CASE STUDY

DRAGOS

Terminal Operator Partners with Dragos to Reduce Costs and Enhance OT Cybersecurity

BACKGROUND

The maritime and logistics industry is highly dependent on efficient and secure operations to ensure timely delivery of goods and cargo. Port owners and operators need to ensure that their operational technology (OT) environments are secure from cyber threats to avoid disruptions in operations.

Cybersecurity is particularly challenging in today's world, partially because of the increase in threats and digital connectivity, and partially because of the shift in how supply chain is managed in the wake of the COVID-19 pandemic. Traditionally, supply chains have primarily relied on the "just in time" model, which emphasizes efficiency and cost reduction by minimizing inventory levels and relying on precise demand forecasts. The pandemic exposed vulnerabilities in this approach, and the concept of "just in case" emerged. This new approach represents a shift toward building more resilience and flexibility into supply chains by maintaining larger inventories, diversifying sourcing options, and developing contingency plans.

In this case study, we discuss how a leading container terminal operator approaches OT cybersecurity in general and how the company leverages Dragos technology and professional services to secure their environments.

BUSINESS OVERVIEW

This customer is one of the world's largest and most innovative container terminal operators, with a history of driving terminal efficiency.

1,200+ vessels handled

3M+ TEU handled per annum

The company operates several large port facilities that handle a significant number of containers daily. Port operations are automated, with various OT systems controlling cargo handling equipment, safety systems, lighting, and security systems.

CHALLENGES

In 2017, a piece of malware called NotPetya infected the computer systems of A.P. Moller-Maersk, a Danish shipping conglomerate, and spread to other companies worldwide.

The attack caused widespread disruption to Maersk's operations, including the temporary shutdown of several of its container terminals and port operations. The company estimated that the incident cost between $200 million and $300 million USD in lost revenue and recovery costs. The Maersk incident is often cited as a cautionary tale for the importance of cybersecurity and the need for companies to take proactive steps to protect their systems and data, and probably served as a trigger for insurance companies to take a closer look at pricing cybersecurity risk into their policies.

During this time, the performance and security of operations technology was managed by the maintenance department at the company, rather than a centralized, security-focused business unit. Facing premium increases, along with heightened focus on OT cybersecurity because of the Maersk headlines, the leadership team kicked off the development of a strategic roadmap that included significant investment in its existing safety-focused culture, a conscious environmental initiative, and projects to evaluate and increase operational technology cybersecurity posture at each of their port locations. Management was already concerned about the potential impact of cyber threats on their OT systems and the potential for disruptions in operations, and the initiatives driven by the roadmap exercise helped to provide the attention and funding needed to tackle the challenges.

THE COMPANY CONSIDERED THE FOLLOWING CHALLENGES WHEN BUILDING THEIR OT CYBERSECURITY ROADMAP AND SELECTING DRAGOS AS A PARTNER:

- **Increased threat surface:** With the integration of digital technology and IoT devices, the attack surface for cyber criminals is permanently expanded. The company understood that their ports could be vulnerable to attacks on their networks, data systems, and IoT devices.
- **Complex supply chain:** The ecosystem involves a complex network of suppliers, partners, and stakeholders. The sharing of data and information between these entities creates more opportunities for cyber attacks and data breaches and must be managed carefully.
- **Legacy systems:** Some of the ports still use legacy systems that are outdated and no longer supported by vendors. These systems are more vulnerable to cyber attacks and are harder to patch or update.
- **Cybersecurity awareness:** The maritime and logistics industry is still catching up with other sectors in terms of cybersecurity awareness and training. The company was ahead of that curve, but still wanted to ensure that all port operators obtain and maintain the necessary knowledge and skills to detect, prevent, and respond to cyber threats.
- **Physical security risks:** The maritime and logistics industry is vulnerable to physical security risks such as theft, sabotage, and espionage. The company has been able to eliminate a lot of these risks through innovative automation, but they remain vigilant because cyber attackers can exploit any vulnerabilities to gain access to critical infrastructure and data.

SOLUTIONS

Addressing cybersecurity challenges in the maritime and logistics industry requires a comprehensive approach that includes risk assessment, policy development, employee training, and technology upgrades. By taking proactive steps to address cybersecurity risks, port operators can reduce the risk of cyber attacks and protect their operations and data.

Our customer took the following steps to develop a world-class OT cybersecurity program:

- The team worked with Dragos and other partners to conduct comprehensive cybersecurity risk assessments to identify vulnerabilities and risks in the port's network and IoT devices.
- Using the challenges outlined above as a backdrop, the team reviewed results of the risk assessments in the context of their environment. Next, they developed and implemented a cybersecurity plan that includes policies and procedures for incident response, data protection, and access control.
- Within this plan, they did a proof-of-concept (POC) with Dragos. Based on the results, **they procured and deployed the Dragos Platform, to monitor and detect cyber threats to the port's OT systems.** The Platform uses advanced analytics to detect and respond to cyber threats, including malware, phishing, and other types of attacks.

IN ADDITION TO THE DRAGOS PLATFORM, THE TEAM ALSO ENLISTED THE FOLLOWING SUPPORT:

- **Dragos Incident Response Retainer:** OT-specific response plans are essential for OT environments. With different devices and communication protocols, OT incident response is distinct from IT, with different attack tactics, techniques, and procedures (TTPs) used by threat groups. The team understood this and worked with Dragos to proactively prepare for cyber threats, conducting tabletop exercises to fine-tune their ability to ensure business continuity. The company also retains 24/7 access to globally recognized incident responders as part of their Dragos Incident Response Retainer.
- **OT Watch Managed Threat Hunting:** Dragos uses their threat hunting capabilities to detect any potential threats in the port's OT environment. This includes conducting analysis of network traffic, log files, and other data sources to identify any suspicious activity.
- **Neighborhood Keeper:** Neighborhood Keeper is a collective defense and community-wide visibility solution that provides a more effective industrial cyber defense by sharing threat intelligence at machine-speed across industries and geographic regions. By participating, each organization's defensive capability is made stronger than what they can achieve on their own.

RESULTS

Through their unwavering dedication to OT cybersecurity and their partnership with Dragos, the company has been able to significantly enhance the security of their OT environments. Today, they can quantify and prove their ability to detect, mitigate, and respond to cybersecurity threats across their networks – resulting in favorable insurance premiums, increased trust and collaboration with internal stakeholders and endorsed by the board, and best-in-class positioning with regulatory bodies.

DRAGOS PLATFORM USAGE PROFILE AND BENEFITS

Dragos Platform technology has provided continuous monitoring and detection of potential cyber threats, allowing the ports to take proactive measures to mitigate the risk of cyber attacks.

- The team uses the Platform to conduct automated asset inventories and analyze multiple data sources including protocols, network traffic, data historians, host logs, asset characterizations, and anomalies.
- Operators use the Platform to verify vulnerabilities or supply chain compromise risks, using the corrected, enriched, prioritized guidance within the Platform to manage the full lifecycle of specific vulnerabilities in their environments.
- The team uses a combination of the Platform and OT Watch Managed Threat Hunting to pinpoint malicious behavior on their ICS/OT networks.
- In the event of an incident, the company uses expert-authored playbooks to guide their security team step-by-step through investigations, decreasing response time and improving efficiency.
- The Dragos Platform and ancillary services make compliance much easier and more streamlined. In fact, the customer estimates that more than 85 percent of their systems qualify two levels above the minimum standards set forth by their local and regional regulations.

The customer considers the following as the top benefits derived from their use of the Dragos Platform:

- Increased efficiency and productivity
- Asset inventory, verification, and changeover is much easier and more streamlined
- It's easier to collect reporting and metrics for compliance, insurance, regulatory requirements, and board reporting
- Less alert fatigue
- Reduction of 'Shadow IT' activities within the OT environments
- Easier and faster identification of misconfigurations
- Increased visibility into threats
- Better, more contextual awareness of vulnerabilities
- Easier and more effective vulnerability management

KEY INSIGHT:
The customer found the sheer volume of assets illuminating — so many PLCs were hidden away, playing small roles in the operations process. Once the Dragos Platform was deployed using sensors that could analyze both IT and OT zones, the team was able to identify, prioritize, and clean up traffic in the environment, reducing extra noise and simplifying monitoring.

> Using the Dragos Platform, we have a comprehensive and constant understanding of our extended OT network environment, and as a result, we can rapidly identify and remediate threats before they have a chance to impact the continuity of our business and operations.

Company Chief Information Officer

OT WATCH MANAGED THREAT HUNTING BENEFITS

An elite team of Dragos analysts, backed by many decades of ICS cybersecurity experience, conducts threat hunts of the customer environment based on insights from the latest global ICS threats and adversaries.

- The team uses OT Watch to reduce the risk of attackers going undiscovered for an extended period of time, affecting the availability of key processes and safety systems.
- Internal teams use the Platform to establish a solid baseline, and they leverage OT Watch to get real-time reports detailing changes in ICS asset characteristics and behaviors.
- Dragos analysts serve as an extension of the customer's Security Operations Center (SOC) to provide enhanced coverage, remotely monitoring and hunting in their OT environments and triages high severity alerts.

The customer considers the following as the top benefits derived from their use of the OT Watch:

- Pro-active, real-time knowledge of what's happening across networks
- Speed and quality of notifications and responses from the Dragos team
- Enhanced situational awareness with contextually appropriate information
- Global insights about the latest IOCs and TTPs are baked-in to reports and recommendations
- Knowledgeable prioritization and triage of high severity alerts

> We've formed meaningful relationships with our Dragos counterparts. We can ask any question in our minds and feel confident that they have a deep understanding of our environment and our company's priorities. They are always available to help us, often proactively giving us easy-to-follow mitigations advice before we've even noticed a detection.
>
> **Company Infrastructure & Security Manager**

NEIGHBORHOOD KEEPER BENEFITS

The Neighborhood Keeper technology is an opt-in on top of the Dragos Platform capable of detecting supply chain risks and equipment, vulnerabilities, and cyber threats that need to be identified and remediated, acting as a sort of collective defense while enabling trusted industry and government partners to leverage the system as a cyber national broadcasting service.

- The customer monitors and contributes to Neighborhood Keeper to help other companies proactively defend their OT environments.
- The team can see anonymous, non-sensitive data relevant to their world region and industry.
- Neighborhood Keeper provides a foundational system that can analyze OT data, get the insights safely to governments around the world, and ultimately get it into the hands of the intelligence community.

8 TAKEAWAYS FOR IMPROVED CYBER DEFENSE

The maritime and logistics industry is highly vulnerable to cyber threats, which can disrupt operations and result in significant financial losses. Our customer is a best-in-class example of how to mitigate risk and improve efficiencies in these unique environments.

Here are some recommendations for other maritime and port logistics companies to follow:

1. **Develop a cybersecurity strategy:** Develop a comprehensive cybersecurity strategy that is tailored to the specific needs of your organization. This should include an assessment of cyber risks including the OT environments and the development of policies and procedures to manage those risks.
2. **Conduct regular risk assessments:** Conduct regular risk assessments to identify vulnerabilities in your network and systems. This will help you prioritize your cybersecurity efforts and ensure that you are addressing the most critical risks first.
3. **Train employees:** Provide regular training to employees on cybersecurity best practices, including how to identify and respond to cyber threats. This will help to ensure that employees are aware of the risks and are equipped to take appropriate action. Use specialized OT related courses for key maintenance staff.
4. **Implement access controls:** Implement access controls to limit who has access to sensitive systems and data. This should include measures such as multi-factor authentication, role-based access control, whitelisting applications, and network segmentation.
5. **Take a risk-based approach to patching and updating systems:** Prioritize patches based on the level of risk they pose to critical systems and operations. This should consider factors such as the criticality of the system, the likelihood of a successful cyber-attack, and the potential impact of an attack.
6. **Use network monitoring and intrusion detection systems:** Implement network monitoring and intrusion detection systems to detect and respond to cyber threats in real-time.
7. **Conduct regular penetration testing:** Conduct regular penetration testing to identify vulnerabilities in your systems and network. This will help you to identify weaknesses and take corrective action before an actual cyber-attack occurs.
8. **Implement incident response plans:** Develop and implement incident response plans that outline the steps to be taken in the event of a cyber-attack. This should include roles and responsibilities, communication procedures, and steps for restoring systems and data. Institute a response retainer with a company who can provide 24/7 access to trained, globally respected ICS practitioners who understand your environment.

By implementing these recommendations, maritime and port logistics companies can better protect their OT systems and data from cyber threats, reduce the risk of a cyber attack, and ensure the secure and reliable operation of critical infrastructure.

To learn more about the Dragos Platform or our other products and services, please contact **sales@dragos.com** or visit **dragos.com**