CONCEPT

Aviation Cybersecurity and Intelligent Transport Systems: SOC Monitoring and Incident Response

31 May – 4 June 2027
London - Central London four-star



Aviation Cybersecurity and Intelligent Transport Systems: SOC Monitoring and Incident Response

Ref: 885_20979 **Date:** 31 May – 4 June 2027 **Location:** London - Central London four-star **Fees:** 25300 SAR

Introduction:

Aviation and intelligent transport cybersecurity incidents rarely stay inside IT: ransomware on common-use check-in, a tampered flight data feed or a compromised signal controller contractor can delay departures and gridlock corridors within minutes. Many airports, airlines and transport authorities still watch these environments with office-network rules and have no playbook linking security analysts to duty managers and traffic operators. This Core Concept course builds sector-specific detection, intelligence sharing and response across airport, air navigation and roadway systems. Participants produce a Sector Threat Model and Incident Response Playbook for a case airport or traffic management centre.

Course Objectives:

- Map the cyber attack surface of airport operational systems, passenger processing, airline IT, air traffic management-adjacent links and roadside infrastructure
- Build a mode-specific threat model that links adversary goals to flight, passenger and roadway consequences
- Exchange threat information through aviation and transport sharing communities and convert alerts into monitoring actions
- Design SOC detection use cases and triage criteria for airport and traffic control technology
- Lead incident response that respects the safety-security interface, including manual fallback and operational restriction decisions
- Produce a Sector Threat Model and Incident Response Playbook covering suppliers, restoration sequencing and exercise testing

Target Audience:

- Security operations analysts and incident handlers who monitor airport, airline or transport authority networks
- IT and OT engineers responsible for baggage handling, airfield, signalling and roadside systems
- Airport and airline operations control staff who coordinate service continuity during disruption
- Traffic management centre operators and ITS engineers who run signals, message signs and tolling
- Information security specialists at air navigation service providers who protect data exchanges with airports and airlines

Course Outline:

Day 1: Aviation and Roadway Attack Surface and Sector Adversaries

- Airport Operational System Map: AODB, FIDS, Baggage Handling and Airfield Lighting Interfaces
- Passenger Processing Exposure: Common-Use Check-In, Self-Bag Drop, Boarding Gates and Biometric E-Gates
- Airline IT and Air Traffic Management-Adjacent Links: Reservations, Crew Apps, Flight Planning and Surveillance Data Feeds
- Traffic Control Centre, Roadside Unit, Signal Controller and Connected Vehicle Message Exposure
- Sector Adversary and Incident Review: Airport Ransomware, Navigation Signal Interference, Signage Defacement and Toll Outages

Day 2: Sector Frameworks, Threat Modelling and Intelligence Sharing

- ICAO Annex 17 Cybersecurity Provisions and the Cyber-Safety Interface Principle
- NIST Cybersecurity Framework Functions Applied to Transport Owners and Operators
- MITRE ATT&CK for ICS Techniques Mapped to Baggage, Airfield and Roadside Controllers
- Aviation ISAC and Transport Sharing Communities: Membership, Alert Handling and Reciprocal Reporting
- Mode-Specific Threat Modelling Worksheet: Assets, Entry Points, Adversary Goals and Operational Consequences

Day 3: Transport SOC Monitoring and Detection Use Cases

- Telemetry Sources: AODB Audit Trails, Common-Use Platform Logs, ATC Interface Gateways and Signal Controller Events
- Passive Traffic Monitoring for Baggage Handling and Traffic Signal Networks
- Detection Use Case Catalogue: Unauthorised Vendor Sessions, Flight Data Feed Tampering and Signal Plan Changes
- Alert Triage With Operations Context: Duty Manager, Tower and Traffic Operator Escalation Criteria
- SOC Runbook for Correlating Passenger-Facing Outages With Security Events

Day 4: Incident Response, Supplier Exposure and Restoration of Transport Services

- Airport Cyber Incident Playbook: Check-In Ransomware and Manual Fallback Processing
- Traffic Management Centre Playbook: Hijacked Variable Message Signs and Signal Timing Manipulation
- Safety-Security Decision Rules: When a Cyber Event Triggers Operational Restrictions or Ground Stops
- Third-Party Access Risk: Ground Handlers, Baggage System Integrators, Toll Operators and Cloud Providers
- Restoration Sequencing for Critical Flight, Passenger and Roadway Services

Day 5: Multi-Agency Cyber Exercise and the Sector Threat Model and Playbook

- Case Brief: Hub Airport and Adjoining Urban Traffic Management Centre Under Coordinated Attack
- Timed Injects Simulation: Security Operations, Airport Operations Centre and Traffic Operators
- Sector Threat Model Build for the Case Airport or Traffic Management Centre
- Incident Response Playbook Drafting: Roles, Decision Points, Communications and Recovery Criteria
- After-Action Review and Playbook Defence Before a Mock Crisis Board

Skills You Will Gain:

- Transport Attack Surface Mapping
- Sector Threat Modelling
- Aviation Threat Information Sharing
- Transport OT Detection Engineering
- Operations-Aware Alert Triage
- Cyber-Safety Decision Making
- Transport Supplier Access Control
- Critical Service Restoration Planning

Why Attend This Course:

- Leave with a Sector Threat Model and Incident Response Playbook for a case airport or traffic management centre, tested in a timed exercise
- Give duty managers and traffic operators clear triggers for switching to manual fallback when systems are compromised
- Turn sharing community alerts into detection rules your SOC can run against airport and roadside telemetry
- Compare response practice with peers from airports, airlines, air navigation providers and road and transit authorities

Conclusion:

Airports and road networks keep moving only when security teams understand what each compromised system means for flights, passengers and traffic. The course moves from the aviation and roadway attack surface and sector adversaries, through ICAO Annex 17 provisions, the NIST Cybersecurity Framework, ATT&CK for ICS and sharing communities, to SOC telemetry, detection use cases and operations-aware triage, then playbooks, safety-security decisions, supplier access and restoration. The final day's timed exercise produces a Sector Threat Model and Incident Response Playbook ready for internal adoption.