CASE STUDY: IoT Security for Airlines

Situation

The CISO of a major airline was on high alert after being informed that cyber criminals had compromised some of their most critical IoT systems, including flight operations, While their IT systems had almost daily attacks against them and strong defenses, their IoT/OT systems historically were not covered at the same level. In fact, the solutions they relied on for ensuring their IT systems were secure would not work with the unique operating systems and communication protocols used outside of IT. Reports of typical IoT devices used at airports like security cameras, access control systems, and routers being compromised elevated the need to take action.

The Board of Directors asked that a plan be presented to them at the next board meeting, including being able to deploy within 6 months. What was driving their focus were the tangible benefits already seen from their IoT investments (and plans to add more), including:

- Improved Operational Efficiency
- Enhanced Safety
- Reduced Costs
- Improved Customer Satisfaction
- Easier Tracking and Management
- Enhanced Environmental Conservation

Solution

The goal was clear: the airline needed an IoT security platform that could perform asset discovery, identify threats, and remediate threats across multiple types of systems. Asset discovery needed to not only look at the devices, but also the applications managing them and the networks they were communicating on, and had to be highly accurate. Threats needed to be judged based on CVE scores and prioritized for actions to be taken. For vulnerability remediation the key requirement was speed and scale in performing firmware patching, password changes, and certificate management across fleets of devices.

The solution also had to support compliance and reporting requirements. Given the public visibility that all airlines face (especially around cybersecurity), the decision was made that data from all system operations and vulnerability management would be captured in a digital twin. This would provide both forensic capability should there be an incident, but also would address the data required to renew cyber insurance (every renewal cycle brought more data requirements, and the insurer had already said they would be a lot more focused on IoT for the next renewal).

VIAKOO

Outcome

Evaluation of the Viakoo solution was performed in a Corporate IT lab, showing goals were met in terms of accuracy of asset discovery (far better than alternatives) and speed of vulnerability remediation. Because of the ease of deployment the airline decided to deploy based on function, not location, to stage the rollout and show immediate benefit in reducing their attack surface. The order of rollout was:

- Aircraft Maintenance
- Baggage handling
- Airport Operations
- Flight Operations
- Passenger Experience

Within 6 months the deployment was complete, with over 50,000 devices brought into the Viakoo Action Platform, with full visibility into their performance and vulnerabilities. In their report to the Board of Director the CISO was able to show that the solution lowered security risks, and had an ROI of a few months.

Challenges

The main challenge facing the airline was to be able to deploy in a timeframe that would both satisfy the Board of Director and fit with their available resources, while being able to show clear reduction in their attack surface. This required that the solution had to be capable of getting to remediation quickly (they had already had a bad experience with asset discovery, where it took forever and they struggled to know when to take action). To address this challenge only a complete platform with integrated discovery, remediation, and reporting would be considered.

Another form of challenge was that the solution could not have any on-site hardware added because of the many types of facilities the airline was operating from and needed to be cloud-based for easy access by Corporate to each facility. Training of onsite personnel (because of union requirements and turnover) had be minimal if at all. While the airline had previous (and successful) experience in deploying SaaS solutions, because it was a security solution they had to ensure the provider was SOC 2 certified and could support their need for penetration testing and SBOMs (Software Bill of Materials).