OTORIO

Smart Infrastructure

How an International Airport Manages Digital Risk with OTORIO in a Diverse OT-IT-IIoT Environment

Case Study

Flexible integration with different airport systems

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**
- **Automated, efficient, and effective security operations**
- **Streamline existing workflow processes** for SOC teams and asset owners

Customer Challenges

- The customer had a partial security governance capabilities to monitor and manage all OT-IT-IIoT digital assets
- The airport OT security team had a limited ability to manage and monitor internal work processes for OT security risk management
- Basic OT-IT-IIoT asset visibility and system automation to track asset configurations and connectivity in the network
- The customer had partial awareness of gaps existing in its OT network security posture. It was missing a clear, practical guide on what steps should be taken to mitigate risks affecting the OT-IT-IIoT environment

Highlights

As a holistic and agile solution, OTORIO's RAM² platform empowers the international airport's operational and security teams to proactively manage digital risks and build resilient operations through a technology enabled ecosystem. RAM² enabled security teams to:

- Get an accurate OT-IT-IIoT asset inventory
- Have a central OT security management view
- Identify risks
- Take feasible mitigation steps tailored for the OT environment

OTORIO's Solution

OTORIO 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
Juniper and Palo Alto

EDRs
Crowdstrike

Airport systems:

- Airplane visual docking guiding station (VDGS)
- Access control system (ACS)
- Closed-circuit television (CCTV)
- Baggage handling system network
- Building management systems
- ServiceNow' ticketing system

The RAM² OT digital risk management platform includes OTORIO's proprietary solutions to enrich the database:

OTORIO's safe active query

OTORIO's passive monitoring, re-using existing SPAN ports

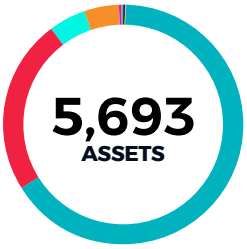
Connecting to different data sources provided valuable, in-depth information about the airport's OT environment:

- 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.
- OTORIO's team developed a unique plug-in for the airport customer's CCTV management system, and identified and expanded the asset inventory visibility.
- RAM² analyzed existing firewalls configurations and provided insights on existing segmentation gaps along with required mitigation steps.

CVEs affecting assets by severity

- Critical **32**
- High **69**
- Medium **33**
- Low **3**

Assests by Type



- Camera **3770**
- Controller **1351**
- Windows machine **282**
- OT device **269**
- Firewall **8**
- Linux machine **5**
- Software **5**
- Network device **3**

OTORIO

Smart Infrastructure

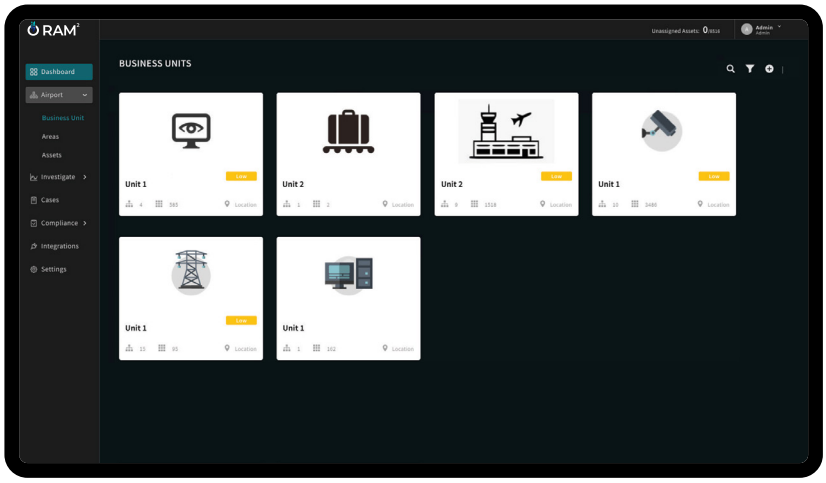
Holistic risk management overview

OTORIO's RAM² platform provided the international airport a unified organizational view of risk. This included:

- OTORIO's team:
  - Developing operational workflows based on priorities and risks
  - Identifying security team users
  - Defining roles
  - Building practical mitigation books suitable for the airport's environment
  - Prioritizing vulnerabilities based on the impact of their risk on the OT environment.
- Broader coverage of security and airport systems in the network by integrating with critical assets and existing security controls such as firewalls and EDRs.
- High-fidelity asset detail with a deeper and richer understanding of its role, impact, vulnerabilities, and relation to the operational hierarchy.
- An assessment of existing security controls and best practices to harden security configurations and OT-IT-IIoT network interfaces.
- Contextualized mitigation steps for each OT security risk, presented in a simple, actionable way that is suitable for the operational environment.

Benefits for the International Airport

- It now has a unified view of converged IT-OT-IIoT risk and network security systems within its OT environment.
- The airport enhanced its **ROI for pre-existing security controls** and solutions by integrating them with OTORIO's RAM² platform to leverage the airport's technology investments.
- Its digital security teams now have **OT operational context and impact analysis of an asset or process** for OT risk-based management.
- OTORIO's RAM² delivered insights that improved the company's Mean-Time-to-Detect (MTTD) and Mean-Time-to-Respond (MTTR), by highlighting and prioritizing OT security risks.
- The airport team obtained a comprehensive digital security assessment report, providing senior management with a full picture of the airport OT cyber security posture.
- Enhanced collaboration between the SOC team and asset owners. Both teams now have feasible OT risk mitigation playbooks with clear, step-by-step instructions.
- The airport is becoming "ransomware ready" by automating gaps and exposure analysis to reduce OT security risks.



About OTORIO

OTORIO's industrial-native OT security platform enables industrial organizations to achieve an integrated, holistic security strategy. Together with its partners, OTORIO empowers operational security practitioners to proactively manage cyber risks and ensure resilient operations. OTORIO's global team brings the extensive mission-critical experience of top nation-state cyber security experts combined with deep operational and industrial domain expertise.

CN 170822