JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Advanced Aviation Cyber Threat Intelligence and Incident Response Training Course

jupiterprime.uk

info@jupiterprime.uk

Registered in the United Kingdom and Saudi Arabia

Advanced Aviation Cyber Threat Intelligence and Incident Response Training Course

Aviation Cyber Threat Intelligence and Incident Response is a 2-week training course for security operations analysts, incident responders and cyber leads at airlines, airports and air navigation providers, who leave with an aviation cyber incident response playbook for their organisation. Ransomware, supplier compromises and attacks on passenger and operational systems now reach check-in halls and flight schedules within hours, so analysts must read threats in aviation terms. The course is delivered by Jupiter Prime Training.

Why Aviation Cyber Threat Intelligence and Incident Response Matter Now

Three forces raise the stakes for aviation security operations. Criminal groups and state-linked actors target airlines and airports because a single outage creates visible disruption and pressure to pay. Shared community platforms, cloud services and ground handlers widen the attack surface beyond any one organisation's network. Aviation authorities increasingly expect operators to treat cyber events as safety and security risks, with prompt reporting and tested recovery. An organisation that turns intelligence into early detection protects flights, passenger data and reputation; one that reacts late faces cancelled departures and long recovery. The course rests on the intelligence cycle and the incident handling lifecycle of preparation, detection, containment, eradication, recovery and lessons learned.

Who Gains Most from Aviation Cyber Threat Intelligence and Incident Response

- Security operations analysts who triage alerts on airline and airport networks
- Incident responders who contain and investigate compromises of operational systems
- Threat intelligence analysts who track actors targeting the aviation sector
- Cyber security leads who report incidents to executives and authorities
- Operational technology engineers responsible for baggage, gate and airfield systems

An airline or airport gains most when its security operations, incident response and operational technology staff attend together and rehearse one shared playbook.

Aviation Cyber Threat Intelligence and Incident Response Capabilities

Participants practise linking what is known about aviation attackers to the alerts, decisions and recovery steps that keep aircraft moving.

- Build intelligence requirements that reflect flight, passenger and cargo risks — chief information security officer
- Assess threat actor profiles and their tactics against aviation systems — security operations leads
- Design detection rules for departure control, airport operational and operational technology networks — detection engineers
- Apply containment decisions that balance security and flight continuity — duty managers and operations control
- Test recovery sequences for passenger and operational systems — IT service owners
- Communicate incident status to executives, authorities and partners — crisis management team

Key Aviation Cyber Threat Intelligence and Incident Response Terms

- Cyber threat intelligence CTI — analysed information about attackers, their intent and methods, used to guide defensive decisions.
- Indicator of compromise IOC — a technical sign, such as a file hash or address, that a system may have been breached.
- Tactics, techniques and procedures TTPs — the patterns of behaviour an attacker uses to achieve objectives.
- Detection engineering — the design, testing and tuning of rules that turn log data into reliable security alerts.
- Containment — actions that limit an attacker's spread while keeping essential operations running.
- Incident response playbook — a pre-agreed sequence of roles, steps and decisions for a specific type of cyber incident.

Aviation Cyber Threat Intelligence and Incident Response Day by Day

Day 1: The Aviation Cyber Threat Landscape

- Aviation Attack Surface Map — Airline, Airport and Navigation Systems
- Ransomware and Extortion Trends — Impact on Check-In and Baggage
- Supply Chain Compromise Cases — Shared Platforms and Service Providers
- Operational Technology Exposure — Airfield Lighting, Gates and Building Systems
- Cyber Risk as Safety Risk — Links to Operational Disruption

Day 2: Intelligence Requirements and Collection

- Intelligence Cycle Planning — Questions Leaders Need Answered
- Priority Intelligence Requirements — Flight, Passenger and Cargo Risks
- Open, Commercial and Sector Sources — Reliability and Coverage
- Information Sharing Communities — Trusted Exchange With Aviation Peers
- Source Grading and Handling Rules — Confidence and Sharing Limits

Day 3: Threat Actor Analysis

- Threat Actor Profiling — Motives, Capability and Targeting of Aviation
- TTP Mapping — Matching Attacker Behaviour to Defensive Gaps
- Campaign Tracking — Linking Incidents Across Organisations
- Analytical Techniques — Competing Hypotheses and Bias Checks
- Intelligence Reporting Formats — Tactical, Operational and Strategic Products

Day 4: Detection Engineering

- Log Source Coverage — Passenger Systems, Networks and Endpoints
- Detection Rule Design — Turning TTPs Into Alerts
- Operational Technology Monitoring — Passive Sensors and Baselines
- Alert Tuning — False Positive Reduction Without Blind Spots
- Threat Hunting Hypotheses — Searching for Undetected Intrusions

Day 5: Security Operations Centre Workflows

- Alert Triage Criteria — Severity Linked to Flight Impact
- Escalation Paths — From Analyst to Incident Commander
- Case Management Records — Evidence and Timeline Integrity
- Shift Handover in the SOC — Continuity During Long Incidents
- SOC Performance Measures — Detection and Response Times

Day 6: Incident Handling and Containment

- Incident Handling Lifecycle — Preparation Through Lessons Learned
- Incident Classification — Categories and Severity for Aviation Events
- Containment Options — Isolation Versus Continued Operation
- Coordination With Operations Control — Manual Fallback Decisions
- Third-Party Incident Coordination — Vendors and Community Platforms

Day 7: Digital Forensics and Eradication

- Evidence Acquisition — Memory, Disk and Log Preservation
- Malware Triage — Behaviour Analysis for Response Decisions
- Root Cause Determination — Initial Access and Lateral Movement
- Eradication Planning — Credential Resets and Rebuilds
- Chain of Custody — Evidence for Legal and Insurance Needs

Day 8: Recovery of Operational Aviation Systems

- Recovery Priority Ranking — Flight-Critical Versus Business Systems
- Restore and Validation Steps — Clean Backups and Integrity Checks
- Manual Operations Procedures — Paper Check-In and Load Sheets
- Business Continuity Coordination — Airline and Airport Partners
- Return-to-Service Criteria — Confidence Before Reconnection

Day 9: Crisis Communication and Reporting

- Executive Briefing Templates — Impact, Options and Decisions
- Authority Notification Workflow — Timelines and Content
- Passenger and Media Messaging — Accuracy Under Pressure
- Ransom and Extortion Decision Factors — Legal and Ethical Considerations
- Post-Incident Review — Lessons Fed Back Into Intelligence

Day 10: Practising the Aviation Cyber Incident Response Playbook

- Ransomware on Departure Control Exercise — Applying Containment and Recovery Steps
- Supplier Breach Exercise — Applying Third-Party Coordination
- Threat Hunt Simulation — Applying Detection Rules and TTP Mapping
- Executive Crisis Briefing Drill — Applying Reporting Templates
- Aviation Cyber Incident Response Playbook — Roles, Triggers and Recovery Order

Applying Aviation Cyber Threat Intelligence and Incident Response After the Course

- Write three priority intelligence requirements with operations leaders and map current detection coverage against them.
- Run a tabletop exercise on a ransomware attack against passenger systems with operations control and IT service owners.

Aviation Cyber Threat Intelligence and Incident Response Questions FAQ

What is aviation cyber threat intelligence and incident response, and why does it matter now?

Aviation cyber threat intelligence and incident response is the practice of tracking attackers who target airlines and airports and handling the incidents they cause. It matters now because ransomware and supplier compromises can halt check-in, baggage and flight planning within hours.

Which roles gain most from aviation cyber threat intelligence and incident response training?

Security operations analysts and incident responders gain most, followed by threat intelligence analysts, cyber security leads and operational technology engineers. If you detect, contain or report attacks on aviation systems, you gain a shared method and vocabulary.

How does aviation cyber threat intelligence and incident response training differ from a general cyber security course?

It applies intelligence and response methods to the systems that keep flights moving. A general cyber security course covers controls broadly; this course works through departure control, airport operational and operational technology incidents and the manual fallback they require.

What do you bring back from aviation cyber threat intelligence and incident response training?

You bring back a tested playbook that sets roles, detection triggers, containment choices and recovery order for aviation incidents. It gives your security and operations staff one plan to follow under pressure.

Aviation Cyber Threat Intelligence and Incident Response: The Way Forward

The aviation cyber incident response playbook first informs who declares an incident and which systems are isolated or kept running. Security operations leads, incident commanders and operations control staff use it during every major alert. After the first exercise or real event, revisit the recovery order and detection triggers against what actually happened.