CASE STUDY

DRAGOS
SAFEGUARDING CIVILIZATION

International Airport Leads the Aviation Industry in Cybersecurity Strength and Innovation

How one of the world's top travel hubs modernized OT security and reduced operational friction with Dragos

Discover why the airport's cybersecurity team trusts the Dragos OT Cybersecurity Platform, OT Watch, and Worldview threat intelligence service to stay prepared and protected against cyber threats. With Dragos, the team ensures that operations – and their customers' travel plans – run smoothly and seamlessly.

AIRPORT STATS

26,500+
flights between 28 different countries

300+
different flight routes

80+
airlines

±3 million
passengers served each month (average)

OT Cybersecurity Team Boosts Awareness and Alignment with Threat Modeling

The airport first implemented a dedicated OT cybersecurity team in the late 2010s. By the time the cybersecurity manager joined the team in 2022, the program had evolved dramatically. The manager explained, "Our Cyber team quickly went from being the naysayers and the police into business enablers. We help the business strategically balance achieving long-term positive outcomes with moving fast."

A key component to that strategy has been threat modeling. The airport cybersecurity team collaborates with operational leaders to run frequent tabletop scenarios that illustrate the impact of various situations.

"If the airport has a problem, the whole country has a problem," explained the cybersecurity manager. "The tabletops help us understand how long it would take us to detect and recover from an incident, as well as what it would take to restore operations and the impact to the business and the wider aviation sector across the country."

The tabletop modeling exercises gave the technical and operational teams critical insight into potential scenarios and ensured strong executive and stakeholder alignment. Early iterations also revealed a gap in the organization's overall cybersecurity approach: they needed sophisticated OT-specific cybersecurity technology that would bring the operational side of the house up to par with the IT side.

IMPORTANCE OF USING THREAT SCENARIOS AND TABLETOP EXERCISES IN OT CYBERSECURITY PROGRAMS

Threat scenarios are critical tools in Operational Technology (OT) cybersecurity programs, offering a multitude of benefits that enhance the overall security posture of operations environments. The airport cybersecurity team understood the value of leveraging realistic scenarios, for these reasons:

1. **Risk Assessment:** Threat scenarios help in pinpointing vulnerabilities within OT systems. By simulating potential attack vectors, organizations can identify weak points and prioritize resource allocation to address the most critical risks.
2. **Preparedness Planning:** Simulated threat scenarios enabled the team to evaluate their readiness for real-world cyber incidents. These exercises helped to identify gaps in security controls and preparedness plans, ensuring that the organization is better equipped to handle actual threats.
3. **Proactive Defense Measures:** Analyzing threat scenarios informed the implementation of proactive defense measures. By understanding potential attack methods, the airport cybersecurity team could deploy security controls designed to mitigate these risks before they can be exploited by adversaries.
4. **Incident Response Planning:** Threat scenario simulations are invaluable for incident response planning. They allow complex organizations like the airport to devise effective strategies, define roles, and outline containment and recovery procedures. This ensures a swift and coordinated response to actual incidents, minimizing downtime and damage.
5. **Employee Training:** Regular training based on threat scenarios educates employees about potential threats and the appropriate responses. This not only aligns with compliance requirements but also fosters a culture of continuous improvement and vigilance.
6. **Enhancing Security, Readiness, and Resilience:** Ultimately, leveraging threat scenarios empowers the airport to enhance their security, readiness, and resilience. By regularly testing and refining their cybersecurity measures, they can better protect their OT environments from evolving threats.

Dragos Brings Advanced Visibility, Holistic Detection Capabilities, and Expert Intelligence

The airport cybersecurity manager began by identifying the most important capabilities of an OT cybersecurity solution. It was imperative that the technology included:

- **Advanced visibility into OT networks** with zero risk of down time or interference
- **Holistic detection capabilities** that go beyond alerts to contextualize and prioritize issues
- **Expert intelligence** for ongoing knowledge of the greater OT cybersecurity landscape

After soliciting several RFPs, "Our requirements drove us overwhelmingly to Dragos," the manager shared. "The insights were well ahead of the competitors. We could understand them and easily act on them. It's easy to put in technology that alerts you to everything. With Dragos, we got context – the ability to confidently know which alerts to ignore and which ones to act on."

> If our airport has a problem, the whole country has a problem. The tabletops help us understand how long it would take us to detect and recover from an incident, as well as what it would take to restore operations and the impact to the business and the wider aviation sector across the country.
>
> **Airport Cybersecurity Manager**

The airport deployed Dragos across several use cases in its complex operational ecosystem. Dragos secures industrial control systems in baggage handling, weather management, security and surveillance, and airport facility management, particularly lighting control systems. The team adopted the software platform, OT Watch, and Dragos Worldview for a comprehensive approach to OT cybersecurity.

Airport Improves Cybersecurity, Operational Efficiency, and Compliance

With Dragos, the airport has transformed OT cybersecurity while improving operational efficiency, compliance, and visibility.

Perhaps most importantly, Dragos gives the cybersecurity manager and his team the information and assurance they need to make smart decisions, fast. This applies to both long- and short-term scenarios. "In the moment," the manager elaborated, "Dragos helps us justify intervention when it's necessary. We feel comfortable taking action even if it causes operational impact because the overall impact will be reduced and leadership trusts our judgment. In general, we're no longer just feeling around in the dark trying to protect ourselves. Dragos lets us know what to protect against so we can make strategic investments in the things that will materially impact our posture."

Dragos also helps the airport do more with a small cybersecurity team. "We only have so many people and so many hours in a day," the cybersecurity manager continued, "so being able to prioritize is really powerful. We take great comfort in the fact that if we ignore something, we know it's low priority or low severity and not going to cause any issues."

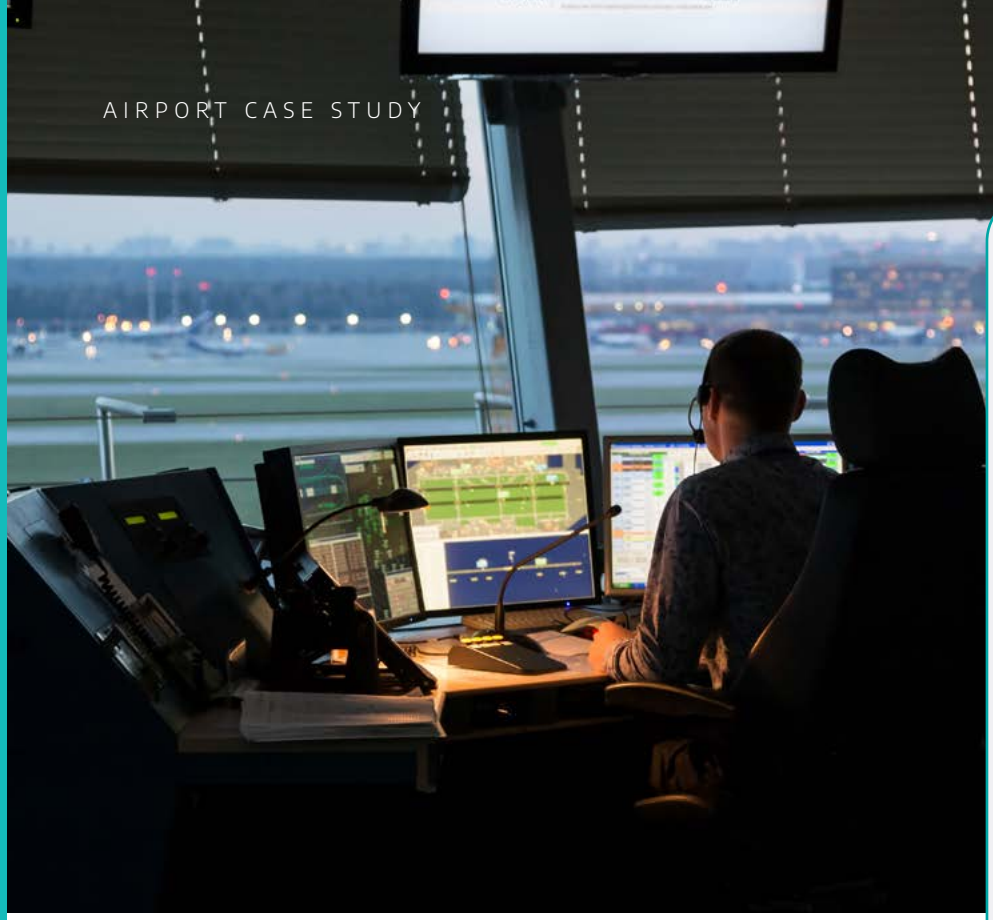
The operational benefits of the Dragos Platform have been significant as well. The ability to inspect any traffic flow in the OT network in real time helps operations team troubleshoot issues more quickly and effectively. Instead of spending hours walking to the "badlands" of the airport, the cybersecurity team can instantly capture packets to figure out the root causes of operational problems. As a result, operations teams have more time to address larger challenges that have long been on the backburner.

Dragos helps with compliance, too. According to the cybersecurity manager, "We used to have a feeling if something was near the end of its life and probably out of compliance but had no way to measure or report on it. Previously, the OT cybersecurity program started and stopped at asset management. Now we know the exact lifecycle status of each piece of technology, including a baseline of activity, so we can proactively increase compliance and identify misconfigurations and operational inconsistencies."

Finally, the airport relies strongly on Dragos OT Watch for staying up to date with the latest cybersecurity trends and threats and making the most of the platform. "OT Watch was a no-brainer. It helps us keep the platform fully tuned and optimized and make the most of our investment. We consider OT Watch mandatory," the cybersecurity manager said.

OT WATCH: AN ESSENTIAL ADD-ON TO THE DRAGOS PLATFORM

Dragos OT Watch adds a layer of advanced and scalable industrial threat hunting to the comprehensive cybersecurity capabilities of the Dragos Platform. Advanced cyber threats can hide within legitimate ICS/OT network operations, making threat detection challenging. To proactively combat these threats, it's critical to combine advanced cybersecurity technology with specialized human expertise.



KEY BENEFITS OF OT WATCH

- **Early Detection of Threats:** Using industry leading threat inputs, including proprietary threat intelligence, OT Watch proactively hunts for sophisticated threats that bypass traditional security measures, reducing potential adversary dwell time in customer environments and mitigating impact of attempted attacks.
- **Improved Response Time:** OT Watch prioritizes suspicious detections within the Dragos Platform and provides the human expertise to escalate high impact threats promptly with actionable guidance.
- **Identification of Misconfigurations:** In the course of hunting operations, OT Watch often finds network, system and application misconfigurations, thus optimizing security posture and limiting attack exposure.
- **Proactive Risk Mitigation:** Proactive threat hunting enables a focused response to high probability threats to reduce risk to the business.
- **Collective Power:** Customers benefit from the shared insights across the OT Watch client base and enhance their security posture by leveraging expert industrial threat hunters to augment their team.
- **Health And Tuning for the Dragos Platform:** With OT Watch Premium, customers gain regular platform health support and assets, zones, and alerts tuning of the Dragos Platform to maintain peak performance.

Up Next: Airport Expands OT Footprint, Secured by Dragos

The airport has made dramatic strides in modernizing OT security in the last few years, and the airport cybersecurity team has no intention to stop now. Exciting plans for the future of the airport come with an expanded footprint of new operational technology, like bringing in 5G towers to support connectivity on all runways. "As we evolve our use of OT with embedded technologies, we will absolutely make sure they are covered with controls through Dragos," the cybersecurity manager concluded. "Now that we have this visibility and these capabilities, it just seems natural. We would never consider not having it again."

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