Customer Case Study: Airline Group Elevates Its Vulnerability Management Program

Industry: Aviation

Engagement Type: Vulnerability Management Deployment

Delivery Format: Remote

Engagement Duration: 1 week

Client Overview

Airline Group is a global leader in passenger and cargo air travel, with an extensive IT and cloud infrastructure supporting critical operations. To meet increasing regulatory demands and improve its cyber resilience posture, the organization adopted Vulnerability Management as its enterprise solution for exposure monitoring.

The engagement was chosen to accelerate deployment, improve scan coverage across business-critical zones, and establish a sustainable governance model for long-term program success.

Engagement Objectives

- Design and validate a scalable vulnerability management architecture across hybrid infrastructure, including Azure-hosted and on-premise environments
- Deploy and configure multiple sensor types, including Scanners, Agents, and WAS Scanners
- Establish clear access controls, tagging policies, and scan responsibilities to align with Airline's organizational structure
- Develop and implement foundational discovery, credentialed, and compliance scans with actionable reporting
- Document and deliver an operational playbook to support knowledge transfer and internal ownership

Strategic Priorities

- **Hybrid Infrastructure Coverage:** The organization operates in a segmented network environment, with zones like an Azure-based zone, PCI (regulated environments), and internal DMZs. Ensuring complete coverage across these zones was a critical success factor.

- **Sensor and Scan Optimization:** Deploying and fine-tuning multiple sensor types, including scanners, agents, and a WAS scanner, was essential to gain depth across both static and dynamic assets.
- **Role-Based Access & RBAC Implementation:** Clear user roles (Administrators, Scan Operators, Web App Readers) and access groups were needed to enable decentralized teams without compromising security.
- **Credentialed Scanning for Depth:** Enabling authenticated scans across Linux, Windows, and perimeter-facing assets was key to identifying misconfigurations and vulnerabilities missed by unauthenticated scans.
- **Compliance Readiness:** CIS benchmark scanning and tagging for compliance zones were requested to prepare for internal audits and external regulatory review.

Approach

Our team delivered the engagement in alignment with a four-phase deployment methodology:

1. Architecture Design & Readiness

- Conducted stakeholder workshops to validate scanning requirements and business priorities
- Reviewed all planned deployments across three Azure subnets and PCI zones
- Pre-validated scanner readiness including naming conventions, NTP sync, IP scopes, proxy configurations, and credential provisioning
- Created architecture diagrams and IP segmentation to map sensor coverage to technical and business zones

2. Sensor Deployment & Configuration

- Deployed six Scanners, including three in Azure and two in PCI on-premise environments
- Installed one WAS scanner for internal web application coverage
- Completed onboarding of Agents on key endpoints for workstation scanning
- Tuned scanners to adhere to organizational standards for performance and security, including proper certificate handling and memory allocation (up to 32 GB RAM)

3. Scan Policy Creation & Optimization

- Created and launched:
    - 12 Discovery Scans to detect live hosts across subnets
    - 16 Credentialed Scans (Windows/Linux) using domain credentials for deep visibility

- 4 Compliance Scans leveraging CIS benchmarks for key systems

- Established automated scheduling:
  - Workstations & servers: daily scans via agents
  - External/DMZ: daily via scanners
  - Compliance scans: monthly or quarterly based on system criticality
- Reviewed credential testing and failure handling with security stakeholders

4. Governance, Access Control & Handover

- Created 12 user accounts across multiple roles and 3 access groups, including an RBAC-compliant structure for Scan Operators, Admins, and Business Viewers
- Configured tagging policies using rule-based tags (e.g., by IP range, function, business unit) to facilitate access control and dashboarding
- Conducted knowledge transfer workshops to demonstrate dashboards, saved searches, and reporting best practices
- Delivered a comprehensive Operational Documentation Package, including:
  - Scanner and sensor deployment details
  - Credential and scheduling playbook
  - Role mapping and tagging policy matrix
  - CIS scanning roadmap

Results & Impact

- **Full Environment Visibility:** Nessus scanners and agents are now actively covering Airline's key infrastructure zones, including Azure, PCI, DMZ, and internal workstations.
- **Scan Automation in Place:** Automated scan schedules and credentialed configurations now provide consistent, reliable visibility across the environment.
- **Compliance-Ready Architecture:** The customer now has validated CIS scan templates, dashboards, and reporting mechanisms tailored for internal audit teams.
- **Operational Handoff Completed:** IT and InfoSec teams have ownership of tagging, user access, scan scheduling, and ongoing operational maintenance.
- **Foundational Governance Established:** Clearly defined roles, asset segmentation, and policy structure enable long-term scalability and auditability of the vulnerability management program.

Customer Feedback

“This engagement gave us clarity, structure, and a working platform for managing vulnerability risk across our diverse environment. We’re now in a position to scale confidently and meet compliance expectations.”

— **Cybersecurity Program Lead**, Airline Group

Address:
1000 Brickell Av, Suite 1015
Miami, FL 33131

Phone:
+1 (786) 397-0480

Maill:
info@mpivpartners.com