scope of security incidents across OT, IT, and IoT infrastructure. Using deep learning, the technology stitches together disparate events into a digestible security narrative that can be actioned in minutes. Combining the skill of human expertise with the speed and scale of AI, Cyber AI Analyst reduces time to triage by up to 92%.

The Need for World-Leading Defenses in the Face of Disjointed Regulations

Shipping companies are faced with a range of maritime-specific regulations, including the Maritime Cyber Risk Management and the IMO guidelines, as well as guidelines from the Oil Companies International Marine Forum (OCIMF), the Baltic and International Maritime Council (BIMCO), and the Cruising Lines International Association (CLIA).

This breadth of ever-changing regulations requires a dynamic cyber security solution which can self-learn and provide real-time detection, visibility, and response across the digital ecosystem. Such capabilities are vital, not only for compliance but to defend against a new era of advanced threat.

"The maritime sector plays a pivotal role in the global supply chain. Advancing digital technologies bring economic benefits to ports but also introduce new cyber-threats."

Juhan Lepassaar, Executive Director, EU Agency for Cybersecurity

"Increased connectivity often via the internet between servers, IT systems and OT systems increases the potential cyber vulnerabilities and risks."

Guidelines on Cyber Security Onboard Ships, Baltic and International Maritime Council (BIMCO)

of organizations do not protect their vessels from OT cyber-threats.

Cyber Catalyst by Marsh

Evaluated by leading cyber insurers, Marsh has recognized that Darktrace's Enterprise Immune System and Antigena Email play a crucial role in reducing cyber-risk.

Threat Finds: Self-Learning AI in Action

Thwarting Malware in its Tracks

Darktrace recently protected a maritime transportation and storage cargo handling organization in Greenland from a fast-moving malware attack. After being infected, a device was detected making new and unusual external connections on ports 85 and 88. During the activity, the device downloaded octet files, uploaded unusual volumes of data, and used new user agents.

Darktrace identified every stage of this attack and immediately notified the organization's security team via a high-priority Proactive Threat Notification. It alerted the team when the device downloaded suspicious files and when it uploaded data to a rare endpoint. If Darktrace Antigena had been active, this malicious activity would have been blocked and neutralized in seconds.

Figure 3: Darktrace Antigena neutralizes threats at machine speed - without the need for human input

Zoom Video Conferencing Impersonation With Phishing Link

At an inland freight water transport company in the EMEA region, Self-Learning AI caught a sophisticated Zoom impersonation phishing attack. Since the start of the pandemic, users have relied on Zoom to conduct their business remotely, and Zoom emails are constantly being sent and received.

Antigena Email, Darktrace's email security solution, identified subtle anomalies that revealed the email to be a sophisticated phishing attempt. The phishing link itself used a legitimate engineering company domain to bypass secure email gateways and was hidden beneath the display text: "Preview789789789789Meeting789789789789 Details789789 789789Here".

Taking a closer look at the encoded URI, Antigena Email automatically decoded the link and identified that it led to a fake Microsoft login page.

Antigena Email held the email back from the recipient's inbox, preventing a credential compromise which could have been used to gather sensitive business data or send additional malicious emails from a corporate account.

"The power of Darktrace is amazing. It is critical that the trust port is fully operational 24 hours a day, 365 days a year, and the Industrial Immune System helps us achieve this."

IT Infrastructure Engineer, Harwich Haven Authority

"With Darktrace Antigena defending our network around the clock, we can finally prioritize strategically important activities while Darktrace's AI works in the background to contain the threats that get through."

Chief Operating Officer, The Caravel Group

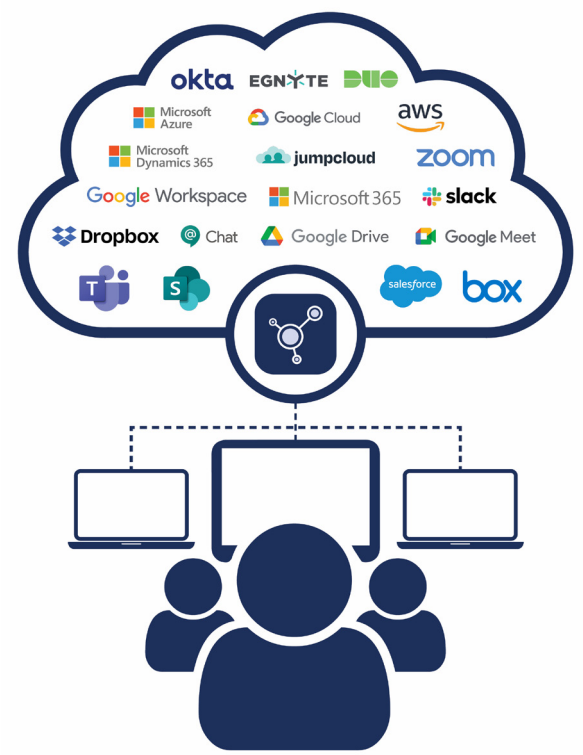

Figure 4: Darktrace seamlessly defends a wide range of cloud and SaaS technologies