
IATA
WORLD
DATA
SYMPOSIUM
Singapore
8 – 9 April 2026
#IATAWDS
IATA

IATA
WORLD
DATA
SYMPOSIUM

Newworks
SOLUTION

Welcome to the Cybersecurity Runway

Ewa Pilat
Chief Information Security Officer, IATA

#IATAWDS

IATA

IATA
WORLD
DATA
SYMPOSIUM

Newworks
SOLUTION

Competition Law Guidelines

Do not discuss:

- Any element of prices, including service charges or remunerations
- Allocations of customers or markets
- Your company's marketing plans, commercial terms or any other strategic decision
- Group boycotts
- Your commercial relations with airlines, fuel suppliers, service providers or any other third parties
- Any other issue aimed at influencing the independent business decisions of competitors

IATA

IATA
WORLD
DATA
SYMPOSIUM

Newworks
SOLUTION

Stay Connected

WIFI

ID:IATAWDS2026

Password: IATAWDS2026

#IATAWDS

IATA

IATA
WORLD
DATA
SYMPOSIUM

Newworks
SOLUTION

Download the Event App!

Apple Store

Google Play

#IATAWDS

IATA

IATA WORLD DATA SYMPOSIUM

With many thanks to all our sponsors

Official Airline Partner

Supporting Organization

Gold Sponsors

Silver Sponsors

Bronze Sponsors

Exhibitors

Silver Media Partners

#IATAWDS

IATA
WORLD
DATA
SYMPOSIUM

Newworks
SOLUTION

Cleared for Takeoff

Doug Blough
Senior Product Security Analyst, Boeing

#IATAWDS

IATA

IATA
WORLD
DATA
SYMPOSIUM

Newworks
SOLUTION

From Cybersecurity to Aviation Resilience

Mehdi Ayari
Chief Product Security Officer and Head of Space Product Security, Airbus Defense and Space

#IATAWDS

IATA

From Cybersecurity to Aviation Resilience

Building an Aviation Security Continuum

AIRBUS

From Cybersecurity to Aviation Resilience

Building an Aviation Security Continuum

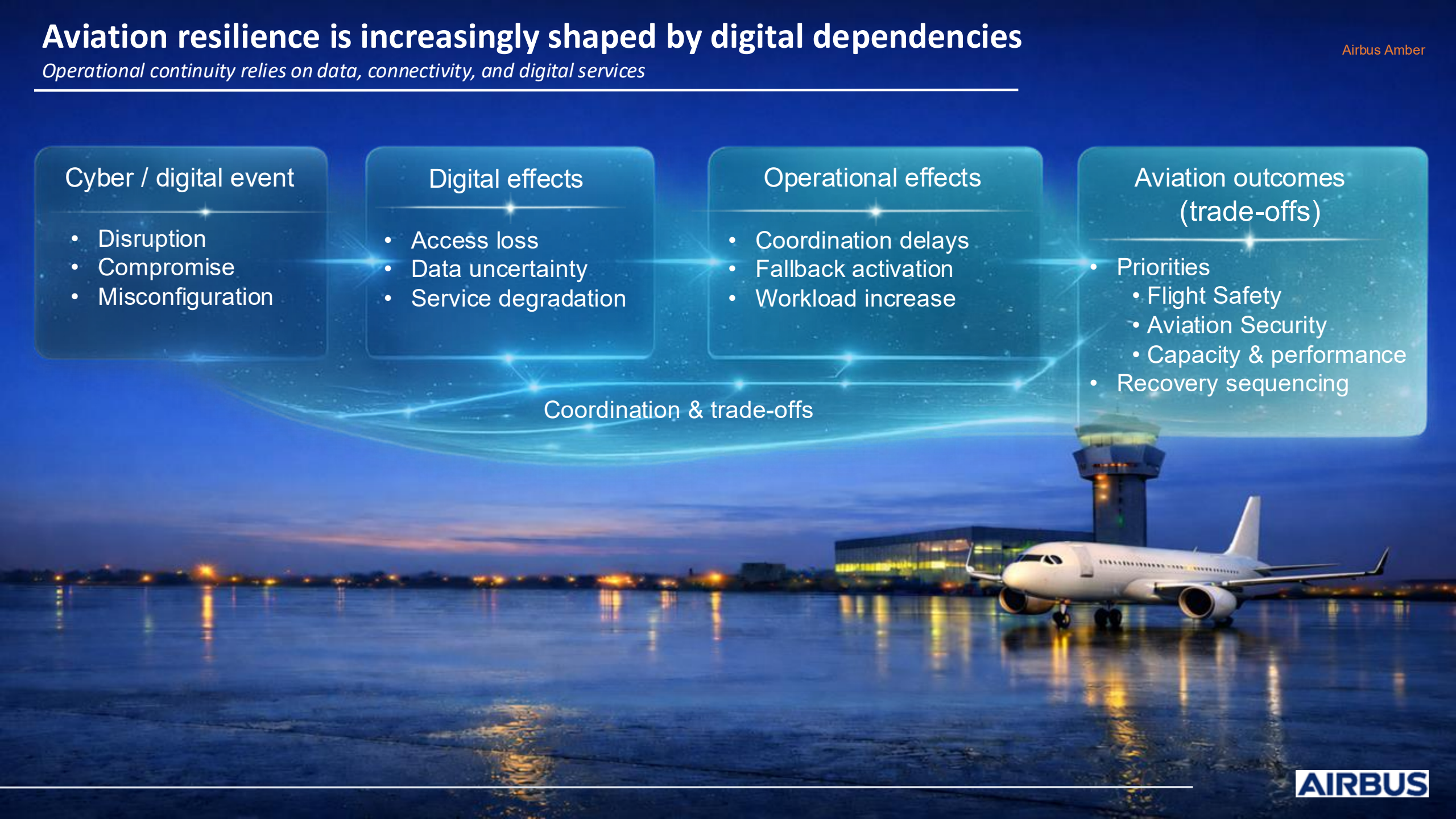
Airbus Amber

AIRBUS

Aviation resilience is increasingly shaped by digital dependencies

Operational continuity relies on data, connectivity, and digital services

Airbus Amber



AIRBUS

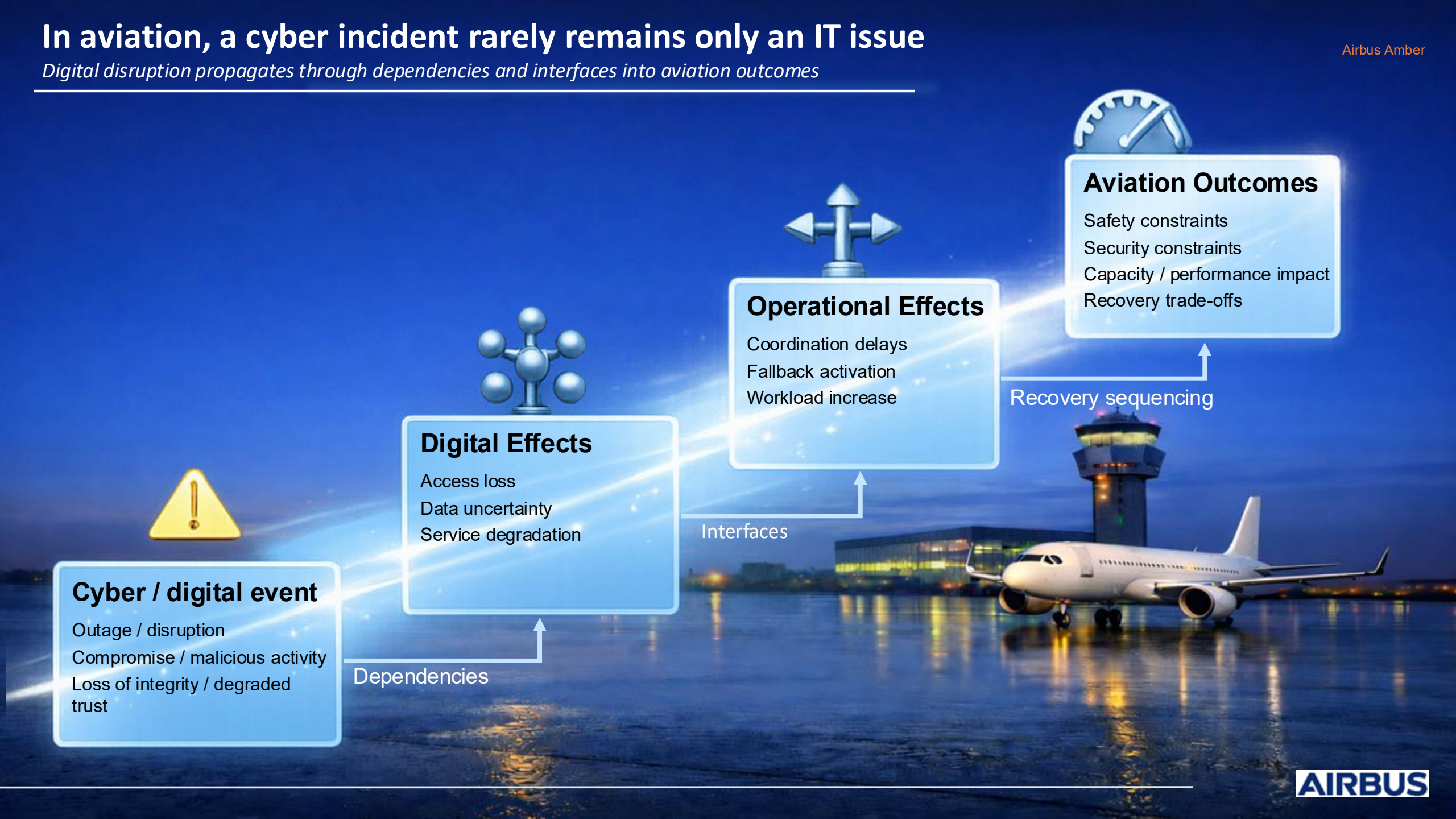
From uncertain data to trusted decisions and safe fallback

Operational reality: digital is a common decision and coordination node

In aviation, a cyber incident rarely remains only an IT issue

Digital disruption propagates through dependencies and interfaces into aviation outcomes

Airbus Amber

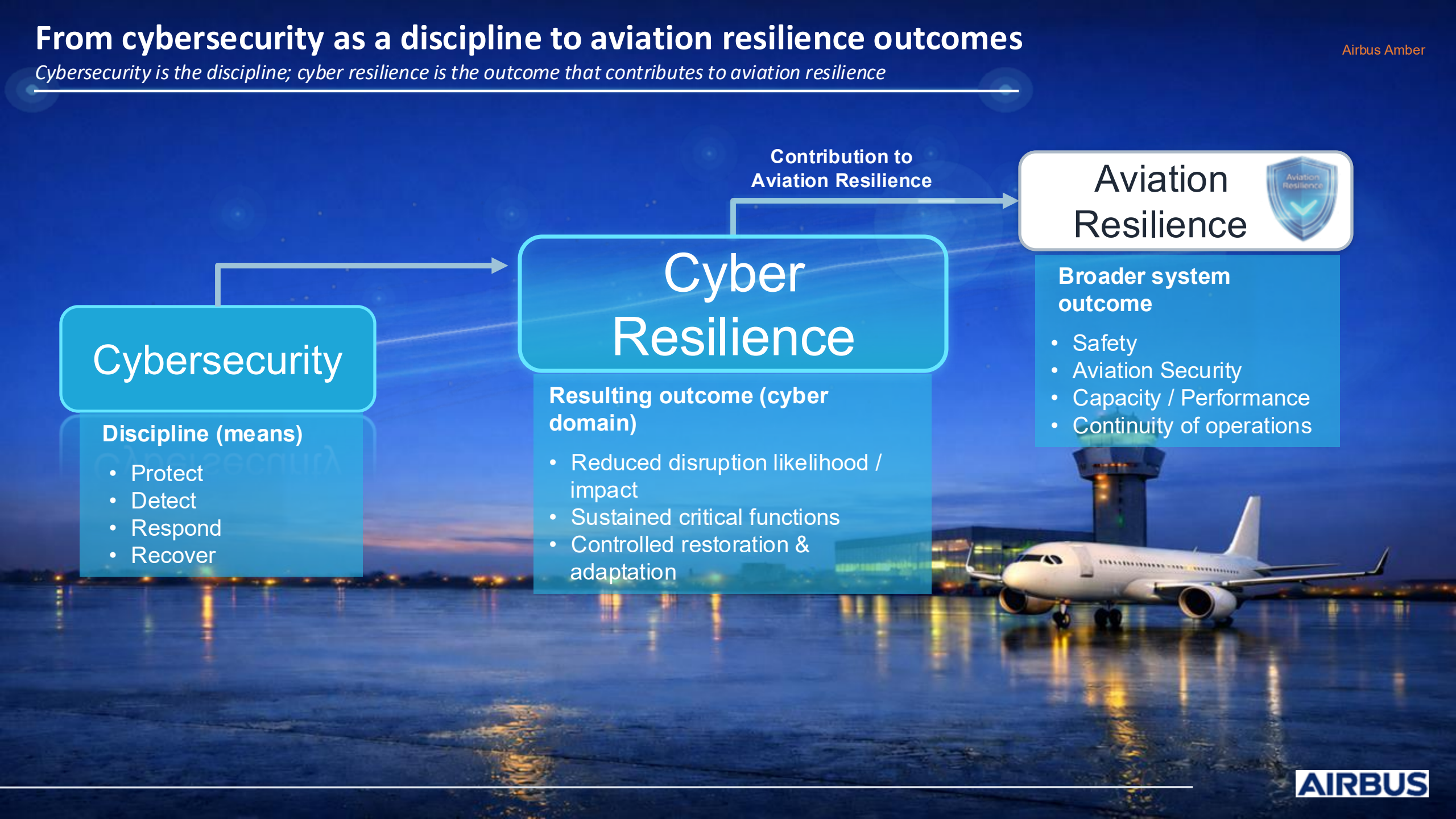


AIRBUS

From cybersecurity as a discipline to aviation resilience outcomes

Cybersecurity is the discipline; cyber resilience is the outcome that contributes to aviation resilience

Airbus Amber



Contribution to Aviation Resilience

Cybersecurity

Discipline (means)

- Protect
- Detect
- Respond
- Recover

Cyber Resilience

Resulting outcome (cyber domain)

- Reduced disruption likelihood / impact
- Sustained critical functions
- Controlled restoration & adaptation

Aviation Resilience

Broader system outcome

- Safety
- Aviation Security
- Capacity / Performance
- Continuity of operations

AIRBUS

Cyber resilience contributes to aviation resilience through critical interfaces

This contribution is enabled through coordinated interfaces with Flight Safety, Aviation Security and Capacity & Performance

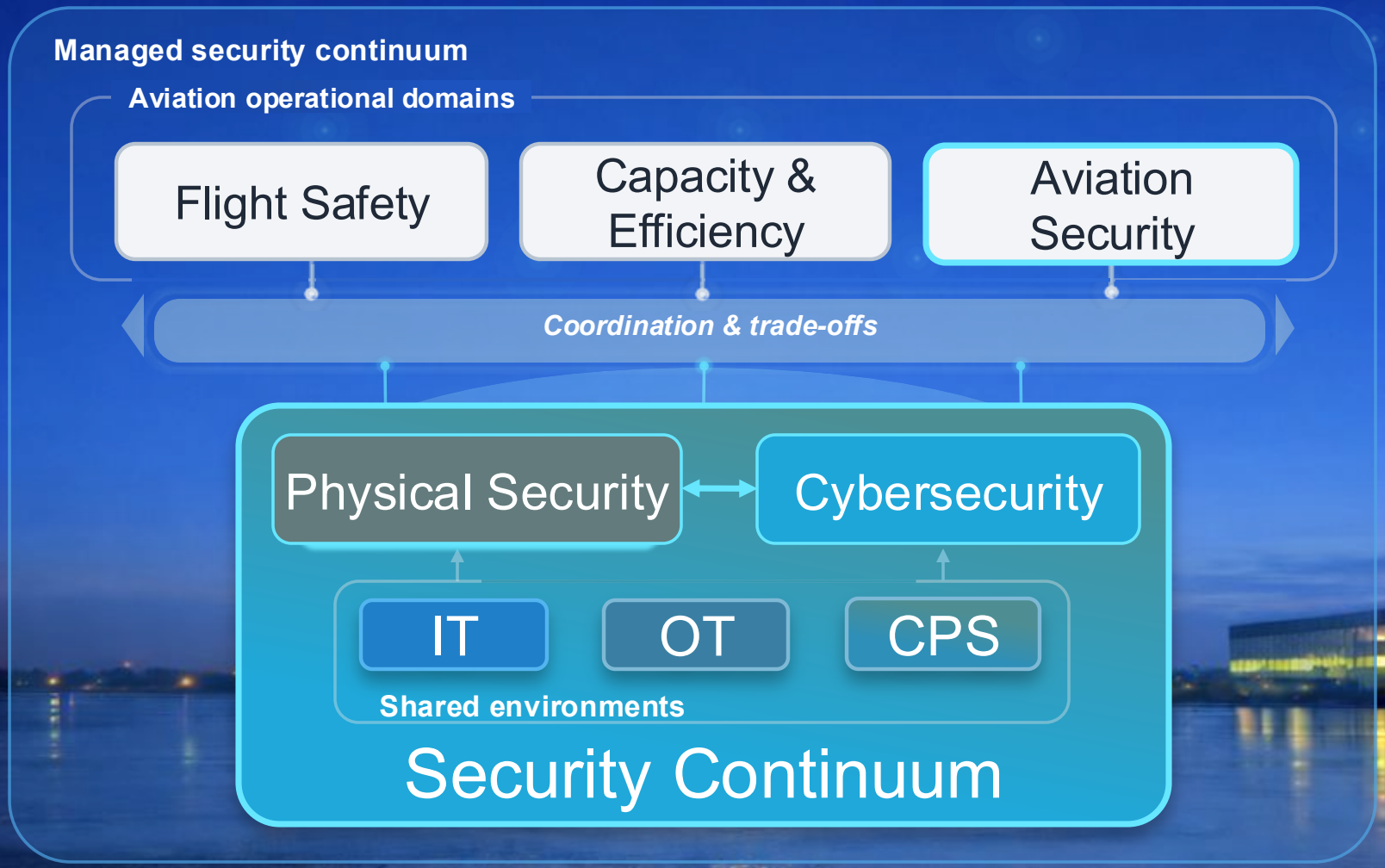
Airbus Amber

AIRBUS

Security continuum: integrating cyber, physical and cyber-physical security

Security coordination across cyber, physical and cyber-physical domains

Airbus Amber

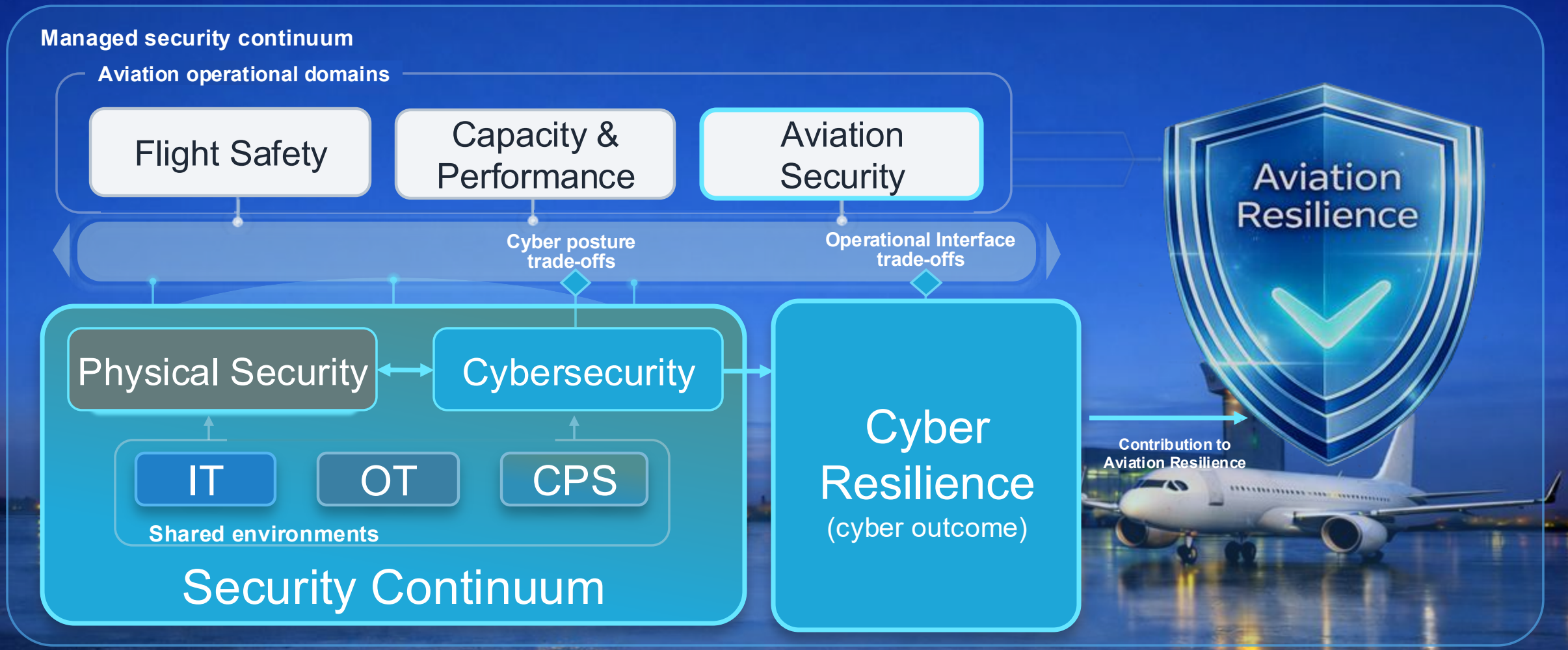


AIRBUS

Security continuum: integrating cyber, physical and cyber-physical security

Security continuum in practice: operational interfaces trade-offs

Airbus Amber



The five interfaces that matter

Operationalized cyber resilience depends on how these interfaces are governed across cybersecurity, operations and recovery

Airbus Amber

Critical interfaces to govern

Architecture & dependencies
What depends on what

Change control & configuration
Posture and design changes

Monitoring & response
Detection, escalation, action

Third-party & supply chain
External dependencies & assurance

Continuity & crisis management
Fallback, sequencing, recovery

Why these interfaces matter

- **Delays and misalignment** emerge here
- Trade-offs are shaped here
- **Resilience outc**omes are determined here

Governance implications

Each interface needs ownership, decision rights and escalation paths

AIRBUS

What must change to operationalize cyber resilience

Shift from technical ownership to cross-functional operating governance

Airbus Amber

Traditional model

- Siloed cybersecurity decisions
- Technical severity over operational impact
- Late operational engagement
- IT-first recovery logic

Operationalized resilience model

- **Shared operational governance**
- Defined trade-off **gates**
- **Early cross functional escalation**
- **Aviation-criticality-led** recovery

Cyber resilience becomes operational when operational domains are built into it — and disruption is governed in operations

AIRBUS

What operationalized cyber resilience requires in practice

It depends on explicit interface governance across cybersecurity, operations and recovery

Airbus Amber

5 mechanisms

Interface ownership
Named owners across cyber and operations

Decision gates & triggers
Predefined gates & escalation triggers

Operational impact assessment
Trade-offs assessed against Safety, AVSEC and Performance

Fallback & recovery orchestration
Fallback modes and recovery sequencing by aviation criticality

Rehearsal & continuous improvement
Exercises, reviews and governance updates

Minimum governance outputs

- Named interface owners and decision rights
- **Gate criteria** and escalation triggers
- **Fallback & recovery playbooks**
- **Exercise and review cadence**

Cyber resilience is made operational through **governed interfaces.**

AIRBUS

From cybersecurity to aviation resilience

Cyber resilience contributes to aviation resilience through governed interfaces and operational trade-offs

Thank you

AIRBUS

IATA
WORLD
DATA
SYMPOSIUM

Newworks
SOLUTION

Panel Discussion

Navigating Today's Turbulence, Securing Tomorrow's Skies

#IATAWDS

IATA

IATA WORLD DATA SYMPOSIUM

Navigating Today's Turbulence, Securing Tomorrow's Skies

Newworks SOLUTION

Moderator

Bruno Spada

CISO,
Amadeus

Masaya Fukushima

Vice President,
Japan Airlines

Prabh Sharan Singh

Vice President,
Coforge

#IATAWDS

IATA

IATA
WORLD
DATA
SYMPOSIUM

Newworks
SOLUTION

Sponsored by:

accelya

Networking Break

Location: Exhibition Hall
The next session starts at 16:00

#IATAWDS

IATA

IATA
WORLD
DATA
SYMPOSIUM

Newworks
SOLUTION

From Cockpit to Cloud: Protecting Digital Aviation in a Connected World

Chris Gorton
Cyber Security Certification Lead, UK Civil Aviation Authority

#IATAWDS

IATA

From Cockpit to Cloud:

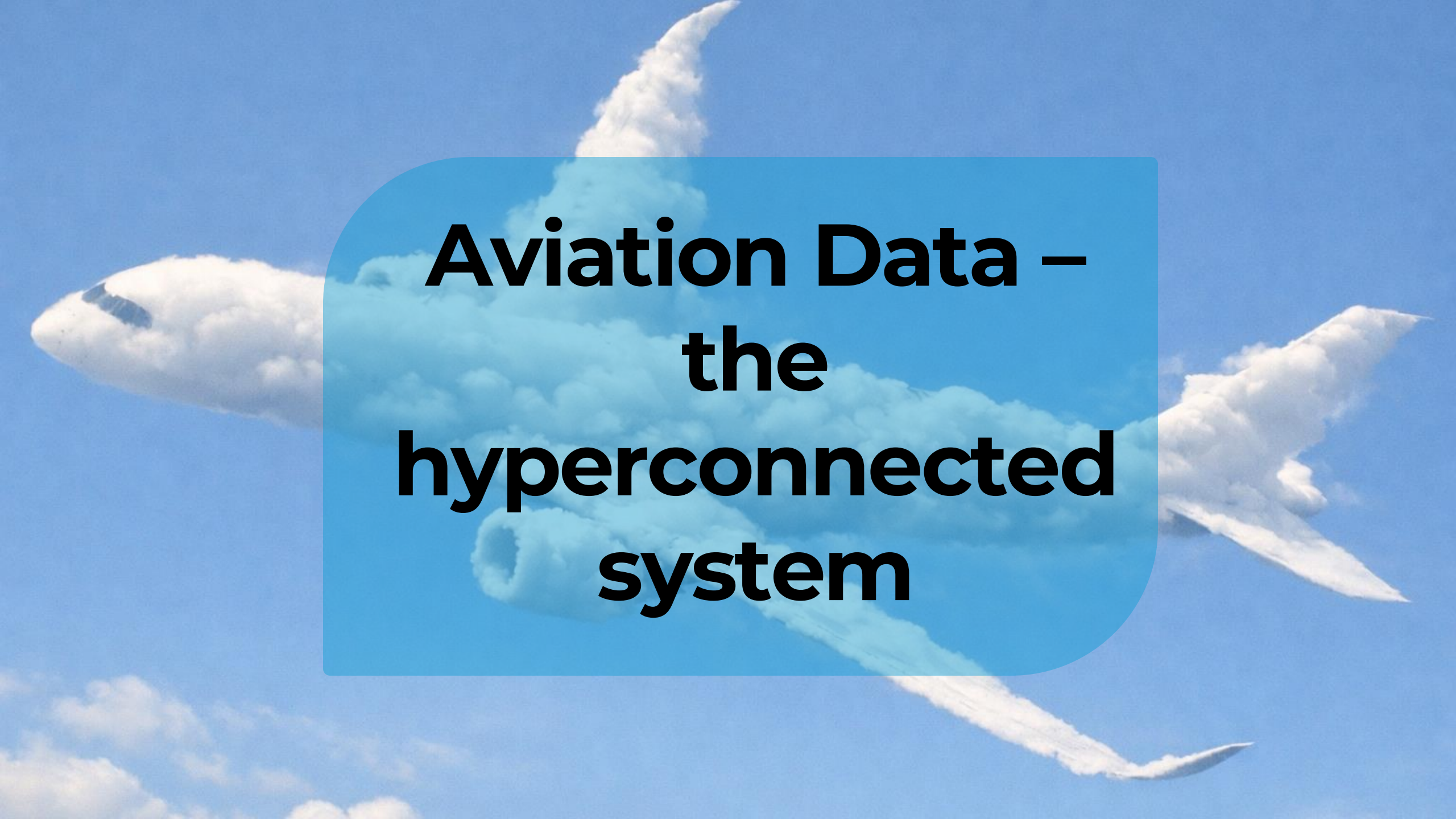
Protecting Digital Aviation in a Connected World

Chris Gorton
Cyber Security Certification Lead
UK CAA


Ready for take-off

1950

2015


Aviation Data –
the
hyperconnected
system

The revolution in connectivity has come to aviation in the form of the Connected Aircraft

TURNING AIRCRAFT-AS-A-PLATFORM VISION INTO A REALITY

THE FUTURE OF AEROSPACE IS MORE CONNECTED

DATA GENERATED BY A MODERN AIRLINER

HUNDREDS OF SENSORS

REAL-TIME MONITORING

50+ TERABYTES
OF DATA PER FLIGHT

GE GENX:
~5,000
DATA POINTS PER SECOND

PRATT & WHITNEY PW1000G:
UP TO 10 GB
OF DATA PER SECOND

OVER 300,000
MONITORED PARAMETERS

- ICAO Connected Aircraft Concept
- Air-Ground Information Exchange
- Many different data sources:
  - EFB
  - CPDLC
  - Weather / Turbulence Data
  - ADS-B & ADS-C
  - Gatelink
  - Sat Comms
  - ACARS

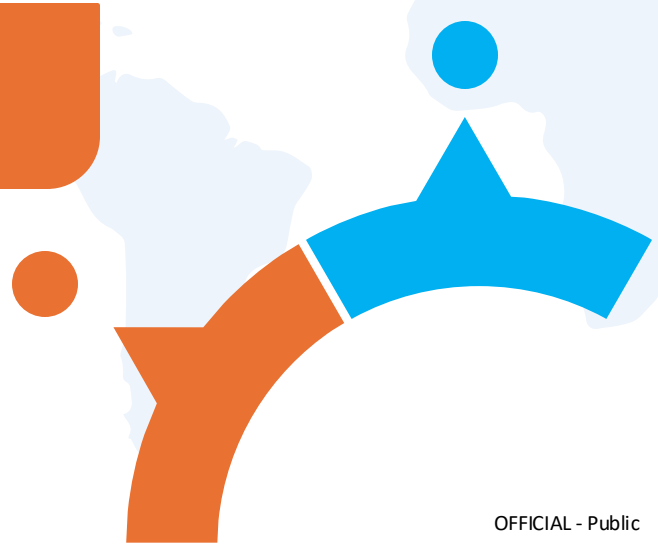
Health Monitoring Systems

The future of predictive maintenance

Aircraft System Monitoring

"After the 2008 crash of Spanair flight 5022, it was discovered that a central airline computer system used to monitor technical problems in the aircraft was infected with malware."

EFB



The Role Of EFBs

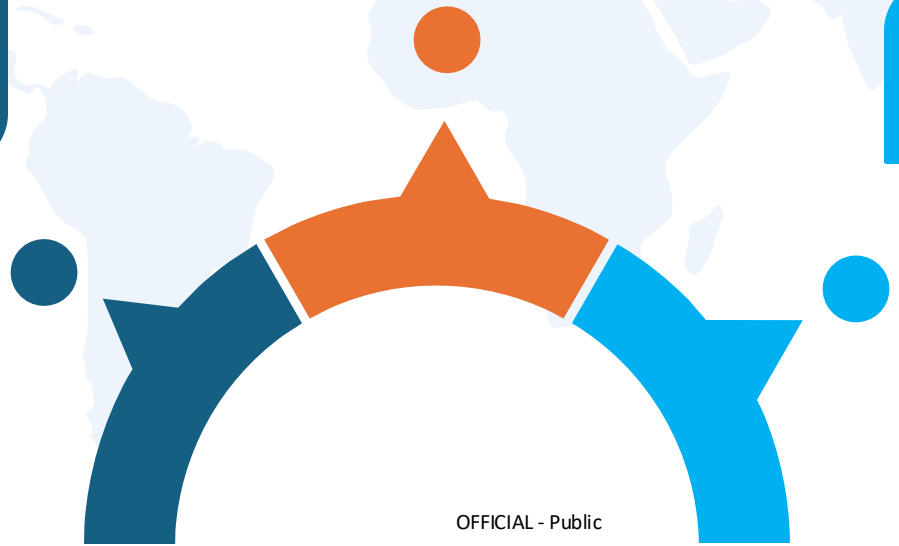
Ever Evolving!!

Take-off Performance Calculations

Thankfully, errors normally caught in cross-check, but could performance data be altered without crew knowledge?

EDB

HMS

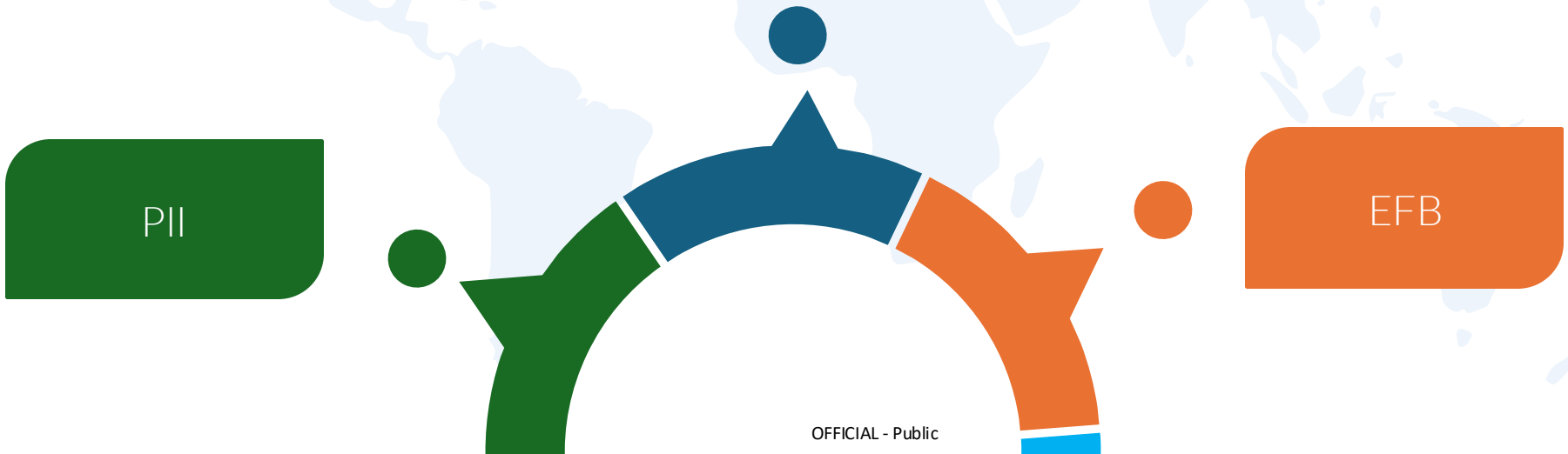


Engineering Data

An entire fleet grounded!?

Flight School ‘Hack’

“In some cases, planes that previously had maintenance issues had been ‘cleared’ to fly”, according to a police report.

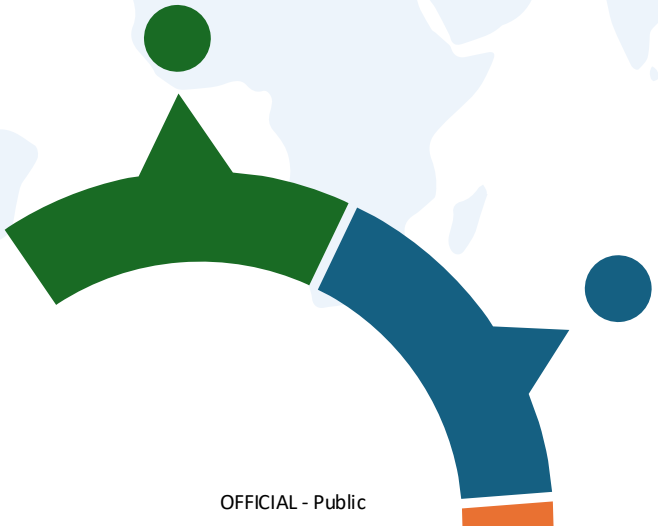


Sensitive Data

Know your attack surface

Airline Information Exposure

"a low-cost airline mistakenly disclosed the personal information of flight crew members, as well as source code and flight data, after misconfiguring an AWS bucket."



EDB

Why Is This Important?

Resilience

- What SOPs are in place for things like unavailable EFB?
- When was this last utilised?
- Is there an inherent reliance, much like GPS?

EFB Security

- OEMs produce security guides; however, the onus is on the owner/operator to create and enforce policies.
- Crews are often required to connect EFBs to open Wi-Fi networks when away from home base.

Backend Systems

- Often hosted in public cloud infrastructure.
- Outsourcing of IT functions to 3rd parties, introducing a reliance on SLA and contractual obligations.

Connectivity

- Many modern aircraft avionics systems allow wired or even wireless connection.
- This connectivity provides an attack vector, particularly from insider threat.

The Future

Tomorrow’s Sky Hubs: The Next-Gen Vertiports

Dependence on Data & Insights for Operational Success

Israeli fighter jets scrambled to intercept a Wizz Air flight from London to Tel Aviv after a child renamed his parents' phone Wi-Fi hotspot to the word 'terrorist'.

The plane was flying from **Luton** to Ben-Gurion airport on Sunday afternoon when panic engulfed the cabin.

A passenger reportedly spotted what appeared to be a threatening message on a mobile phone belonging to an ultra-Orthodox couple, Israeli media reports.

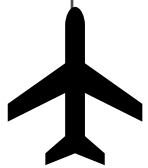
The crew informed the control tower at Ben-Gurion Airport and they sent fighter jets to escort the plane.

A passenger plane from Turkey to Spain declared an emergency after a Wifi name containing a bomb threat appeared mid-air.

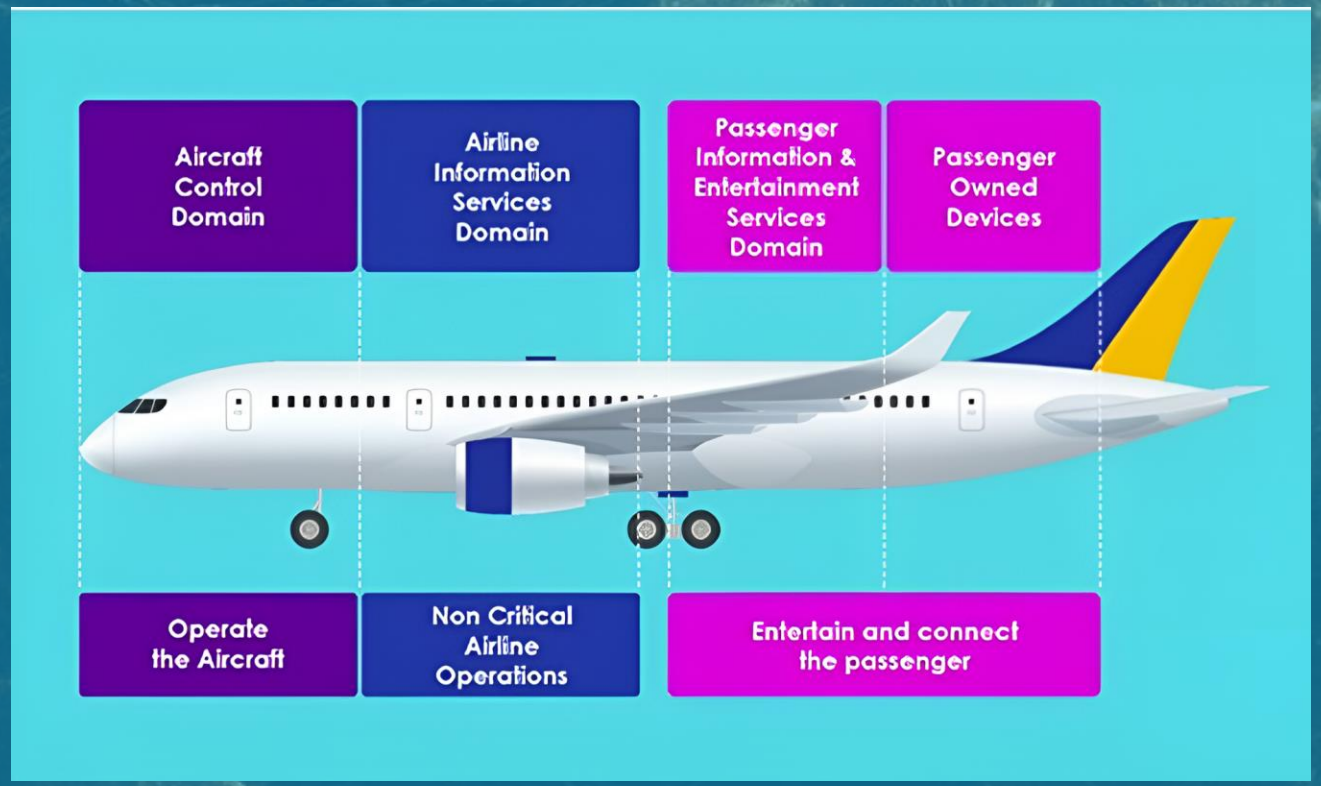
The Turkish Airlines plane was en route from **Istanbul** to **Barcelona** when pilots alerted the air traffic controllers to an incident.

A passenger had created a wireless network on board the plane and set the network name containing a bomb threat, the airline's spokesperson said.

The plane carrying 148 passengers and seven crew members was escorted by Spanish and French warplanes over the Mediterranean, El Nacional reports.

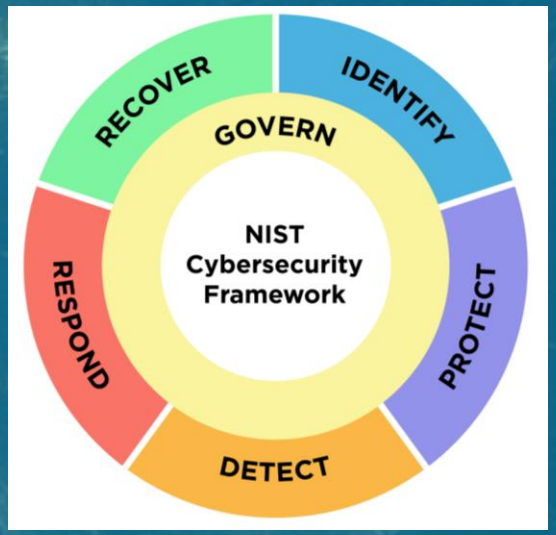


Need to maintain existing network boundaries



Focus on basic cyber-safety hygiene

CIS Controls™



Security by Design

- Help avoid budget overspend
- Early identification of product deficiencies
- Influence design requirements and change management
- Increase traceability and analysis
- Implement secure software lifecycle & DevSecOps

Consider the whole ecosystem

Thank You For Listening

IATA
WORLD
DATA
SYMPOSIUM

Newworks
SOLUTION

Beyond the Runway: Cyber Threats Shaping Aviation's Future

Melania Haro
Partner, Deloitte

#IATAWDS

IATA

Beyond the Runway: Cyber Threats Shaping Aviation's Future

2026

Cyber Threats Shaping Aviation's Future

Aviation Ecosystem

Cyber Challenges

Deloitte at-a-glance

Global Cyber

- **30+ year history**
- **3,500+ cyber clients**
- **4 Cybersphere Centers**
- **35K+ cyber practicioners**
- **$5 billion**
- **Expansive Global Network**
- **Strategic alliances & Ecosystem relationships**
- **End-to-End**
- **Destination for Top talent**

Deloitte in the Industry

Deloitte Cyber is a **global leader** in security services. Deloitte supports **100+ airlines** worldwide, including **top carriers**, with broad expertise, **global scale**, and strong industry impact.

Aviation Ecosystem

Challenges posed by the industry

Industry in expansion and digital transformation

- Growth and consolidation (4.7B passengers by end of 2024)
- Pressure to optimise operations and resilience.
- Digitalisation drives integration of new technologies (AI, IoT, advanced air traffic management systems)
- Rising vulnerabilities/attack surface from interconnectivity and dependence on external providers.
- Regulations elevate cybersecurity. Resilience relies on: Compliance, Clients, and Manufacturing.

Current challenges and vulnerabilities

MAIN CYBERSECURITY CHALLENGES IN THE INDUSTRY

01 Increase in cyber attacks

02 Interconnection between IT and OT systems

03 Regulations

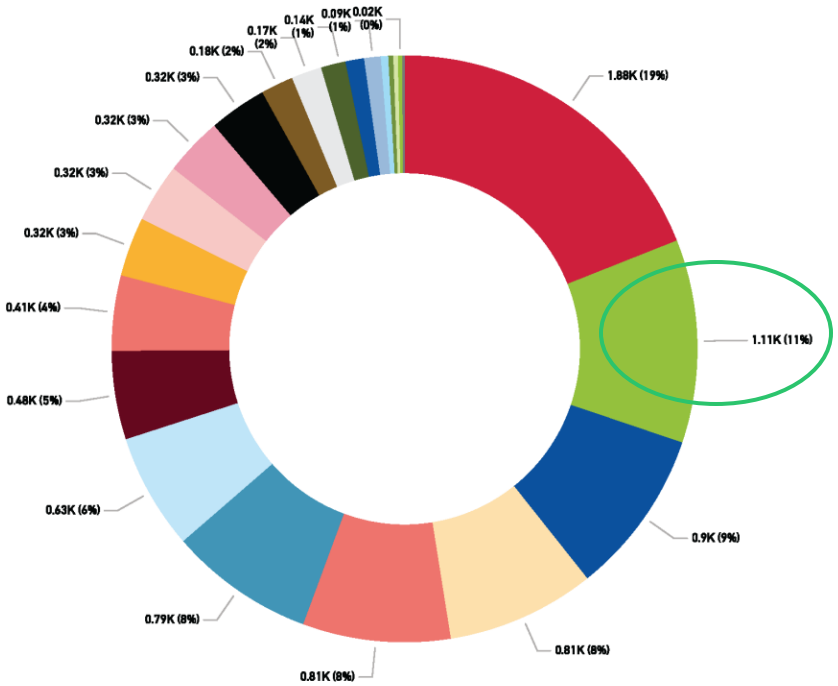
04 Training and awareness

Impact of attacks

- On IT systems
- On OT systems
- On IoT devices

CURRENT STATE OF MATURITY

High cybersecurity maturity is critical to protect complex, highly interconnected aviation.



Aviation Ecosystem Overview

Cyber Challenges

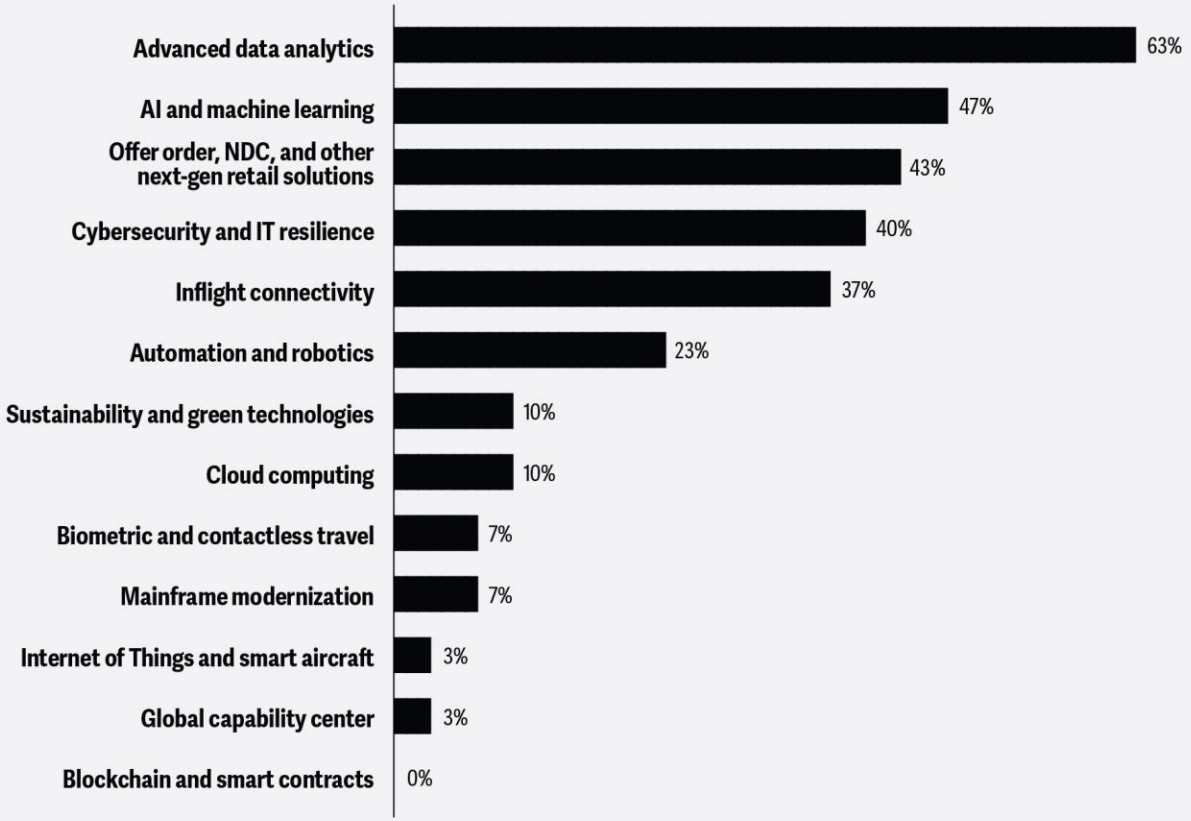
CEOs Focus on Technology investments: new cyber challenges ahead

- Technology is now central to airlines' growth agenda.
- Around half of CEOs prioritize transformative technology.
- 63% rank advanced data analytics as the top tech investment for near-term impact.
- Modern data environments drive efficiency and profitability.
- Cybersecurity is critical to risk management and resilience.

Figure 7

Strengthening data foundations and analytical capabilities underpins tech investments

Which technologies are you prioritizing for investment over the next 12 months? Please select your top three.



Notes: n = 32 global airline CEOs; NDC stands for new distribution capability.

Source: Deloitte Global's 2025 Airline CEO Survey.

Deloitte. Insights | deloitteinsights.com

CISOs voice: a peek into their challenges

Six key insights

01

AI, main CISO challenge in 2026, requiring new operational approaches.

02

Regulation elevates cybersecurity to management, demanding accountability.

03

Cyber talent shortage slows sector evolution.

04

Third-party visibility investment is a game changer for CISOs.

05

Operational continuity remains a major concern; CISOs are key.

06

Mature companies place the CISO near Management. Alignment gaps between business and cybersecurity.

CISOs voice: a peek into their challenges. The future of cyber

The Five Paradoxes

01

Cyber confidence is high

But are organizations ready?

02

The executive team believes in and prioritizes strategy

Cyber doesn't have the same level of influence elsewhere

03

We want fewer vendors

We need more vendors

04

Cyber breaches remain steady and persistent

Their business impact is contained

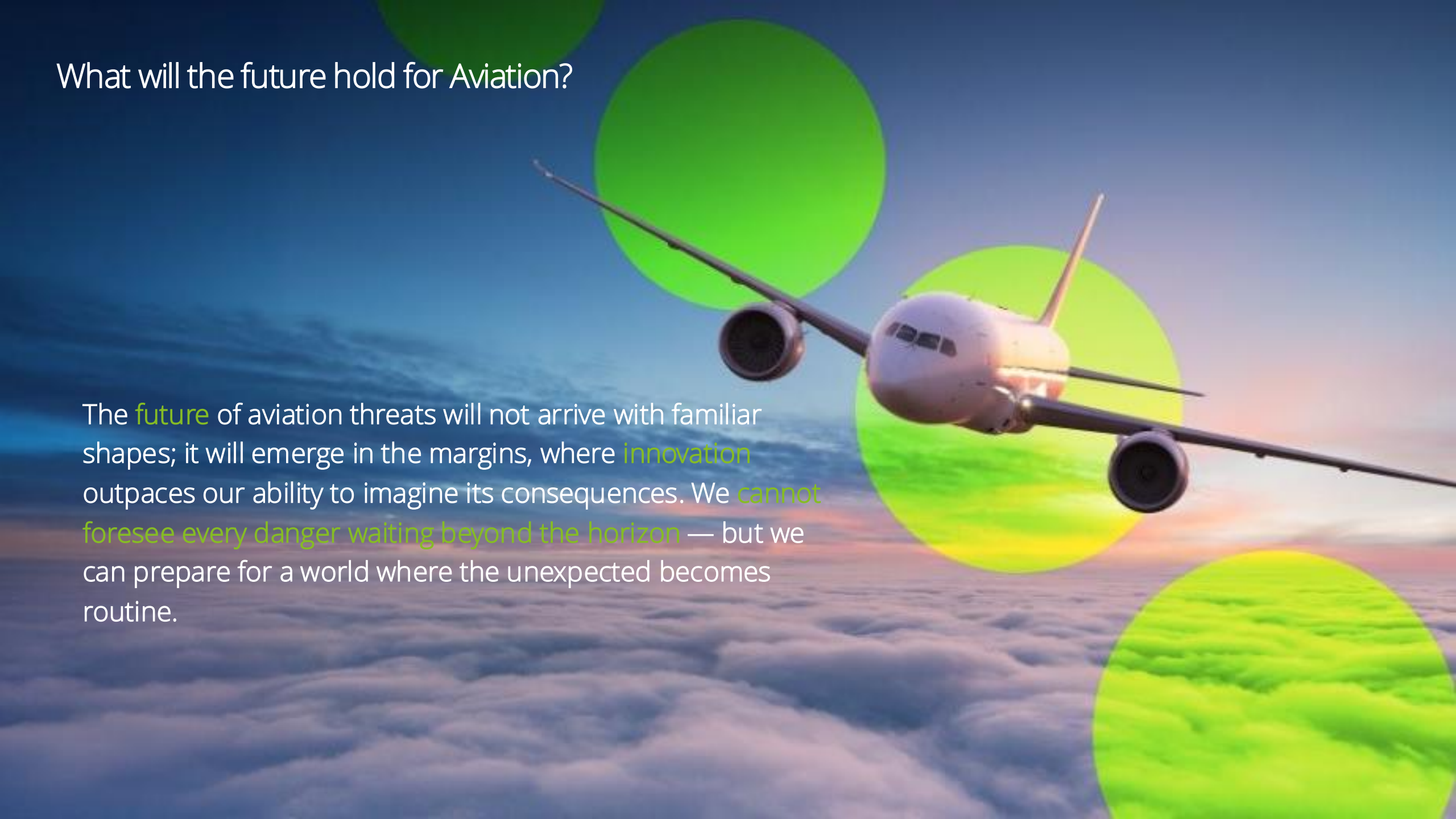
05

Year-to-year cyber budgets are stable

The cyber environment is wildly unstable

Our view for 2030

What will the future hold for Aviation?



The future of aviation threats will not arrive with familiar shapes; it will emerge in the margins, where innovation outpaces our ability to imagine its consequences. We cannot foresee every danger waiting beyond the horizon — but we can prepare for a world where the unexpected becomes routine.

Deloitte.

MAKING AN IMPACT THAT MATTERS since 1845

IATA
WORLD
DATA
SYMPOSIUM

Newworks
SOLUTION

The Rise of the Machines

Reinhart Hansen
Director of Technology – Cyber Security, Thales

#IATAWDS

IATA

imperva

THALES
Building a future we can all trust

CYBERSECURITY

Rise of the Machines

AI in the hands of Bad Bots

www.thalesgroup.com

Speaker

Reinhart Hansen

Director of Technology

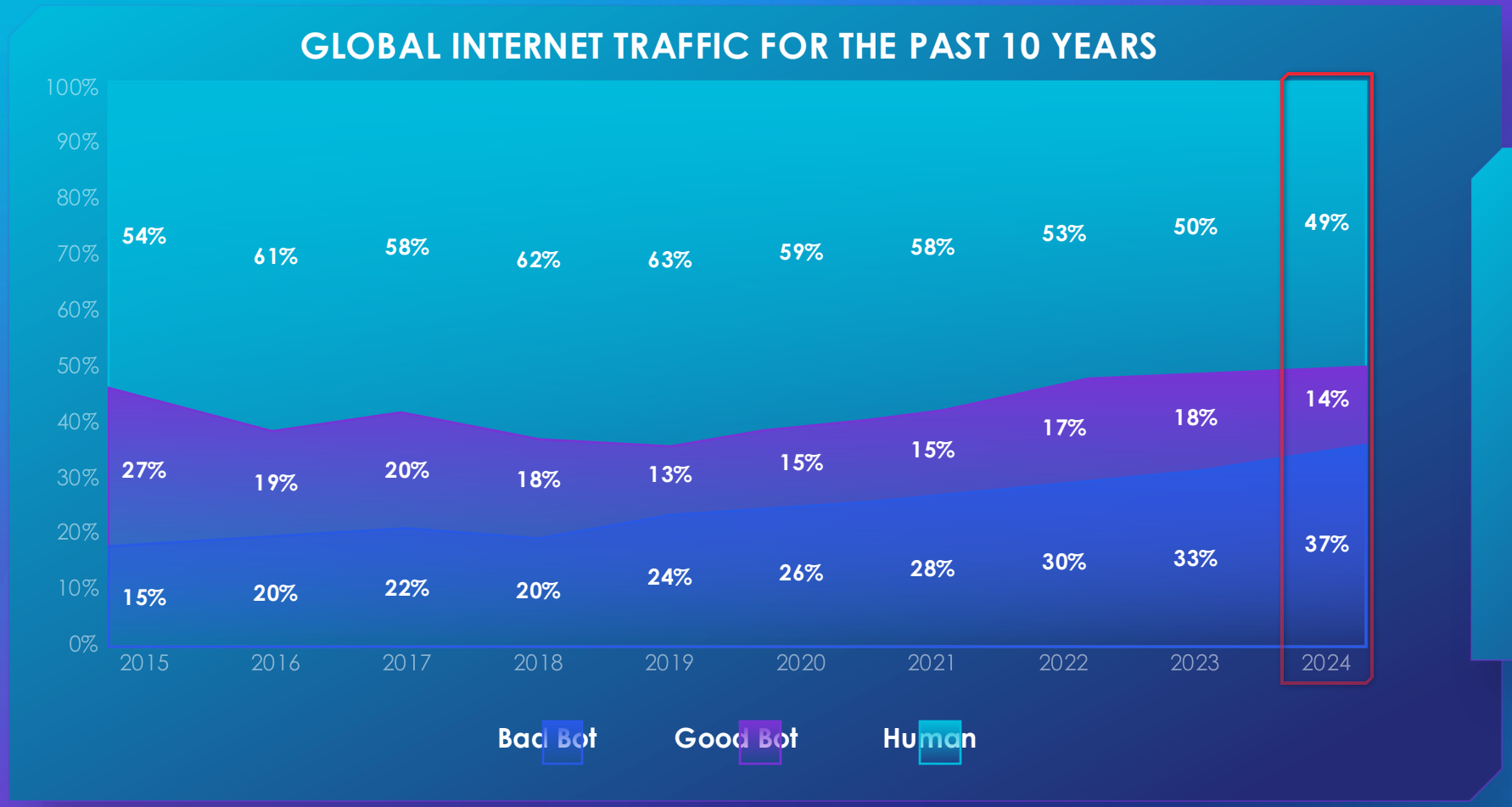
Thales Cyber Security

Agenda

1. The Bot Landscape Unveiled
2. AI in the Hands of Bad Bots
3. Airline Ticketing & Thales Imperva Fights Back

Bot landscape

Thales Imperva Bad Bot Report 2025



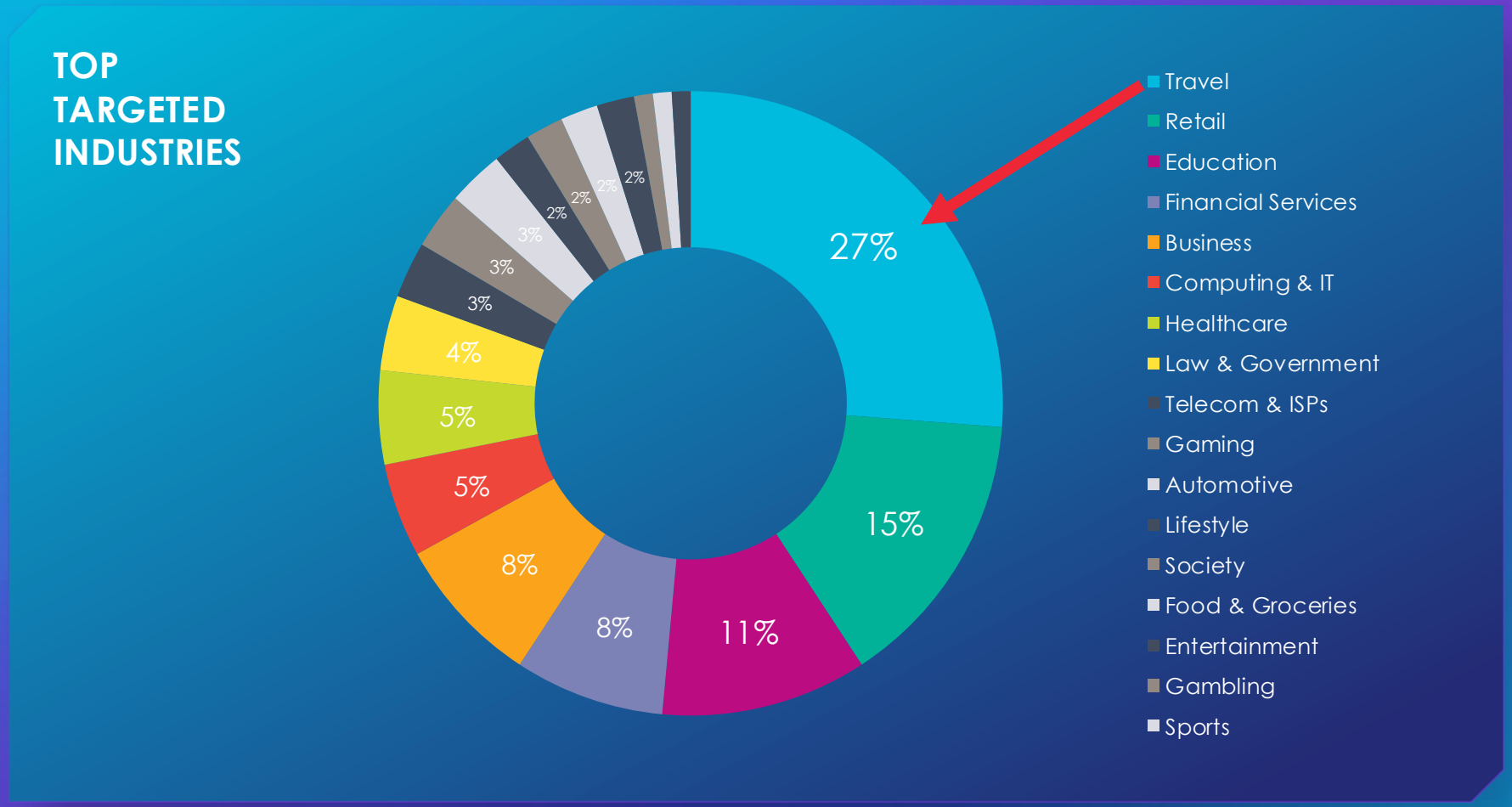
1st time Bot traffic becomes higher than Human traffic

imperva

THALES
Building a future we can all trust
CYBERSECURITY

Top-Targeted Industry

Travel accounted for 27% of all bot attacks in 2024



imperva

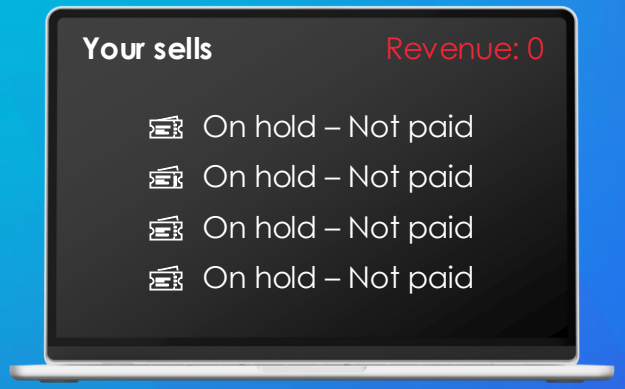
THALES
Building a future we can all trust
CYBERSECURITY

Bots in the Airline Ecosystem

imperva

THALES
Building a future we can all trust
CYBERSECURITY

Sophisticated Bot Attacks—Functional Abuse



Denial Of Inventory

- Disrupt supply and demand → Requests
- Impact revenues and operations → Purchases
- Defeat the competition → Revenues
- Holding cheapest fares → Reputation

SMS Pumping

- Impact revenues → Revenues
- Generate revenue through network operators → Reputation

imperva

THALES
Building a future we can all trust
CYBERSECURITY

AI in the Hands of Bad Bots

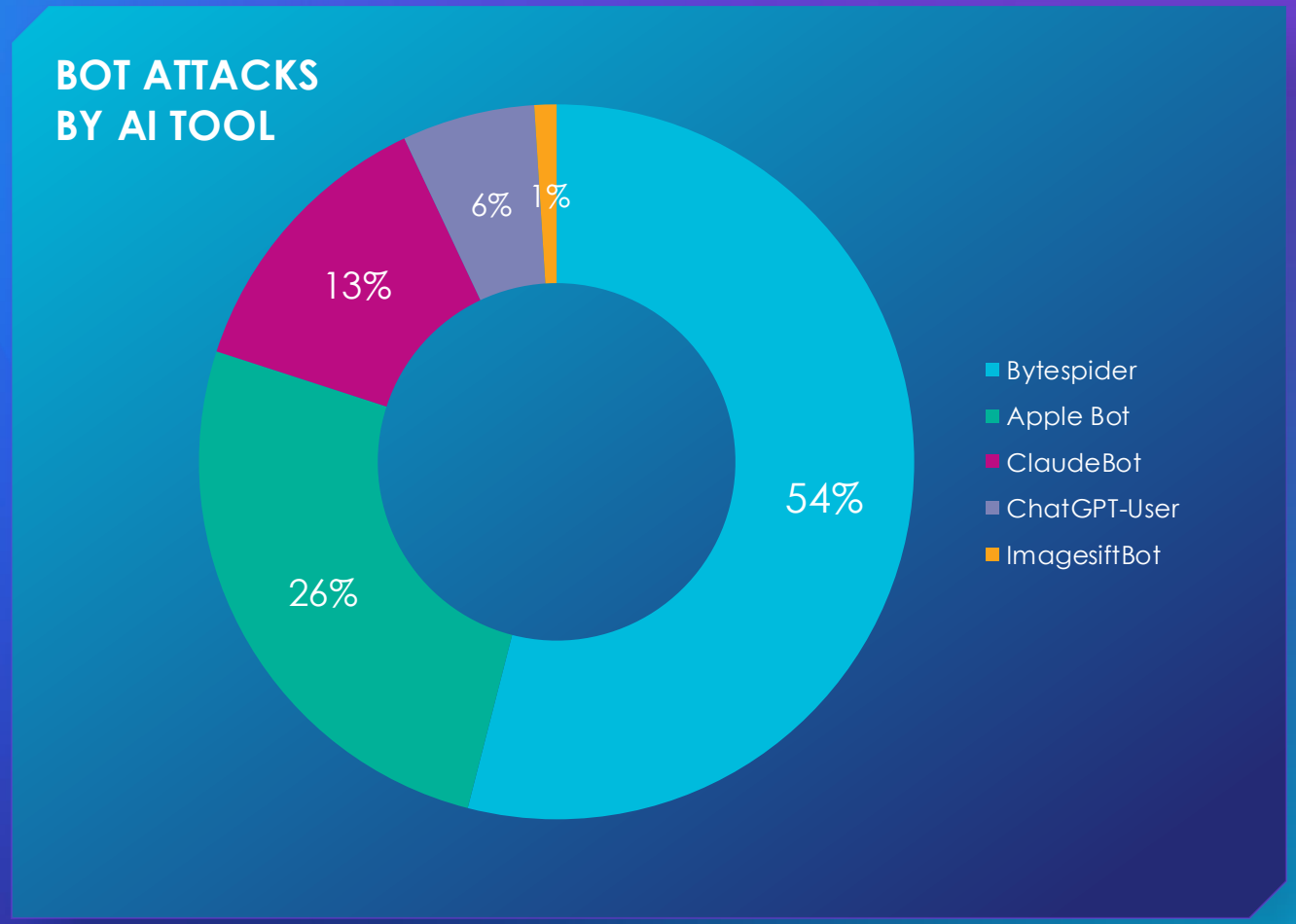
imperva

THALES
Building a future we can all trust
CYBERSECURITY

Rise of AI-Driven Cyber Threats

Thales Imperva Bad Bot Report 2025

- 41% of AI attacks involve malicious bots or business logic abuse
- Mainly target APIs and business logic vulnerabilities
- Attacks are faster, more sophisticated, harder to detect
- Many AI tools involved



imperva

THALES
Building a future we can all trust
CYBERSECURITY

AI Bot Evasion Technics

Bypass Captcha Mechanism

AI bots now bypass CAPTCHAs, weakening traditional security

Headless Browsers

AI tools like Puppeteer and Selenium mimic users to evade detection

imperva

THALES
Building a future we can all trust
CYBERSECURITY

AI Bot Evasion Technics

Polymorphic Bots

Self-learning bots adapt their attributes in real time to avoid detection

AI Assisted Scripting

AI scripts amplify attack scale and automation

imperva

THALES
Building a future we can all trust
CYBERSECURITY

Rise of AI-Driven Cyber Threats

GenAI helps create bots that can evade anti-bot protection (Thales Imperva 2025 Bad Bot Report)

You

could you create in python a bot that enters in a website and clicks on a button called submit simulating human-like mouse movements?

Copilot

Absolutely! Here's a Python script that uses Selenium and `pyautogui` to simulate human-like mouse movements and click on a button called "submit":

1. **Install the necessary libraries**:

```
pip install pyautogui
pip install selenium
```

2. **Write the script**:

Python

```python
import pyautogui
import time
from selenium import webdriver
from selenium.webdriver.common.by import By
from selenium.webdriver.support.ui import WebDriverWait
from selenium.webdriver.support import expected_conditions as EC

# Set up the Selenium WebDriver
driver = webdriver.Chrome()  # Make sure you have the ChromeDriver installed
driver.get('http://example.com')  # Replace with your target website

# Wait for the submit button to be clickable
```

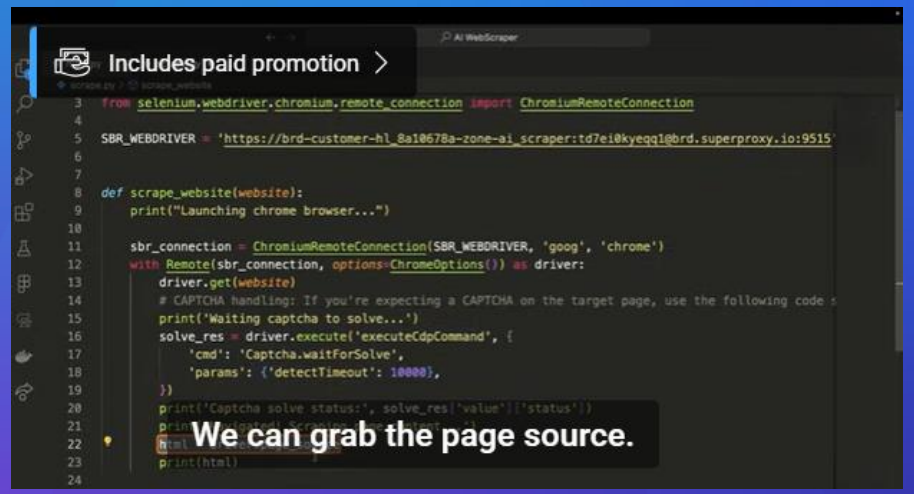

imperva

THALES
Building a future we can all trust

CYBERSECURITY

Internet Video Tutorials

Scrape ANY Website With AI For Free—Best AI Web Scraper
94K views • 10 months ago



Python AI Web Scraper Tutorial—Use AI To Scrape ANYTHING
296K views • 8 months ago

YouTube

How do we respond to the rise of AI-driven bot attacks?

Lower the ROI for Attackers

DNA Detection Strategy

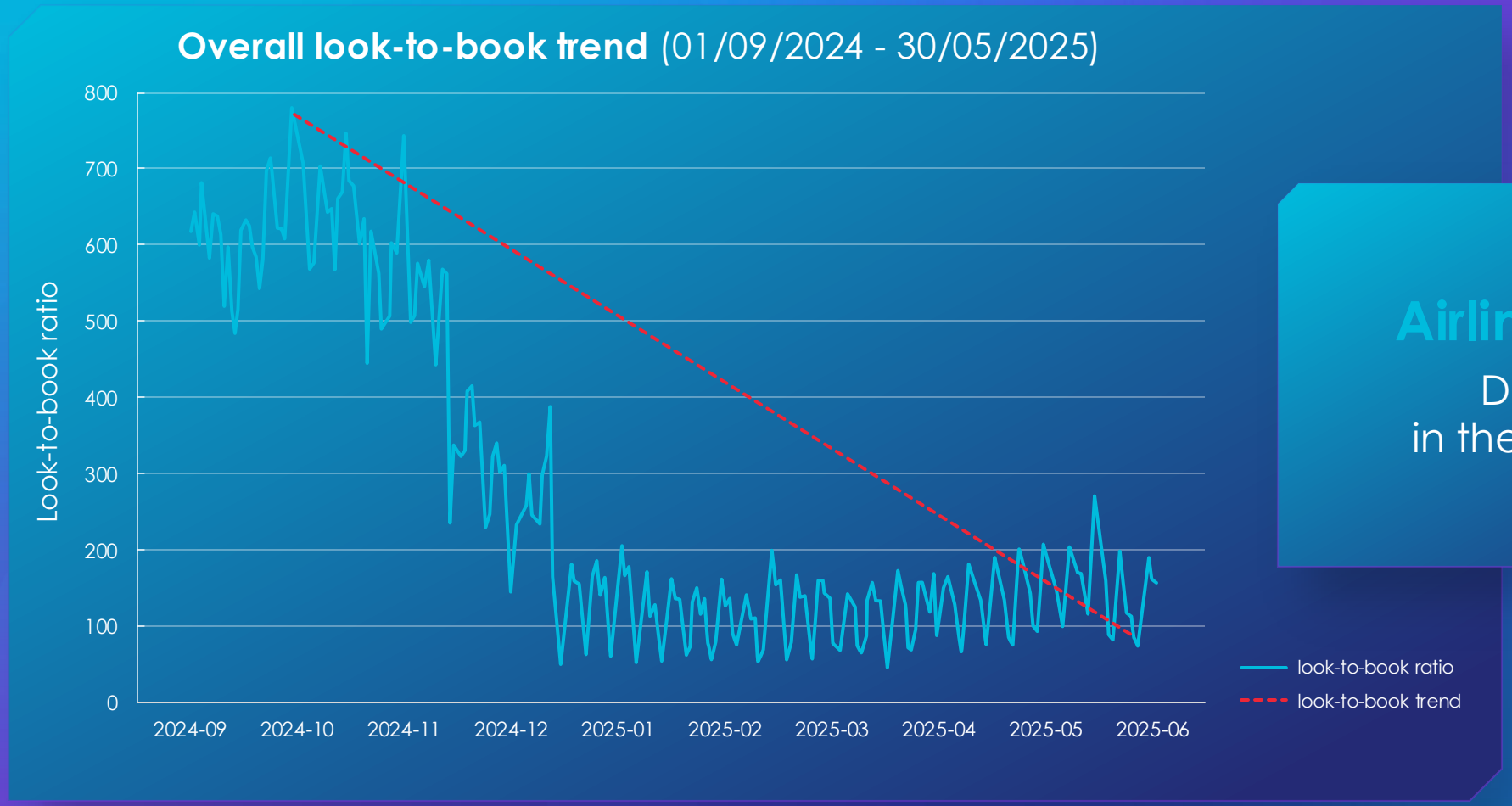
Normal traffic Bot #1 Bot #2

- Detect Bot Mutation
- Precompute Blocking options

imperva

THALES
Building a future we can all trust
CYBERSECURITY

Outcome



Airline A using DNA

Decrease of **80%**
in the look-to-book ratio

imperva

THALES
Building a future we can all trust
CYBERSECURITY

Proof of Work Mitigation

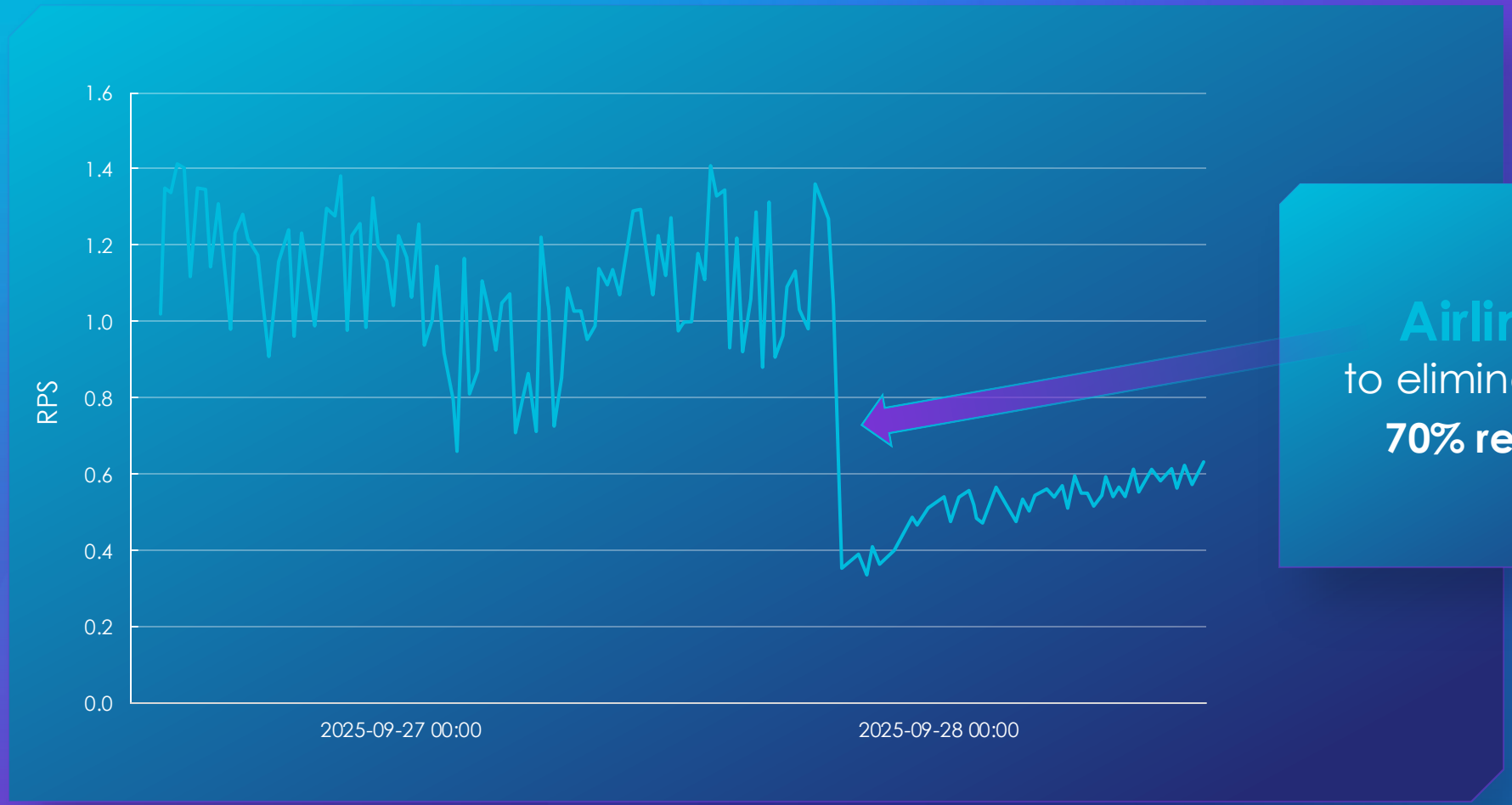
Forces attackers' machines to solve computationally expensive algorithms to slow down their efforts and increase their costs

imperva

THALES
Building a future we can all trust
CYBERSECURITY

Proof of Work Outcome (Effects on look to book ratio)

Airline facing denial of inventory



Airline A using PoW

to eliminate abusive BOT traffic

70% reduction of false PoW

imperva

THALES

Building a future we can all trust

CYBERSECURITY

CAPTCHA Farms Detection

Why CAPTCHA is ineffective

CAPTCHA SOLVING SERVICE

Better call AntiCaptcha.
Your automation API choice since 2007.

LOWEST PRICE ON THE MARKET

Starting from 0.5USD per 1000 images, depending on your daily spending volume

Propagation time inconsistent with geographic location → Risk of CAPTCHA FARM

imperva

THALES
Building a future we can all trust
CYBERSECURITY

Recommendations for the Aviation Industry

To Reduce the Bad Bot Threat

- **Proof of Work Mitigation**
- **DNA Detection for Adaptive Bots**
- **Detect Use of Residential Proxies**

Scan the QR code for the full List of recommendations

imperva

THALES
Building a future we can all trust
CYBERSECURITY

Thank You

www.thalesgroup.com

imperva

THALES
Building a future we can all trust

CYBERSECURITY

IATA
WORLD
DATA
SYMPOSIUM

Newworks
SOLUTION

Eyes in the Sky

#IATAWDS

IATA

IATA WORLD DATA SYMPOSIUM

Eyes in the Sky

Newworks SOLUTION

Jonathan Butts

Founder,
QED Secure Solutions

Issac Lee

Security Developer,
QED Secure Solutions

Eyes in the Sky

How to make cybersecurity visibility a reality at 35,000 feet

Jonathan Butts, PhD
Isaac Lee
QED Secure Solutions
contact@qedsecure.com

About QED

- Proven Capabilities
  - One of the few organizations with actual hands-on experience evaluating real-world commercial aircraft and avionics systems
  - Decades of experience in aviation environments solving complex problems

- Extensive Experience Working with Commercial Aviation
  - Lead research organization for DHS Aircraft Cybersecurity Study
  - Expertise in Aircraft Information / Network Security Program development
  - Aircraft log analysis tools employed by multiple major US operators
  - Lead cyber firm/consultant to national airline carriers

- Recognized Experts on Complex System Evaluations
  - Commercial Aviation
  - Military weapon systems
  - Unmanned aircraft systems
  - Locomotives
  - Automobiles
  - Medical devices
  - Industrial control systems
  - Critical infrastructure

Logs??

We know about logs for traditional IT systems

- Power Grid Attack —Network & System Logs
  - VPN authentication logs showed logins from unusual geographic locations
  - Admin accounts used outside normal working hours
  - Network logs recorded remote desktop sessions into control systems
- Retail Breach —Security Logs
  - Endpoint security logs flagged suspicious memory scraping malware
  - Network monitoring tools detected large outbound data transfers
  - SIEM alerts identified command-and-control communications
- Pipeline Intrusion — Account Activity Logs
  - VPN logs showed login using previously compromised password
  - Account had no multi-factor authentication
  - Login originated from an anomalous IP address
- Microsoft Exchange Exploitation — Web Server Logs
  - IIS web logs showed unusual POST requests
  - Repeated access to suspicious URLs
  - Abnormal process execution tied to web server

Logging Source	What It Detects
Firewall logs	Suspicious connections
VPN logs	Stolen credential use
Active Directory logs	Privilege escalation
EDR telemetry	Malware execution
NetFlow/network telemetry	Data exfiltration
Protocol monitoring	Unauthorized commands
SIEM correlation	Attack patterns across systems

Logs??

We know about logs for traditional IT systems

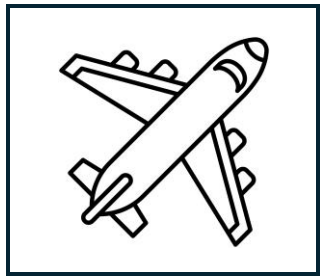
- Power Grid Attack — Network & System Logs
  - Network logs recorded remote desktop sessions into control systems
- Retail Breach —Se
  - Endpoint security lo ory scraping malware
  - Network monitoring und data transfers
  - SIEM alerts identifie ommunications
- Pipeline Intrusion · gs
  - VPN logs showed lo omised password
  - Account had no mu
  - Login originated fro s
- Microsoft Exchange Exploitation — Web Server Logs
  - IIS web logs showed unusual POST requests
  - Repeated access to suspicious URLs
  - Abnormal process execution tied to web server

What about aircraft and avionics systems

Logging Source	What It Detects
Firewall logs	Suspicious connections
VPN logs	Stolen credential use
Active Directory logs	Privilege escalation
EDR telemetry	Malware execution
NetFlow/network telemetry	Data exfiltration
Protocol monitoring	Unauthorized commands
SIEM correlation	Attack patterns across systems

First—Where Can We Get Aircraft Logs

Aircraft

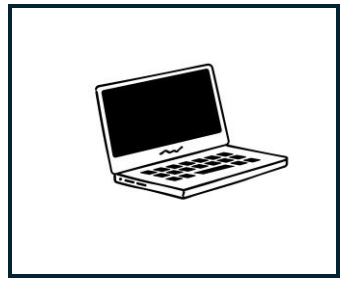


- FOMAX
- ONS
- CIS
- CSM
- NIM
- AID

Ground Support Information Systems

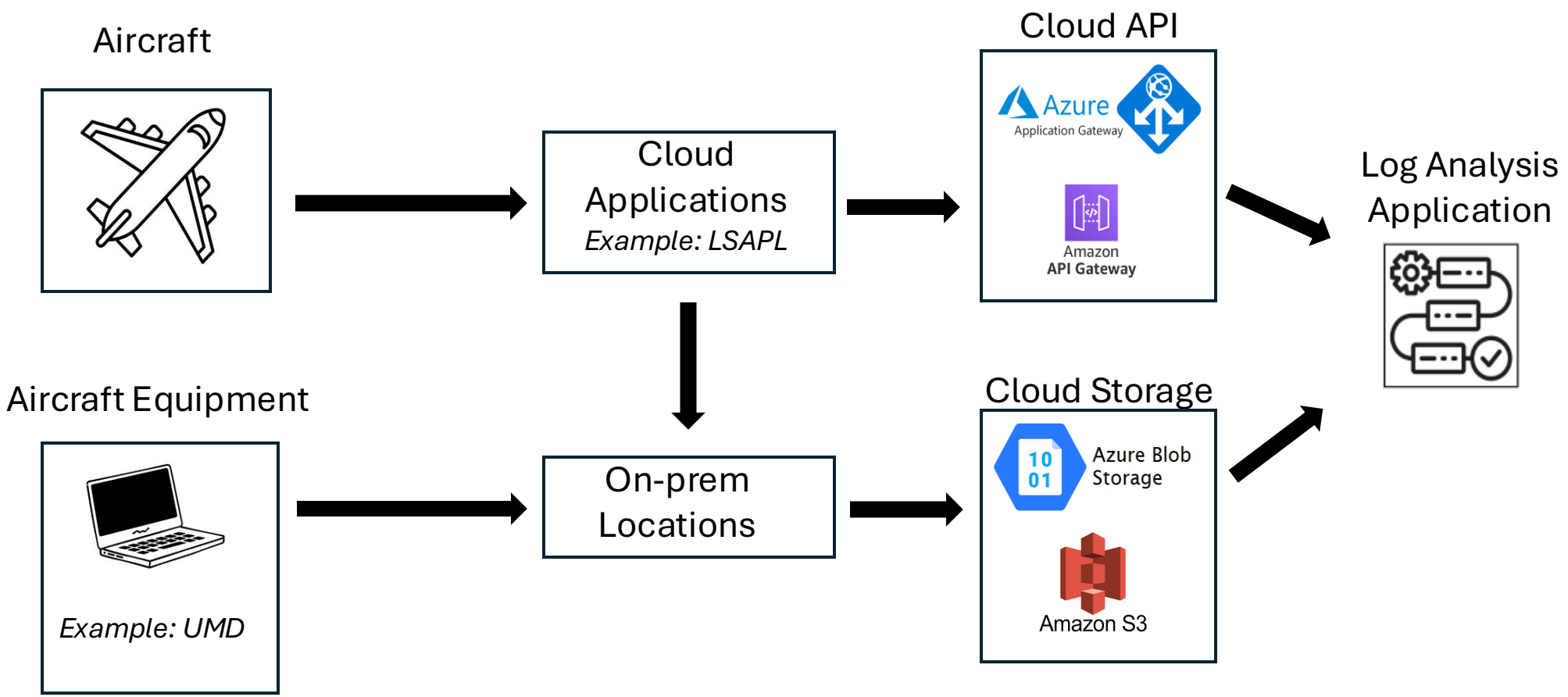
- PKI
- LSAPL
- G-FOMAX
- PWB
- Storage Lockers

PDLs



- UMDs
- PMATs
- HHMPIs

Second—What Can We Do With Them

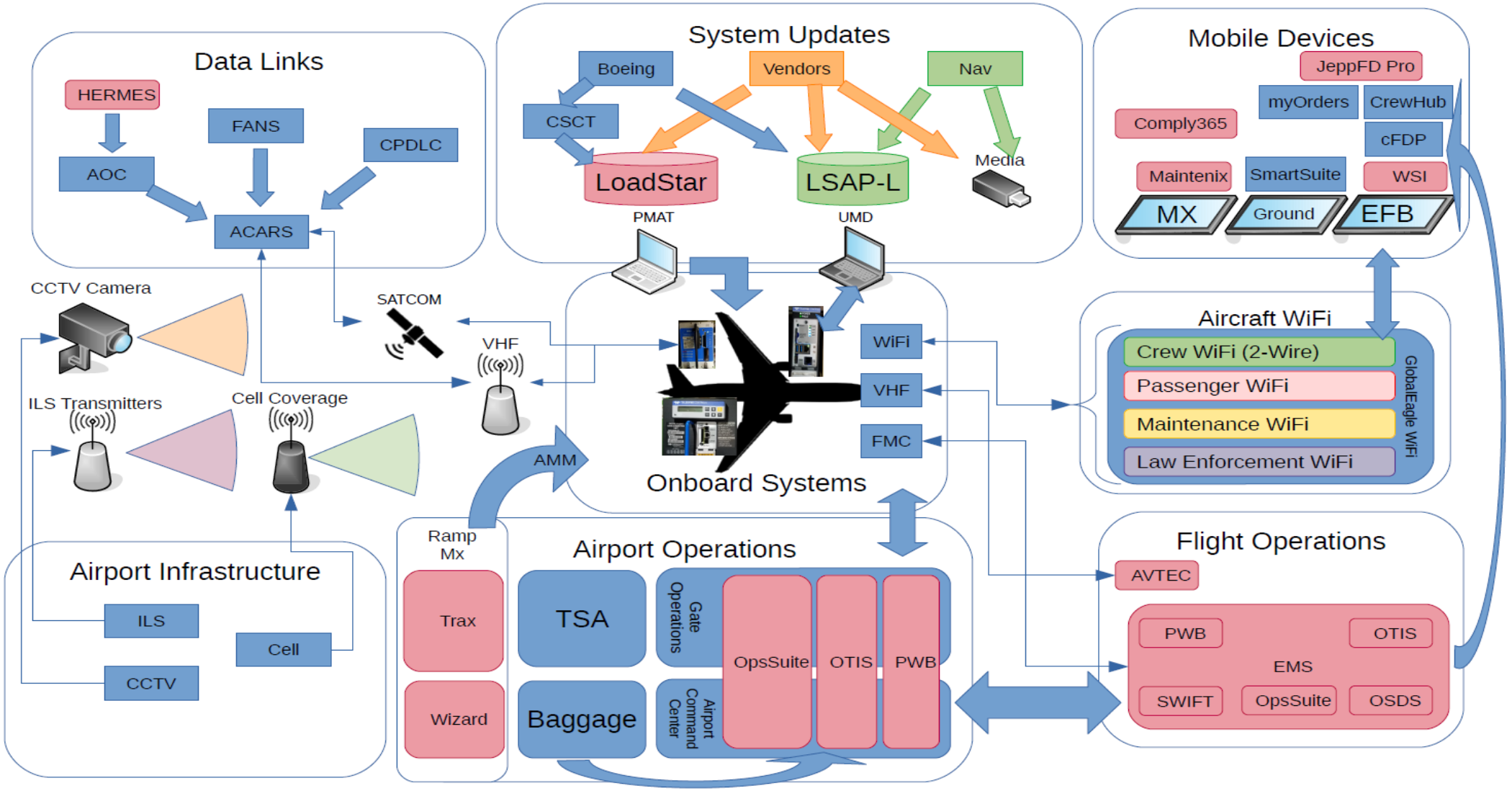


Third—Why Do We Care

- Regulatory Requirements
- Risk Reduction
- Fleet Health

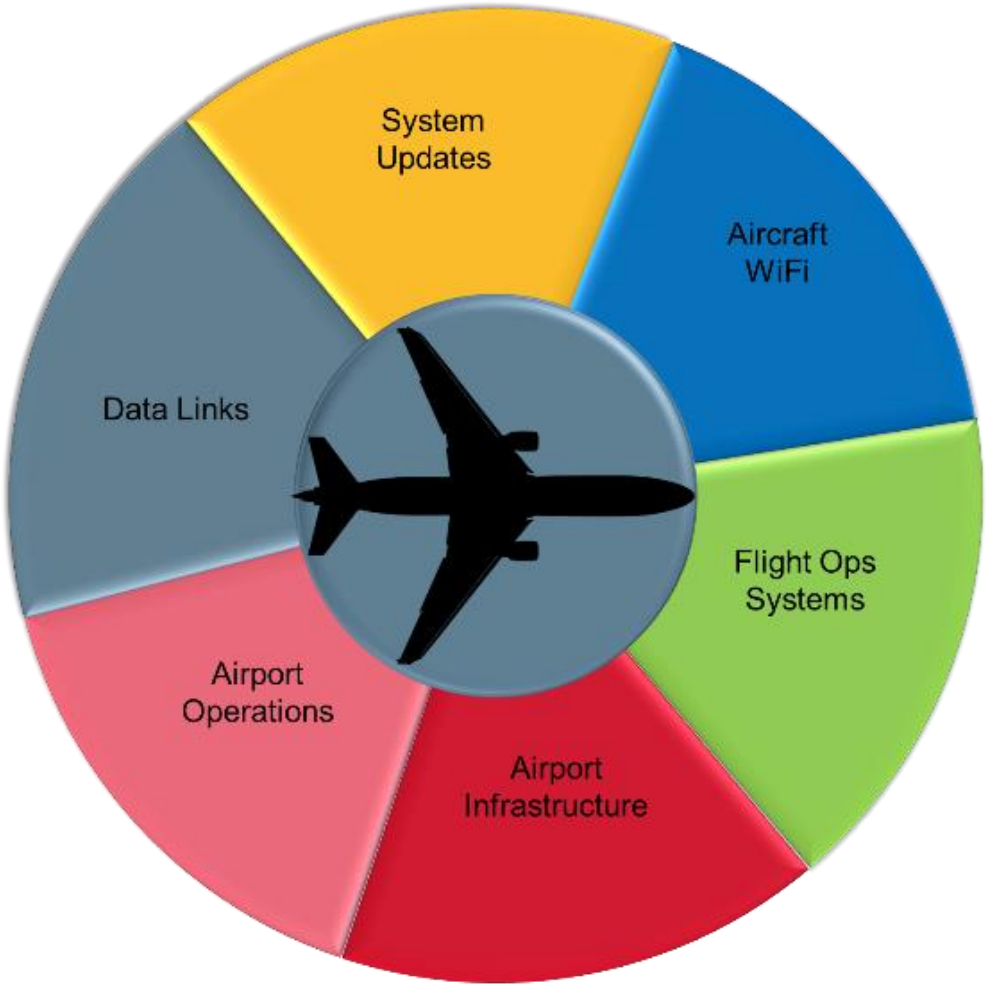
- Security Team Composition and Direction
- Reporting

Complexity


Data Links
HERMES
FANS
CPDLC
AOC
ACARS
System Updates
Boeing
Vendors
Nav
CSCT
LoadStar
LSAP-L
Media
PMAT
UMD
Mobile Devices
JeppFD Pro
myOrders
CrewHub
Comply365
cFDP
Maintenix
SmartSuite
WSI
MX
Ground
EFB
CCTV Camera
SATCOM
VHF
ILS Transmitters
Cell Coverage
AMM
WiFi
VHF
FMC
Onboard Systems
Aircraft WiFi
Crew WiFi (2-Wire)
Passenger WiFi
Maintenance WiFi
Law Enforcement WiFi
GlobalEagle WiFi
Airport Infrastructure
ILS
Cell
CCTV
Ramp Mx
Trax
Wizard
Airport Operations
TSA
Baggage
Gate Operations
Airport Command Center
OpsSuite
OTIS
PWB
Flight Operations
AVTEC
PWB
OTIS
EMS
SWIFT
OpsSuite
OSDS

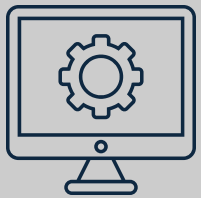
Attack Surface Characterization

Are you monitoring communications and touchpoints appropriately?



Logging Solutions – Technical Approach

Artifact Collection



Collect artifacts directly from the systems

Collect artifacts that are relevant to operations and compromise detection

Maintain centralized and single-solution collection capability

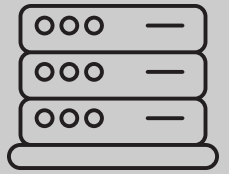
Normalization and Storage

Develop a data structure for collected data

Enable storage of artifacts with robust, scalable search capability

Establish a chronological history of system disposition

Analysis

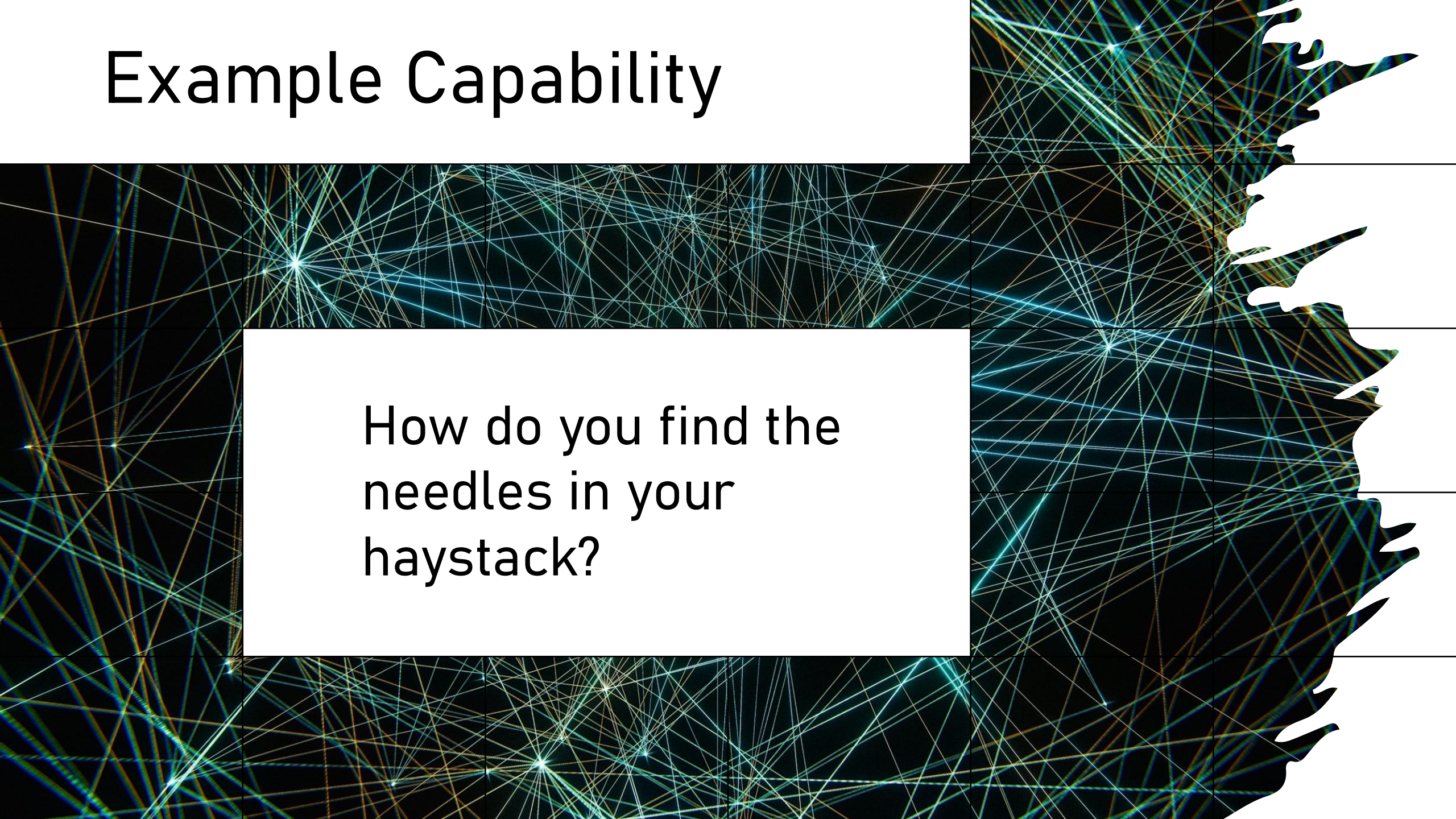


Develop a graphical interface designed specifically for analysis activities

Enable interfaces designed for operations and correlation

Enable interfaces for deep, complex analysis

Example Capability



How do you find the needles in your haystack?

WaveDash

OBSERVE

DETECT

IDENTIFY

REPORT

ANALYZE

CORRELATE

Specialized Tool for Aircraft Log Analysis

Quick, customizable, no-code log filtering software enables Cyber Analysts to fully automate discovery.

Tailored software tracks data back to each crate while log data is matched to flights. Integrated alerting and event management ensures all significant events are addressed.

Top-Level alert-based workflows of documented critical events identified by airline manufacturers, cyber threat events, and custom event mappings.

Cross System Monitoring & Cross Fleet

Aircraft activity and fleet metrics increases certainty in both cybersecurity and maintenance observations. Specialized aircraft tooling allows individual aircraft activity to be compared to other aircraft, its own fleet, and even other fleets.

Cross referencing data between aircraft systems enables deep visibility and insights. *For example: Aligning UMD, LSAPL and Aircraft Security Logs enables trust-train monitoring for software part installations.*

Cycle Anomaly Detection & Machine Learning

Creating data flight models from log data events launches early threat detection and non-conformity checks between flight cycles. Enabling cybersecurity teams to alert response teams as quickly as possible for Boeing and Airbus aircraft.

Flight based data structures are ideal for sanitized datasets for machine learning training. Enabling airlines to integrate AI/Machine Learning to provide additional insights and reducing workload for Cyber Analysts.

Monitoring for Unauthorized Activity

- Discern normal
- Identify deviations
- Isolate known and predicted behaviors
- Map risk levels to events
- Discover and alert on indicators in Aviation Systems

Capabilities

- Map critical information to enhance log analysis
- Perform event type threshold analysis
- Examine trend analysis
- Provide near real-time alerting

There are very few solutions that focus on Aviation/Aircraft

disabled

```
#2025 06 24 12:07:05#1#AirlinePFController #[WARN]#[System]#7613#Airline Po
#2025 06 24 12:08:41#1#AirlinePFController #[WARN]#[System]#7613#Airline Po
#2025 06 24 12:10:37#1#AirlinePFController #[WARN]#[System]#7613#Airline Po
#2025 06 24 12:07:04#N/A#SatcomController #[WARN]#[System]#7202#SATCOM Serv
#2025 06 24 12:08:3
#2025 06 24 12:10:3
#2025 06 24 12:12:1
#2025 06 24 12:12:1
#2025 06 24 12:14:0
#2025 06 24 12:14:0
#2025 06 24 12:15:2
#2025 06 24 12:15:2
#2025 06 24 12:25:1
#2025 06 24 12:25:1
#2025 06 24 12:07:0
#2025 06 24 12:08:4
#2025 06 24 12:10:3
#2025 06 24 12:12:1
#2025 06 24 12:14:0
#2025 06 24 12:15:2
#2025 06 24 12:25:1
#2025 06 24 12:07:06#1#A619Transceiver #[WARN]#[System]#6102#AcarsforEFB se
#2025 06 24 12:07:06#1#A619Transceiver #[WARN]#[System]#6802#FMS FPLN servi
#2025 06 24 12:08:41#1#A619Transceiver #[WARN]#[System]#6102#AcarsforEFB se
#2025 06 24 12:08:41#1#A619Transceiver #[WARN]#[System]#6802#FMS FPLN servi
#2025 06 24 12:08:41#1#A619Transceiver #[TRACE]###619 Controller PostDepend
#2025 06 24 12:10:38#1#A619Transceiver #[WARN]#[System]#6102#AcarsforEFB se
```

Quick, customizable, no-code log filtering software enables Cyber Analysts to fully automate discovery.

WaveDash

Choose File Log_X9001X_20250624_123024_229_0U.log

fpgamonitor

fpgamonitor

```
{
  "attributes": [
    "id",
    "registername",
    "address"
  ],
  "rows": [
    [
      1,
      "DEV_ID0"
```

ook for keywords

le contents will appear here...

Input prefix...

#2025 06 24 12:08:42#1#FpgaMonitor #[TRACE]###I2C register

0: 1: 2:

Select operation

Save Entry | Use Regex | Add Event Type

Line: #2025 06 24 12:08:42#1#FpgaMonitor #[TRACE]###I2C register name : DEV_ID0, address : 0x00, value : 0x4350#

Add Selected | Insert Prefix from Selection

Add End Delimiter

Download

Current Selection

Highlight text and click 'Add Selected'...

Clear Selections | Clear All Fields | Clear Saved Entries

Saved Entries

Line: #2025 06 24 12:08:42#1#FpgaMonitor #[TRACE]###I2C register name : DEV_ID0, address : 0x00, value : 0x4350#

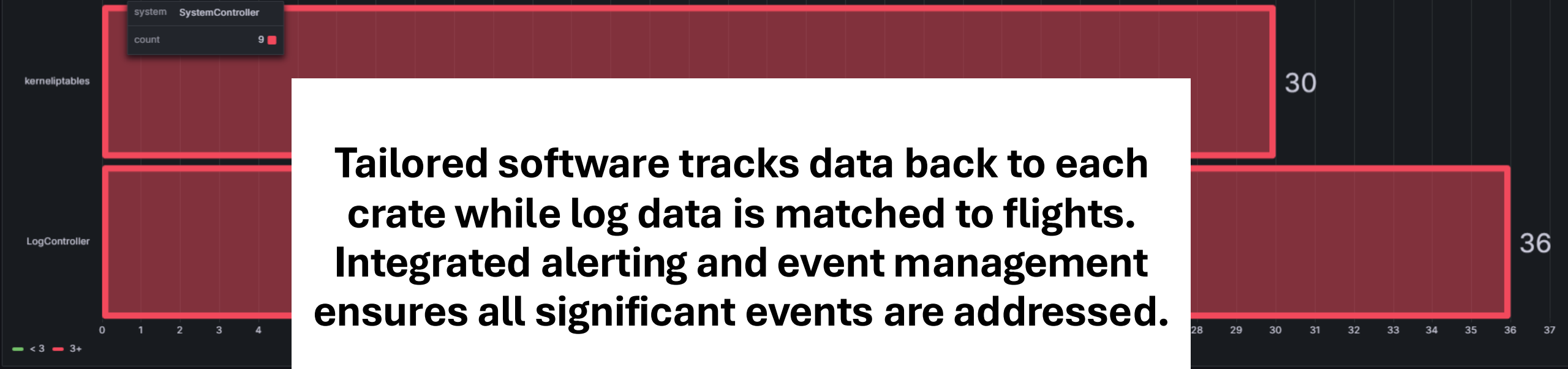
Add Selected | Insert Prefix from Selection

Add End Delimiter

Download

Current Selection

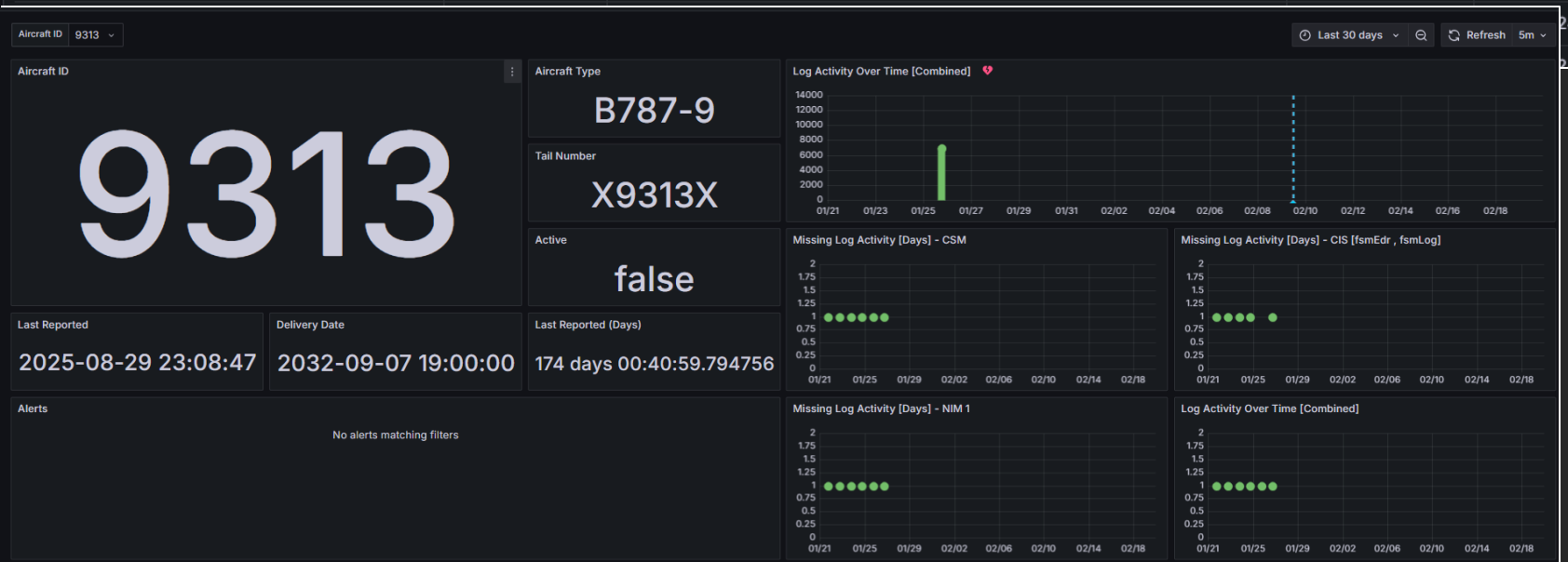
register name :

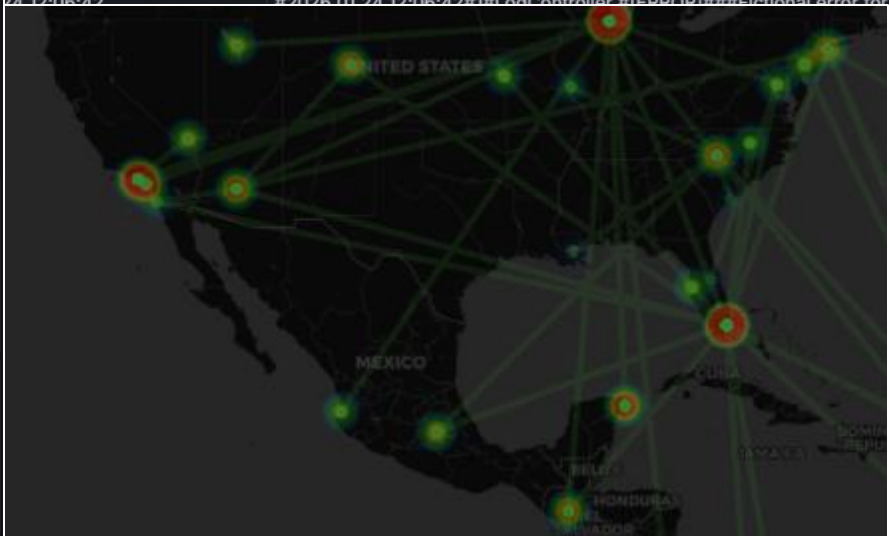


Tailored software tracks data back to each crate while log data is matched to flights. Integrated alerting and event management ensures all significant events are addressed.

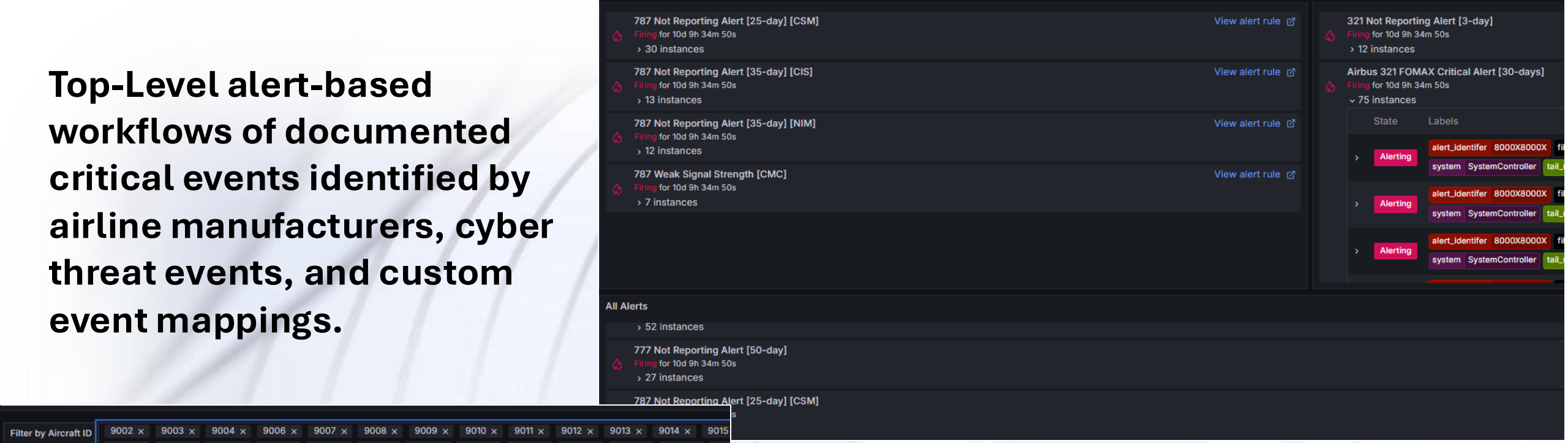
Logfiles with Critical Events

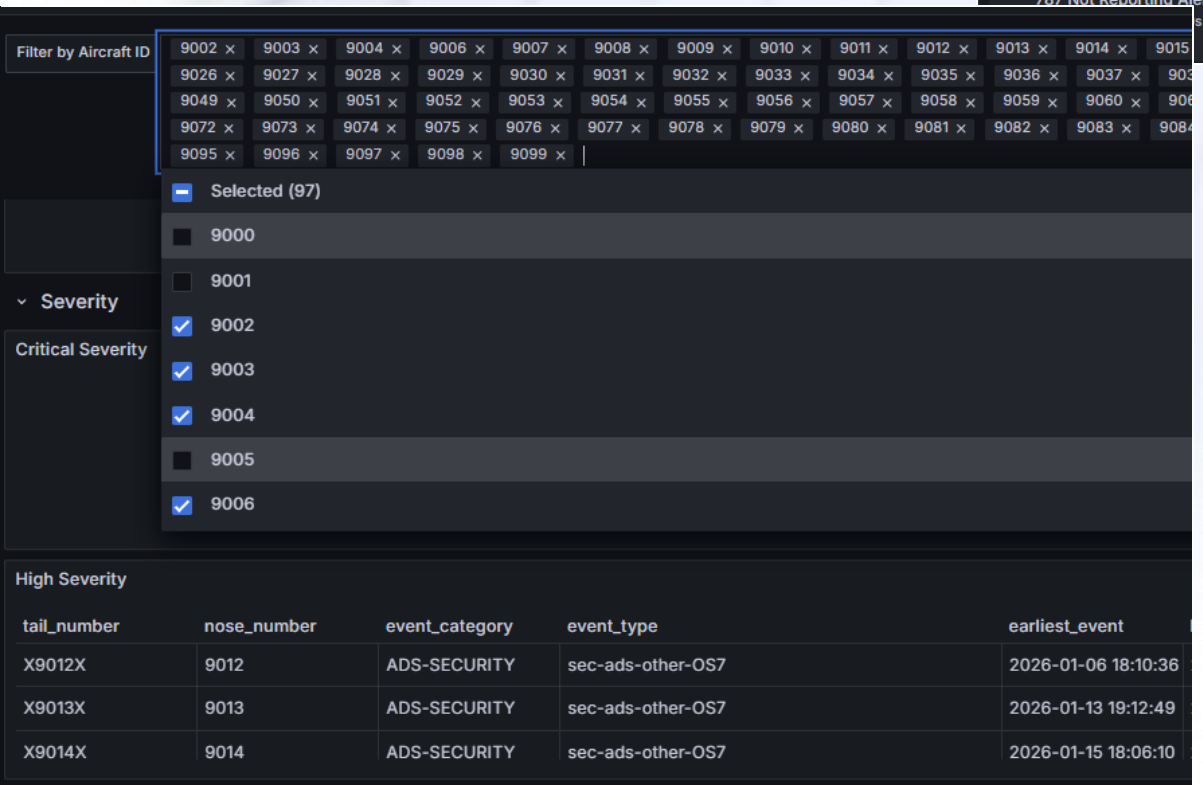
file_name	location_in_file	crate_name	tail_number	time_critical_event_occured	critical_event
Log_X8000X_2026qed_test.log	240	Log_X8000X_2026qed_test.log	X8000X	2026-01-24 12:10:55	#2026 01 24 12:10:55#1#SystemController #[ERROR]#[Sec]Status of ap
Log_X8000X_2026qed_test.log	3170	Log_X8000X_2026qed_test.log	X8000X	2026-01-24 12:26:37	#2026 01 24 12:26:37#1#kerneliptables-OUTPUT-DROP:IN= OUT=eth1
Log_X8000X_2026qed_test.log	3171	Log_X8000X_2026qed_test.log	X8000X	2026-01-24 12:26:38	#2026 01 24 12:26:38#1#kerneliptables-OUTPUT-DROP:IN= OUT=eth3
				24 12:06:42	#2026 01 24 12:06:42#1#LogController #[ERROR]###Fictional error for





Top-Level alert-based workflows of documented critical events identified by airline manufacturers, cyber threat events, and custom event mappings.

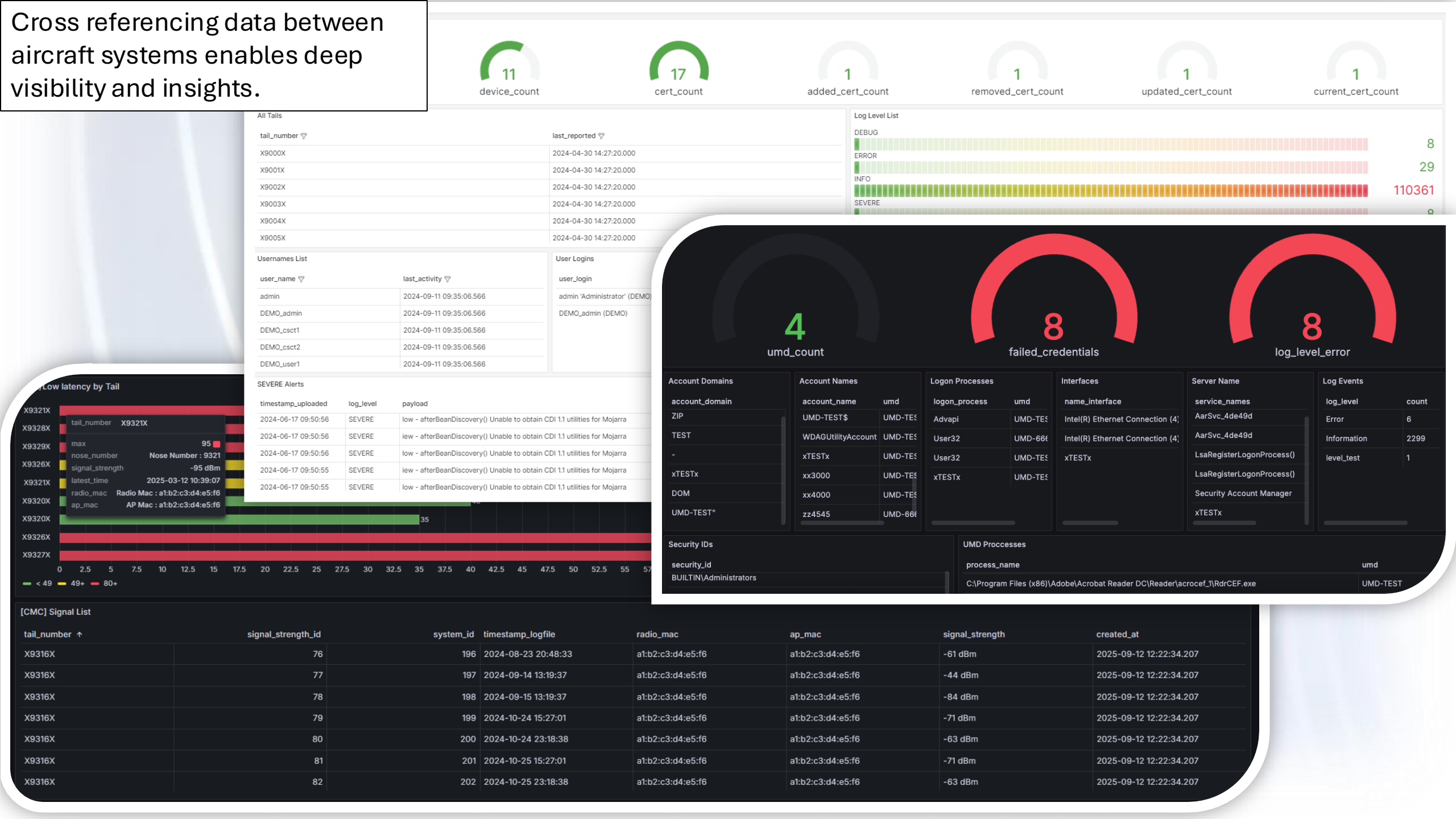


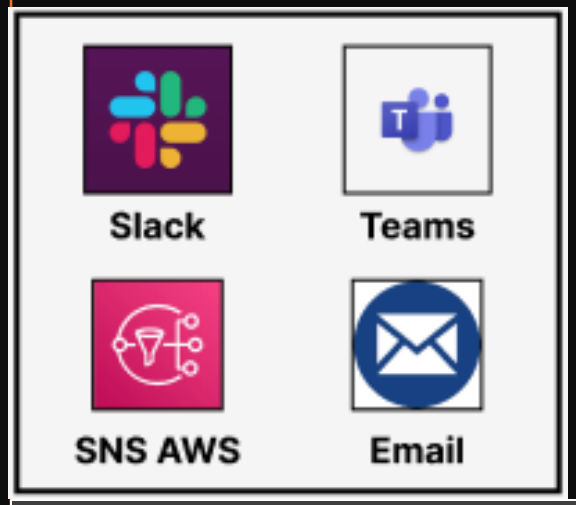


WaveDash

Aircraft activity and fleet metrics increases certainty in both cybersecurity and maintenance observations. Specialized aircraft tooling allows individual aircraft activity to be compared to other aircraft, its own fleet, and even other fleets.

Cross referencing data between aircraft systems enables deep visibility and insights.





Alert on indicators in Aviation Systems with near-real time on Slack, Teams, Emails, AWS SNS, or utilize a toolbox of other integrations.

Azure Managed Grafana

Amazon Managed Grafana

737 Alerts

737 Not Reporting Alert [3-day] — View alert rule
Firing for 13d 9h 30m 27s
› 52 instances

737 Unexpected IP [Last 90 Days] — View alert rule
Firing for 9h 27s
› 19 instances

737 Unknown Device [All Time] — View alert rule
Firing for 9h 20m 27s
⌄ 2 instances

State	Labels	Created
Alerting	alertname: 737 Unknown Device [All Time] · grafana_folder: WaveDash · last_found_in_logfile: 2025/05/18 10:05:50 · last_upload_to_database: 2025/08/20 03:08:29 · mac_trim: CC:33:DD:44:EE:55 · Hide common labels	2026-02-22 12:38:20
Alerting	alertname: 737 Unknown Device [All Time] · grafana_folder: WaveDash · last_found_in_logfile: 2025/08/18 10:08:50 · last_upload_to_database: 2025/08/20 03:08:43 · mac_trim: E5:F6:G7:H8:I9:J1 · Hide common labels	2026-02-22 12:38:20

WaveDash › WaveDash

State	Name
Firing	for 13d 9h 54m 737 N
Firing	for 13d 9h 54m 777 N
Firing	for 13d 9h 54m 787 N
Firing	for 13d 9h 54m 787 N
Firing	for 13d 9h 54m 787 N
Firing	for 9h 44m 737 U
Firing	for 13d 9h 54m 787 W
Firing	for 13d 9h 54m Airbus
Firing	for 13d 9h 54m 321 N
Firing	for 9h 24m 737 U

WaveDash

WaveDash automatically analyzes aircraft logs for cyber threats, providing deep insight into aircraft component behavior, detailed reporting, event management, and near real-time alerting.

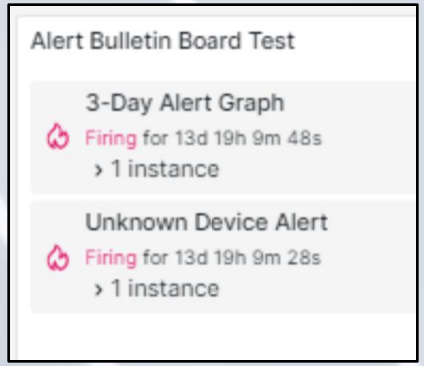


Table 1 - 737 Certificate Violation Detail

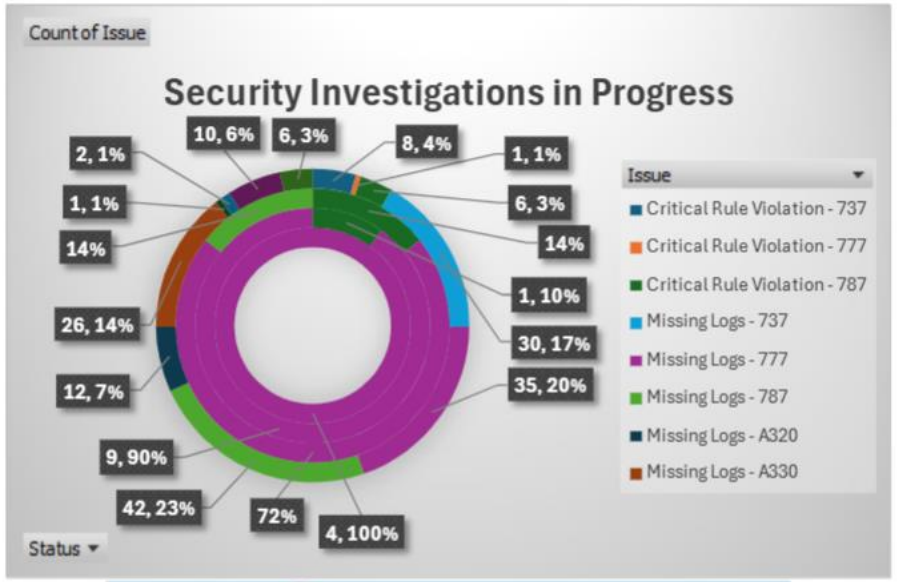
Tail	Event Type	Earliest Event	Latest Event	Total
XX1234	sec-oas-reposit-get-airplane-key-not-found	1/1/2026 4:35	1/31/2026 23:07	40818
XX1234	sec-oas-reposit-get-airplane-cert-not-found	1/1/2026 4:35	1/31/2026 23:07	40818
XX1235	sec-oas-reposit-get-airplane-key-not-found	1/1/2026 0:00	1/31/2026 0:26	33640
XX1235	sec-oas-reposit-get-airplane-cert-not-found	1/1/2026 0:00	1/31/2026 0:26	33640
XX1238	sec-oas-reposit-get-airplane-key-not-found	1/1/2026 7:13	1/31/2026 3:24	17394
XX1238	sec-oas-reposit-get-airplane-cert-not-found	1/1/2026 7:13	1/31/2026 3:24	17385
XX1240	sec-oas-reposit-get-airplane-key-not-found	1/3/2026 8:25	1/31/2026 12:14	13125
XX1240	sec-oas-reposit-get-airplane-cert-not-found	1/3/2026 8:25	1/31/2026 12:14	13125
XX1242	sec-oas-reposit-get-airplane-key-not-found	1/1/2026 13:59	1/31/2026 2:54	6352
XX1242	sec-oas-reposit-get-airplane-cert-not-found	1/1/2026 13:59	1/31/2026 2:54	6352

Table 2 - 777 Certificate Violation Detail

Tail	Event Type	Earliest Event	Latest Event	Total
XX1234	sec-oas-crcheckt-error	11/1/2025 0:58	11/22/2025 3:02	26
XX1235	sec-oas-crcheckt-error	11/3/2025 5:06	11/16/2025 20:45	24
XX1236	sec-oas-crcheckt-error	11/3/2025 16:30	11/28/2025 21:34	23
XX1237	sec-oas-crcheckt-error	12/1/2025 22:22	12/18/2025 10:55	15
XX1238	sec-oas-crcheckt-error	11/5/2025 20:44	11/26/2025 22:12	12
XX1239	sec-oas-crcheckt-error	11/19/2025 0:10	11/27/2025 6:33	3
XX1240	sec-oas-crcheckt-error	12/7/2025 7:10	12/9/2025 2:41	3

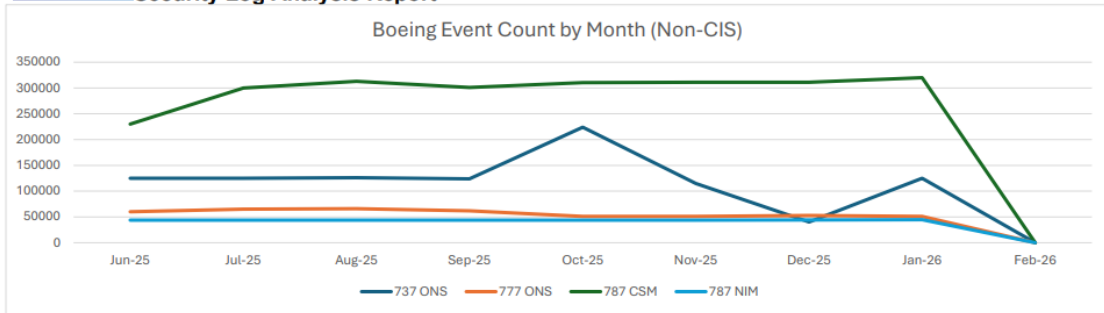
Summary of Security Events Under Analysis

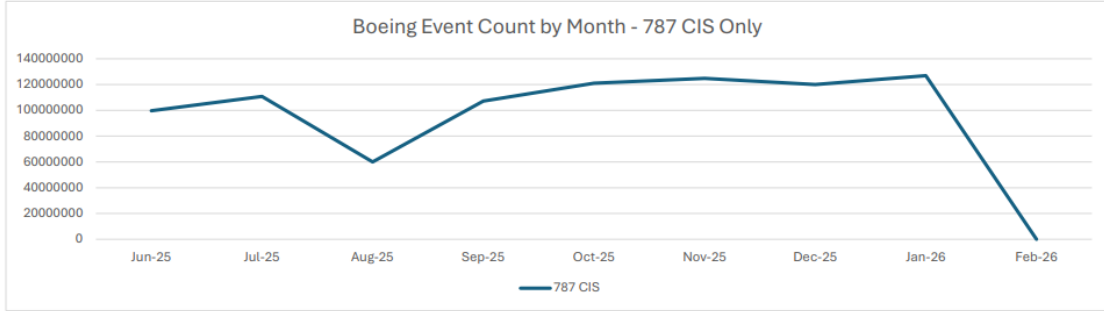
Purpose: Summarize completed or ongoing security events not related to Security Log Profile analysis.



Row Labels	New	In progress	Blocked	Completed	Grand Total
Critical Rule Violation - 737				8	8
Critical Rule Violation - 777				1	1

WaveDash **Security Log Analysis Report**





Wrap-up

- Threats to aircraft and avionics systems are real
- Effective log monitoring enhances cybersecurity posture supporting compliance and risk
- Effective log tools:
  - Prevent analysts from drowning in data
  - Standardize reporting
  - Enable rapid updates
  - Provide near-real time analysis and historical records
  - Augment and correlate maintenance data
- IATA collaboration via WaveDash
  - Customized deployment options
  - Flexible architecture and environments

Contact Information

contact@QEDsecure.com

www.QEDsecure.com

*Coordinated Demos on April 9th

IATA
WORLD
DATA
SYMPOSIUM

Newworks
SOLUTION

Runway Recap

Doug Blough
Senior Product Security Analyst, Boeing

#IATAWDS

IATA

IATA WORLD DATA SYMPOSIUM

With many thanks to all our sponsors

Official Airline Partner

Supporting Organization

Gold Sponsors

Silver Sponsors

Bronze Sponsors

Exhibitors

Silver Media Partners

#IATAWDS

IATA
WORLD
DATA
SYMPOSIUM

Newworks
SOLUTION

Networking Dinner

The Networking Dinner will start at 19:00.

#IATAWDS

IATA


IATA
WORLD
DATA
SYMPOSIUM
Singapore
8 – 9 April 2026
#IATAWDS
IATA


IATA
WORLD
DATA
SYMPOSIUM
CTRL + ALT + SKY
SINGAPORE 8-9 APRIL 2026
#IATAWDS
www.iata.org/wds
IATA