Case Study

Airline Passes TSA Security Requirements and Operationalizes Asset Intelligence with Armis Centrix™

The Challenge

- Comply with new TSA AOSSP cybersecurity requirements to avoid potential fines
- Identify IoT and OT assets and vulnerabilities at the corporate campus and key airport locations
- Ensure that mission critical OT systems can continue to run safely when an IT system is compromised
- Limited in-house deep domain expertise specific to IoT/OT management and security

The Solution

- Deployed Armis Centrix™ in operational centers where most IoT/OT assets exist
- Created repeatable playbooks and processes customized to company's needs at each location
- Brought in a full-time Armis Resident Engineer onsite to oversee deployment, assist with developing new processes, troubleshooting, and training the team

The Results

- Developed capabilities to continuously identify, classify, and monitor OT assets in compliance with TSA AOSSP regulations
- Zeroed in on and prioritized vulnerabilities based on business risk to proactively remediate potential security issues
- Reduced risk of operational downtime
- Ensured OT vendors have resiliency plans in the event of unforeseen events
- Established a proven process for future onboarding and knowledge transfer

Industry: Aviation

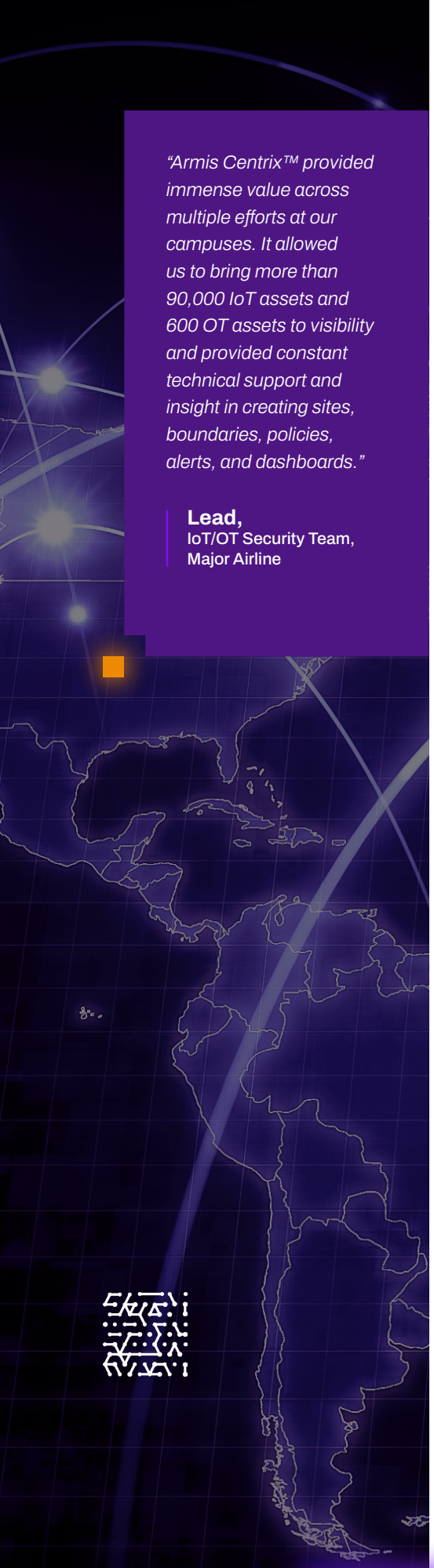
Location: United States

Size: 100,000 employees

Armis Centrix™ for OT/IoT Security

Background

This major airline operates close to 5,000 flights daily and is one of the oldest operating airlines in the U.S. It has major hubs across the United States. There are about 150 people on their security team, 30 of those sitting on the Cyber Monitoring Incident Response team. One of Armis' Resident Engineers (RE), works exclusively with the airline and is responsible for optimizing the airline's use of the Armis Centrix™ platform.



"Armis Centrix™ provided immense value across multiple efforts at our campuses. It allowed us to bring more than 90,000 IoT assets and 600 OT assets to visibility and provided constant technical support and insight in creating sites, boundaries, policies, alerts, and dashboards."

Lead,
IoT/OT Security Team,
Major Airline

The Challenge

Like all airlines in the U.S., this airline is subject to the regulations of the Transportation Security Administration (TSA). Through the Aircraft Operator Standard Security Program (AOSSP), the TSA requires that all aviation organizations identify all assets connecting to their environments and also be able to pinpoint any vulnerabilities associated with those assets. If an airline is found to be noncompliant with AOSSP, it risks potential fines by the TSA.

This airline was using a well known vendor as its main configuration management database (CMDB) to keep track of IT assets and configurations, but it lacked information on its IoT and OT devices, such as who manages them and potential vulnerabilities.

Their objective was to build and automate security capabilities so IoT and OT assets are protected with the same rigor and fabric of controls as its traditional IT assets. In anticipation of an upcoming TSA inspection, the new IoT/OT security team lead decided to deploy Armis Centrix™ for IoT/OT Security, leveraging an Armis engineer to oversee deployment, setup, and configuration.

The Solution

The initial deployment spanned across 21 locations, starting in one of the operational centers where planes are repaired and where OT assets, such as power distribution units and programmable logic controllers, are located. In just three months, the team deployed 25 Armis Collectors and completed 60 integrations to enrich the Armis data and optimize monitoring of their environment.

A big part of the initial work was to establish standard processes, writing templates, and building playbooks so that the work could be duplicated at other sites and when new people came on board. The Armis Resident Engineer worked onsite with the airline's engineers to ensure the right equipment was ordered, built dashboards and reports in Armis Centrix™, and provided customized troubleshooting procedures.

600+
unique OT asset types identified

90,000+
IoT assets brought to visibility

26 Sites

14 Terminals

340,000+
total assets managed and protected

The Results

Within 9 months, the airline was able to satisfy TSA requirements during a two-day onsite inspection. The team at the airline provided TSA with granular reports and dashboards showing where its OT assets are and who manages them, along with plans and timelines for remediating critical or high-severity vulnerabilities. “The TSA agent spent less than an hour looking at the report and then said everything looked to be in place. The bulk of the data came directly from Armis,” said the IoT/OT Security Team Lead.

Internally, they now have full visibility and a clear process on how and when to upgrade, replace, or take an asset offline. The airlines can also connect risks to operational efficiency for improved decision making.

The airline team further exceeded expectations by identifying 1,100 cameras in their headquarters that were previously hidden behind a network video recorder (NVR) that can store footage in the cloud. Armis helped to write a custom script to run in the AWS cloud that utilized the Armis data set specifically for video surveillance devices.

In the near future, the airline will be expanding the Armis Centrix™ presence in aircraft repair sites and pilot training facilities and will soon roll out the platform to airports in other states. As part of a larger network segmentation project, the platform will be used to identify rogue networks and gain visibility into other networks at the airports operated by third parties.

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.

See how leading organizations secure their environments with Armis.

See Armis Centrix™ in Action

+1 888 452 4011
www.armis.com