CASE STUDY

How an International Airport Manages Cyber Exposure Risk with a Diverse IT/OT/IIoT Environment

The Challenge

- Limited ability to monitor and manage digital assets across operational technology systems
- Insufficient processes for OT security risk management
- Lacked clear and prioritized guidance for addressing identified security gap

The Solution

- Armis provided unified risk visibility with broader security coverage by discovering and gaining deep awareness of every critical asset and existing control
- Delivered detailed asset information with clear and prioritized understanding of vulnerabilities and operational impact
- Offered actionable, contextualized mitigation along with assignments and steps tailored specifically for airport operations and resiliency

The Results

- Comprehensive asset inventory
- Expanded asset inventory along with interrelationships between devices and business impacts
- Improved Mean-Time-to-Detect (MTTD) and Mean-Time-to-Respond (MTTR), through prioritization of OT security risks

Industry: Transportation

Location: N/A

Size: N/A

Armis Centrix™ for OT/IoT Security (On-prem)

Background

An international airport is a large critical infrastructure organization that operates in a complex environment of OT-IT-IIoT assets. The airport's digital security team had limited security governance, initial asset documentation, and a partial work process to identify and reduce security risks. They sought a solution that would provide:

- Comprehensive OT-IT-IIoT asset visibility to identify and inventory all of the airport's digital assets and their configuration details
- Digital security risk governance to support the security team with a 'big-picture' management view of the airport's digital security and operational technology systems
- Prioritize risks based on business and operational impact
- Feasible risk mitigation steps in a facility that could not regularly schedule downtime for maintenance
- Automated, efficient, and effective security operations
- Streamline existing workflow processes for SOC teams and asset owners

The Challenge

Prior to engaging with Armis, this customer maintained limited security governance across its OT, IT, and IIoT environments, lacking the comprehensive oversight needed to effectively monitor and manage its digital asset landscape.

The airport's OT security team had constrained capabilities for orchestrating and enforcing internal OT risk management workflows.

Asset visibility was rudimentary, with only baseline discovery of OT-IT-IIoT devices and minimal system automation to track asset configurations, firmware versions, and network connectivity.

While there was partial awareness of security gaps within the OT network, the organization lacked a structured, actionable framework for prioritizing and addressing risks across its converged infrastructure.

The Solution

Armis worked with the airport's cyber security and operations teams to deploy the RAM2 (Risk Assessment, Monitoring, and Management solution) for central extended visibility of all risks affecting the airport's different OT-IT-IIoT assets. RAM2 provided the team with a comprehensive asset inventory and overview of the digital environment by integrating with the airport's existing firewalls, EDRs, and Airport systems (Airplane visual clocking guiding stations (VDGS), Access control system (ACS), Closed-circuit television (CCTV), etc.).

The RAM2 OT digital risk management platform included Armis Centrix™ for OT/IoT Security (On-prem) to enrich the database, using a multi-detection engine that leveraged safe active query, and passive monitoring re-using existing SPAN ports.

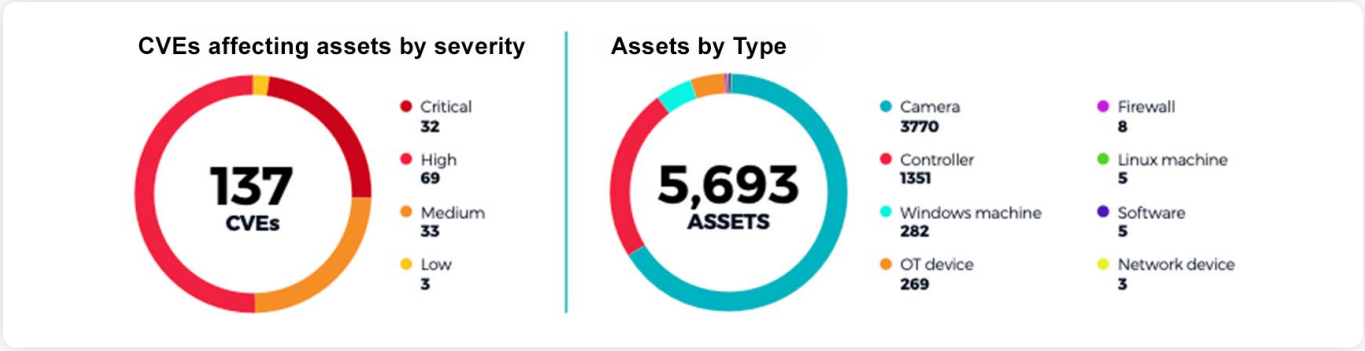
Connecting to different data sources provided valuable, in-depth information about the airport's OT environment:

- RAM2 performed a comprehensive, accurate OT-IT-IIoT asset inventory using safe active query, discovering assets that the airport's digital security team was unaware of, as well as their configuration details.
- A unique plug-in for the airport 's CCTV management system identified and expanded the asset inventory as well as pathways.
- RAM2 analyzed existing firewalls configurations and provided insights on existing segmentation gaps along with required mitigation steps.

Business Outcomes & Key Benefits

- **Unified Risk Visibility -** The airport now benefits from a centralized, real-time view of converged IT, OT, and IIoT risk across its entire operational environment, enabling more effective and informed decision-making.
- **Maximized ROI on Existing Security Investments -** By integrating Armis Centrix™ for OT/IoT Security (On-Prem) with its existing tools and controls, the airport significantly enhanced the value and effectiveness of its prior security investments.
- **Operational Context for Risk-Based Management -** Security and operations teams now have full visibility into the operational context and potential business impact of assets and processes thus enabling more accurate OT risk prioritization and faster response planning.
- **Improved Detection and Response -** Armis Centrix™ delivered actionable intelligence that reduced Mean-Time-to-Detect (MTTD) and Mean-Time-to-Respond (MTTR), accelerating the airport's ability to identify and contain OT cyber exposure threats.
- **Executive-Level Visibility -** A comprehensive digital security assessment report now provides senior leadership with clear insights into the organization's OT cybersecurity posture (along with drill down capabilities), helping drive strategic alignment and informed risk management.

- **Strengthened Cross-Team Collaboration -** The solution fostered tighter coordination between the SOC and OT asset owners through shared visibility and executable OT risk mitigation playbooks with step-by-step guidance.
- **Proactive Preparedness -** The airport is now better equipped to prevent and respond to ransomware and threats through automated exposure analysis and continuous monitoring of OT vulnerabilities, misconfigurations and risk.



[1] A RAM2 assessment refers to the Risk Assessment Methodology for Critical Infrastructure Protection developed by Sandia National Laboratories, often used in sectors like transportation, energy, and water systems. It is a structured, scenario-based risk assessment framework designed to evaluate security risks at facilities such as airports, seaports, rail systems, and other critical infrastructure.

ARMIS

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011
www.armis.com