International Civil Aviation Organization

WORKING PAPER

ATConf/7-WP/201
21/10/26
(Information Paper)
English only

SEVENTH WORLDWIDE AIR TRANSPORT CONFERENCE (ATCONF/7)

Montréal, HQ, 16 to 20 November 2026

Agenda Item 4: Emerging technologies, new business models and other associated aspects
4.3: Leveraging air transport data and the digital ecosystem for seamless, secure and resilient operations

AUTOMATED & CORRELATED THREAT INTELLIGENCE PLATFORM TO ENHANCE CYBERSECURITY IN AVIATION SECTOR FOR SEAMLESS, SECURE & RESILIENT OPERATIONS

(Presented by India)

EXECUTIVE SUMMARY

This working paper addresses the incorporation of Emerging technologies like Artificial Intelligence (AI) models and Automation to support seamless, secure & resilient cybersecurity operations.

This paper presents the leveraging of enriched & correlated threat intelligence model towards establishing automated Correlated Threat Intelligence Platform (CTIP)to Enhance Cybersecurity in Aviation Sector.

AI model-based threat intelligence collaboration platform enables organization to anticipate threats, detect attacks early, respond faster, recover efficiently, and continuously improve their security posture. Rather than relying entirely on predefined rules and manual monitoring, AI can analyze large volumes of security data, identify abnormal patterns, and support security teams in making faster, risk-informed decisions.

The emphasis is placed on building interoperable, accessible cybersecurity ecosystem that strengthen oversight and enables provides predictive threat intelligence across the aviation system.

1. INTRODUCTION

1.1 This working paper aims to develop an action plan to support States and industry in the adoption of the Emerging technologies to strengthen the Aviation Cybersecurity Strategy. Accordingly, the proposed action plan complements the International Civil Aviation Organization (ICAO) developed the Cybersecurity Action Plan (CyAP).

1.2 The CyAP provides the foundation for ICAO, States and stakeholders to work together, and proposes a series of principles, measures, and actions to achieve the objectives of the Aviation Cybersecurity Strategy's seven pillars, namely –

a) International cooperation
b) Governance
c) Effective legislation and regulations
d) Cybersecurity Policy
e) Information sharing
f) Incident management and emergency planning
g) Capacity building, training and cybersecurity culture

1.3 To that end, the CyAP develops the pillars of the Strategy into 32 Priority Actions, which are further broken down into 51 tasks to be implemented by ICAO, States, and stakeholders.

1.4 Pillar 2 – Governance mentions "*Ensure coordination at the State level between Civil Aviation authorities and the competent national authorities for cybersecurity*"

1.5 Pillar 5 – Information Sharing mentions "Develop or leverage existing sharing of information platforms and mechanisms which are recognized, in line with existing ICAO provisions, ***to enable cyber situational awareness thus allowing prevention, early detection and mitigation of relevant cybersecurity events."***

1.6 This working paper presents building Automated & Correlated Threat Intelligence Platform (ACTIIP) to Enhance Cybersecurity in Aviation Sector and enable cyber situational awareness thus allowing prevention, early detection and mitigation of relevant cybersecurity events.

1.7 This paper is an attempt to meet the measure(s) under CyAP 2.4 - Promote coordination mechanisms between civil aviation authorities and cybersecurity authorities and CyAP 5.2– ICAO, with support of the Member States and Industry, to identify cybersecurity-related information sharing, collaboration needs (including but not limited to times of crisis), and policies.

2. BACKGROUND

2.1 Building Automated Correlated Threat Intelligence Platform to Enhance Cybersecurity in Aviation Sector

2.1.1 A Correlated Threat Intelligence Platform (CTIP) is a solution that aggregates, correlates, and analyzes threat data from various sources to provide participating organizations with actionable insights, helping them to detect, prioritize, and respond to cyber threats more effectively.

2.1.2 CTIPs collect threat data from multiple sources, including internal security systems, external threat feeds, and open-source intelligence, and then correlate this data to identify patterns and relationships between threats.

2.1.3 Major Challenges in manual and non-collaborated CTIP are Data Overload, Lack of contextual information, Timely threat detection & response and Integration with existing security tools.

2.1.4 Overcoming these common challenges in threat intelligence requires a combination of advanced technologies, comprehensive data analysis, real-time monitoring, and seamless integration with existing security systems.

3. PROPOSED AUTOMATED CORRELATED THREAT INTELLIGENCE PLATFORM (TIP) AND VALIDATION

3.1 The platform functions as a trusted intelligence exchange connecting aviation stakeholders through standardized, secure and timely data-sharing mechanisms. Correlated CTIPs collect threat intelligence from engineered to provide robust mechanism for two-way exchange of Threat Intelligence and cybersecurity related information between the participating organizations and thus develop/ leverage sharing of information platforms which already exists in the various cybersecurity devices implemented in the organizations.

3.1.1 **Layer 1** — Aviation intelligence sources: Airport Security Operations Centers (SOCs), Airlines, Air Navigation Service Providers (ANSPs), Regulators, Computer Emergency Response Teams (CERTs), Cloud and data centers, Original Equipment Manufacturers (OEMs), Technology and service providers

3.1.2 **Layer 2** — Secure data ingestion and interoperability: Threat feeds, Advance Passenger Information (APIs), Structured Threat Information eXpression (STIX)/ Trusted Automated Exchange of Intelligence Information(TAXII), Incident reports, Vulnerability data, Asset and dependency context

3.1.3 **Layer 3** — Intelligence fusion and analytics: Deduplication, Context enrichment, Threat actor and Tactics, Techniques, and Procedures (TTP) analysis, AI-assisted correlation, Risk scoring

3.1.4 **Layer 4** — Aviation threat intelligence services: Early warnings, Sector-specific advisories, Risk dashboards, Vulnerability prioritization, Incident coordination

3.1.5 **Layer 5** — Coordinated action and resilience: SOC action, Risk-based remediation, Continuity planning, Recovery coordination, Oversight reporting

3.1.6 Feedback from incidents, investigations, and remediation improves subsequent intelligence.

3.2 The true positive threat intelligence generated in one organization/ Member State can be leveraged through the CTIPs across Organizations/ Member States. This shall promote coordination mechanisms between civil aviation authorities and cybersecurity authorities within/ between the State(s) and industries.

3.3 The CTIPs can be centrally correlated to enrich the threat intelligence as a whole and provide aviation sector specific early warning signals.

3.4 Such correlated threat intelligence eventually shall create an Adaptive Cyber Defence Framework (ACDF) for Civil Aviation sector. AI based Cyber Threats are growing rapidly and there is a strong need for a sustainable AI based cyber threat intelligence framework at the international, regional and national levels.

4. GLOBAL GOVERNANCE AND ECOSYSTEM BENEFITS

4.1 By consolidating threat intelligence, vulnerability information, incident reports, and relevant operational risk data, the platform will facilitate early threat identification, intelligence-led risk assessments, coordinated incident response, and proactive mitigation of emerging cyber risks.

4.2 AI-enabled analytics will support threat correlation, risk prioritization, and the generation of actionable security advisories. Standardized data exchange mechanisms, appropriate access controls, and defined information-sharing protocols will ensure interoperability, confidentiality, and accountability.

5. CONCLUSION

5.1 The Conference is invited to take note of the information contained in this paper.

— END —