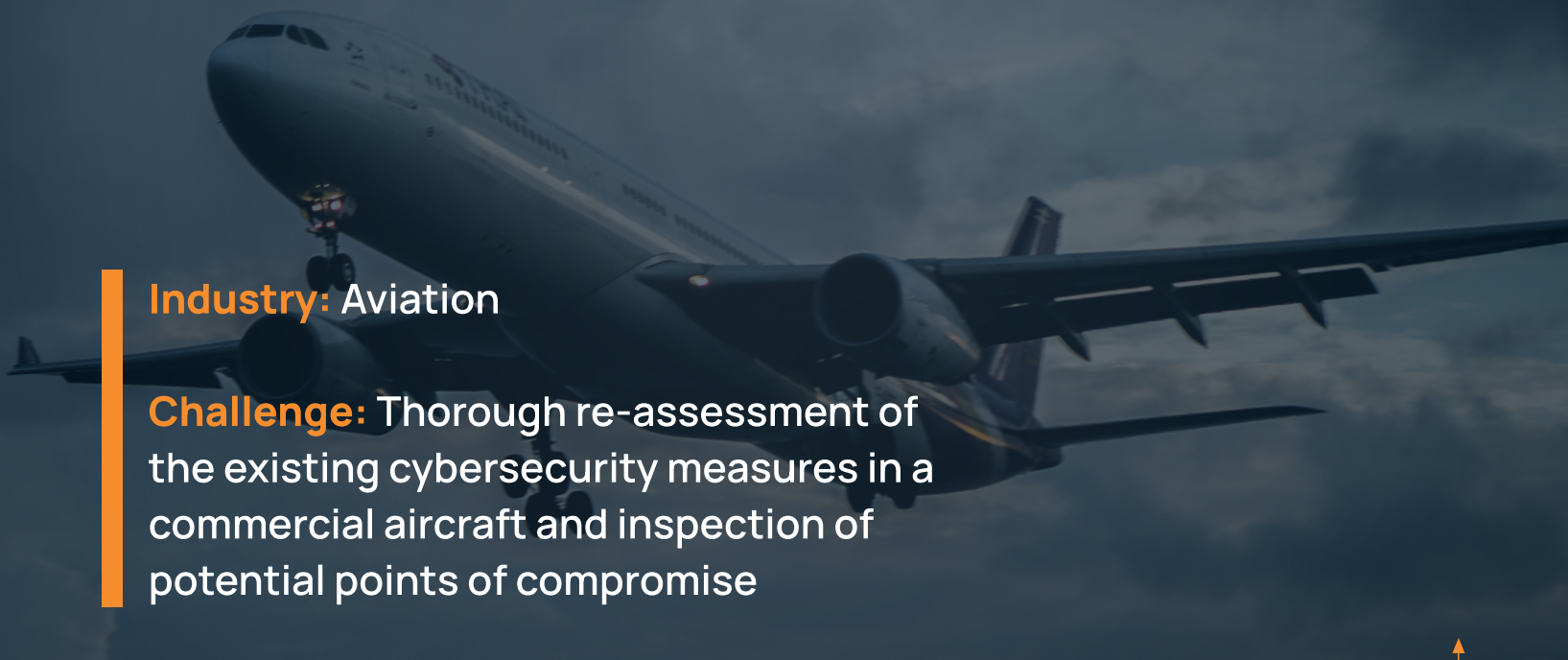
PRODAFT

CASE STUDY

ASSESSING A PASSENGER AIRCRAFT WITH OUR INTELLIGENCE-DRIVEN SECURITY



Industry: Aviation

Challenge: Thorough re-assessment of the existing cybersecurity measures in a commercial aircraft and inspection of potential points of compromise

Who is the Client?

A large-scale airline company that has been ranked among the top 10 biggest airlines in the world.

What Was Their Struggle?

The client needed to make sure that their aircraft are safe and attack-proof, shall there be any cybersecurity compromise targeting them. Our objective at PRODAFT was to conduct a threat intelligence-driven cybersecurity assessment of their commercial aircraft to find out any potential areas of compromise.

What Were Their Main Challenges?

As we sat down together, we managed to pinpoint the most important challenges that needed to be addressed adequately:

- Facing a lack of available resources and practices within the industry for assessing the airlines' cybersecurity position.
- Dealing with regulatory and budgetary constraints that result in limited actual testing time.
- Understanding a wide array of vendors and third parties that have to be analyzed from a supply-chain perspective.
- Overcoming the physically isolated nature of internal and external aircraft networks originally manufactured to protect avionics from external threats.

How Were We Able to Help Them?

Within the framework of this project, our PTI (PRODAFT Threat Intelligence) and Penetration Testing Teams have evaluated out-of-band risks against a passenger aircraft, primarily focusing on threats that pose significant risks against safe and seamless flight operations.

What Was Needed?

Duration

1 Week of Remote Analysis;
2 Days of On-Site Testing on Aircraft (Passenger and Service Areas)

Tool

Threat Intelligence Platform (as the main source of intelligence)

Manpower

2 Senior specialists from our Threat Intelligence (PTI) Team
2 Senior Specialists from our Penetration Testing Team

What Were the Main Findings?

Credential Leak Detection

Various third-party vendors' credential leaks were detected. We are talking about value-added services such as airport planning and automation, in-flight entertainment, and logistics of meal and food delivery providers. These leaks have been observed as actively circulating among the threat actors and therefore possible to be exploited at any given time, regardless of the security mechanisms in place.

Detection of Crucial Vulnerabilities

Multiple vulnerabilities in update and firmware management services were detected. The services had been provided by globally recognized aircraft parts manufacturers, therefore could be considered a systemic risk on a global scale.

Insufficient "IFE" protection

After the physical analysis of the aircraft, it was explored that there was a possibility to access and take over full control of all the IFE (In-Flight Entertainment) systems.

- **Future points of compromise**

We observed multiple data leaks, compromised credentials and tailored-access operations against the leading in-flight vendors in the industry. After a careful evaluation, those findings could allow any threat actors to deploy malicious updates in the IFE systems, change the content of all media and lead to global disruptions in content management operations. On top of that, if those techniques are used in combination with scenarios that aim to spread panic during the flight, such as deploying psychologically challenging and falsified content, such findings need to be addressed accordingly for safe flight operations and overall brand reputation.

What Was the Outcome?

Due to this research being conducted, it was possible to discover multiple third-party risks present in the aviation industry. Although there are undoubtedly high standards for the security of avionic systems and crew safety, our rigorous assessment allowed the client to comprehend potential scenarios that could compromise flight safety. The scenarios were based on real tactics, techniques, and procedures that cybercriminals use to gain unauthorized access, especially without accessing any flight instruments and navigation per se.

Do you want to learn more about how such an assessment could contribute to the safety of your organization in the aviation industry?
Then do not hesitate to contact us to learn more about our intelligence-driven penetration testing.