CASE STUDY

DRAGOS
SAFEGUARDING CIVILIZATION

A Collaborative Approach to Building a Stronger OT Security Posture with the Dragos Platform and Threat Intelligence Services

This anonymous technical case study demonstrates how Dragos OT cybersecurity technology and threat intelligence solutions, working together, assist customers in delivering security outcomes that build cyber resilience across their industrial control systems (ICS) and operational technology (OT) environment.

The customer deployed the Dragos Platform, our OT cybersecurity technology that provides OT-native network visibility and monitoring, in their OT environment. Additionally, they added the Dragos OT Watch threat hunting service and a Dragos WorldView Intelligence subscription with concierge analyst support. This case study demonstrates how the combination of people, processes, and OT-native cybersecurity technology can provide the guidance, resources, and hands-on approach required to deliver effective OT security outcomes.

OT Cybersecurity Challenges & Solutions

Overall, the customer faced visibility challenges across their environment prior to implementation of Dragos solutions. Those visibility challenges not only stemmed from gaps in asset visibility, but overall threat visibility across their environment. The Dragos Platform provided the customer with visibility they had lacked and felt they had gaps in prior.

The customer faced limited knowledge of threats and threat intelligence and had limited resources to devote to the problem. Additionally, it was difficult to find actionable information as the information they were getting was vague. The time and resources to parse through the numerous intelligence sources they already had in order to determine what was or wasn't applicable also posed challenges. Onboarding the fleet of Dragos OT cybersecurity technology and solutions supported efforts to identify critical threats and vulnerabilities to their environment while allowing them to lean on experts in the space to provide guidance.

The Dragos Concierge Service has provided statistics and facts around the customer's cybersecurity threat posture to support industry presentations. The customer found that onboarding Dragos OT Watch provided the SOC monitoring capabilities and resources they needed, with someone that could look at their Dragos Platform environment regularly. The customer identified their in-house skillsets were more geared for maintenance not system security, therefore were unable to investigate potential threat activity or detect such activity.

A Real-Life Threat Scenario

During daily activities within the customer's environment, the Dragos Concierge Analyst observed multiple peculiar logins taking place recurrently several times a day within their environment. Subsequently, these logins were accompanied by domain controllers (DC) executing domain name service (DNS) queries within the OT network, notably this same activity was linked to the Oldsmar water utility attack of 2021. Moreover, the analyst unearthed numerous New DCSync alerts permeating the environment.

Following an extensive investigation in collaboration with the OT Watch team and the customer, it was collectively determined that the queries were benign, yet the underlying cause remained unknown. The customer received a custom report from Dragos Intelligence with contributions from OT Watch. Notably, Dragos had identified similar alerts in other customer environments, prompting the realization that providing additional context would be advantageous for all Dragos customers.

Intelligence reporting and playbooks for DCSync operations were already integrated into the Dragos Platform, but this engagement sparked a collaborative endeavor with OT Watch to formulate an Analysis & Assessment (AA) specifically addressing New DCSync operations and persistent DCSync detections. The objective was to provide insights into the nature of these operations and guidance on how to respond. This joint effort culminated in the creation of the inaugural Dragos OT Watch and Intelligence joint report, a significant milestone in enhancing cybersecurity awareness within OT.

Furthering the proactive approach, the concierge analyst collaborated with the customer and their Dragos technical account manager (TAM), a service included with the purchase of the Dragos Platform, to fine-tune the customer's environment appropriately. This involved a meticulous examination of why DCSync operations were occurring with such frequency. Leveraging the capabilities of Dragos Concierge Intelligence facilitated seamless collaboration within the customer's organization, ultimately assisting in resolving the issue. This not only curtailed unnecessary operations but also bolstered the customer's confidence in the Dragos Platform notifications. The comprehensive approach taken mitigated the immediate concern and contributed to a more robust and secure OT cybersecurity posture for the customer.

An Intelligence-Driven Approach

Collaborating seamlessly, the Dragos concierge analyst and OT Watch team orchestrated a coordinated effort to eliminate redundant tasks and maintain transparent communication with the customer. The Dragos concierge analyst adeptly used Neighborhood Keeper to gain insights into critical cyber activities spanning various environments, discerning prevalence patterns that could signal potential threats to ICS and OT environments.

This enhanced use of OT cyber threat intelligence tools further enriched the collaborative efforts, including the refinement of the Dragos Platform playbook, the creation of a tailored joint OT Watch and Intelligence report delivered to the customer, and the development of a threat intelligence report accessible to all WorldView subscription customers. Dragos Concierge Intelligence, bolstered by tools like Neighborhood Keeper, emerges as a pivotal asset for any OT security or intelligence team, seamlessly integrating and fortifying all aspects of the cybersecurity mission.

Benefits

- Leveraging Dragos Platform, Dragos Concierge Analyst and OT Watch provide a coordinated investigation to determine real threat of peculiar DCSync operations and detections.
- The collaboration produces the first joint customer report from Dragos Intelligence and OT Watch, further enhancing OT cybersecurity awareness.
- Dragos Concierge worked closely with the Dragos Platform TAM to operationalize the technology to address and resolve the DCSync issues and fine-tune the customer's OT environment, giving them more confidence in platform notifications.
- The joint Dragos solution and coordinated efforts across teams leveraging Dragos Platform and Neighborhood Keeper technologies proved to be a pivotal asset in fortifying the customer's organizational security.

About Dragos, Inc.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

Learn more about our technology, services, and threat intelligence offerings:

Request a Demo   Contact Us