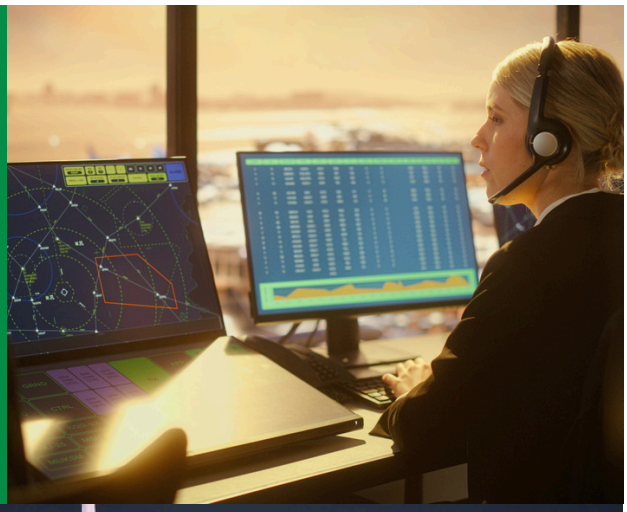
One of the World's Largest Airports Modernizes Cybersecurity with Seceon



Executive Summary:

One of the world's largest and busiest airports by passenger volume faced a significant cybersecurity challenge. With millions of travelers, thousands of flights, and critical infrastructure at risk, the airport was a high-value target for cyber threats. The existing security model relied on 10 different security tools and an outsourced 24x7 Security Operations Center (SOC) run by a Big Four consulting firm, which was costly, slow to respond, and difficult to scale.

To modernize its cybersecurity, reduce costs, and build its own advanced security center, the airport replaced its fragmented security tools with Seceon's AI-driven Open Threat Management (OTM) platform. The transformation enabled the airport to:

- Eliminate reliance on multiple disjointed security tools
- Reduce security costs by 60%
- Build an in-house, AI-powered 24x7 Security Operations Center (SOC)
- Extend cybersecurity services to other critical infrastructure organizations
- Achieve continuous compliance with aviation and government cybersecurity regulations

The Challenge: Securing Critical Infrastructure in a High-Risk Environment

Aviation Cybersecurity Threats

As one of the busiest airports globally, the airport faced constantly evolving cybersecurity risks, including:

- **Nation-State & Advanced Persistent Threats (APTs)** – Sophisticated cyberattacks aimed at disrupting airport operations, stealing passenger data, and targeting national security.
- **Ransomware & Insider Threats** – Potential cyber threats from both external and internal actors that could lead to flight disruptions and sensitive data breaches.
- **IoT & Operational Technology (OT) Vulnerabilities** – Security gaps in baggage systems, air traffic control, airport networks, and automated systems.
- **Compliance Pressure –** Strict regulatory requirements, including TSA, FAA, NIST, GDPR, and ISO 27001, made compliance management a continuous burden.

Limitations of the Existing Security Model

The airport relied on 10 different security tools, including:

- A traditional SIEM – Slow and reactive, creating overwhelming alerts.
- Multiple endpoint protection solutions – Lack of unified visibility and control.
- Firewall and intrusion detection systems (IDS/IPS) – Not effective against zero-day threats.
- Threat intelligence platforms – Data overload without actionable insights.
- Separate compliance tools – Increased complexity and inefficiency.

In addition, the airport had outsourced its 24x7 SOC to a Big Four firm, which led to:

- **High operational costs** – Millions spent annually on outsourced SOC services.
- **Slow incident response times** – Delays in correlating and responding to threats.
- **Limited scalability** – The SOC model did not effectively cover new digital transformation initiatives at the airport.

The Need for a Unified, AI-Powered Security Platform

To modernize cybersecurity and reduce costs, the airport required a single platform that could:

- Replace 10+ security tools with an integrated solution
- Leverage AI to detect and respond to threats in real-time
- Enable the airport to build its own advanced 24x7 SOC
- Support multi-tenancy to offer cybersecurity services to other critical infrastructure organizations
- Ensure continuous compliance with aviation security regulations

The Solution: Seceon's AI-Driven Open Threat Management (OTM) Platform

The airport selected Seceon's OTM platform to consolidate security operations, leveraging:

1. **AI-Driven Threat Detection & Automated Response**
- Real-time AI Behavioral Analytics detected anomalies in:
  - Passenger data systems
  - Airport network traffic
  - IoT devices and baggage systems
- Automated Incident Response blocked threats without human intervention, significantly reducing response times from hours to seconds.

2. **Single Unified Platform Replacing 10+ Security Tools**
- Replaced SIEM, EDR, IDS/IPS, firewall monitoring, threat intelligence, compliance reporting, and log management with a single AI-powered platform.
- Reduced alert fatigue by automatically correlating threat signals across all airport systems.

3. **Building an In-House 24x7 Advanced Security Operations Center (SOC)**
- Seceon's OTM platform enabled the airport to establish its own SOC, eliminating the need for an outsourced Big Four security service provider.
- The new SOC provided:
  - Real-time monitoring & response without third-party delays.
  - Lower operational costs and higher efficiency.
  - Scalability to secure additional critical infrastructure beyond the airport.

4. **Multi-Tenancy for Extending Cybersecurity Services**
- Seceon's multi-tenant architecture allowed the airport's SOC to offer cybersecurity-as-a-service to:
  - Other airports
  - Transportation hubs
  - Critical infrastructure organizations
- Provided a new revenue stream while enhancing nationwide aviation cybersecurity.

5. **Continuous Compliance & Audit Readiness**
- Automated compliance monitoring ensured adherence to:
  - Local regulatory cybersecurity guidelines
  - GDPR & ISO 27001 for data privacy
  - NIST frameworks for critical infrastructure security
- Eliminated manual compliance tracking, reducing audit preparation time by 80%.

Implementation: Seamless Migration to Seceon OTM

Phase 1: Risk Assessment & Security Evaluation

- Seceon's cybersecurity team conducted an extensive evaluation of the airport's existing security gaps and compliance risks.

Phase 2: Deployment & Integration

- Integrated Seceon OTM with the airport's existing network, cloud systems, SaaS services and operational technologies, including:
  - Passenger reservation systems
  - IoT-enabled baggage tracking
  - SaaS based flight data processing

Phase 3: AI-Powered Threat Monitoring & Response

- Within the first month, Seceon's AI detected:
  - A nation-state reconnaissance attack
  - Unauthorized insider access to sensitive passenger data
  - A ransomware attempt targeting critical infrastructure

Phase 4: SOC Expansion & Multi-Tenant Cybersecurity Services

- Established a fully operational in-house SOC, eliminating reliance on external providers.
- Began offering cybersecurity services to other critical infrastructure partners, leveraging Seceon's multi-tenancy feature.

The Results: Transforming Airport Cybersecurity & Cost Savings

1. **Reduced Cybersecurity Costs by 60%**
   - Eliminated 10+ security tools, cutting licensing and operational expenses.
   - Replaced costly outsourced SOC services with an in-house AI-powered SOC.

2. **Faster Incident Detection & Response**
   - Mean time to detect (MTTD) threats reduced by 90%.
   - Automated response blocked threats in seconds, preventing operational disruptions.

3. **Multi-Tenant SOC for Critical Infrastructure Security**
   - The airport's SOC expanded to secure other transportation and aviation hubs.
   - Generated new revenue streams by providing cybersecurity services to partners.

4. **Continuous Compliance & Audit Readiness**
   - Automated compliance reporting eliminated manual audit work.
   - Local cybersecurity guidelines, GDPR, and NIST compliance maintained effortlessly.

Airport Cybersecurity Modernization with seceon

AI-Driven Open Threat Management (OTM) Platform

The Challenge

- 10 Disjointed Security Tools
- High SOC Costs
- Slow Incident Response
- Complex Compliance
- Limited Scalability

Key Cybersecurity Threats

- Nation-State & APTs
- Ransomware & Insider Threats
- IoT & OT Vulnerabilities

The Seceon Solution

- ✓ AI-Driven Threat Detection & Automated Response
- ✓ Unified Platform Replacing 20+ Tools
- ✓ In-House 24x7 Advanced SOC

The Results

60% Cost Reduction

90% Faster Threat Detection

Multi-Tenant SOC for Extended Services

Centralized security for multiple environments

Continuous Compliance with Aviation Regulations

Automated updates for aviation security standards

Conclusion: A New Era of Aviation Cybersecurity

By replacing 10+ security tools with Seceon's AI-driven OTM platform, the airport modernized its cybersecurity, reduced costs, and built its own advanced SOC.

Key Benefits

- AI-Powered, Real-Time Threat Detection & Automated Response
- Eliminated Outsourced SOC Costs by Establishing an In-House Security Center
- Multi-Tenant Security Model Extended to Other Critical Infrastructure Organizations
- Continuous Compliance Monitoring & Audit Readiness

About Seceon

Seceon enables MSPs, MSSPs, and Enterprises to reduce cyber threat risks and their security stack complexity while greatly improving their ability to detect and block threats, and breaches at scale. Seceon's Open Threat Management (OTM) platform augments and automates MSP and MSSP security services with our AI and ML-powered aiSIEM, aiXDR, and aiMSSP platforms. The platform delivers gapless coverage by collecting telemetry from logs, identity management, network logs and flows, endpoints, clouds, and applications. It's all enriched and analyzed in real-time by applying threat intelligence, AI and ML models built on behavioral analysis, and correlation engines to create reliable, transparent detections and alerts. Over 464 partners are reselling and/or running the industry's lowest TCO, efficient security services with automated cyber threat remediation and continuous compliance for over 8,800 clients.