SUPPORTING
EUROPEAN
AVIATION

Cyber in aviation

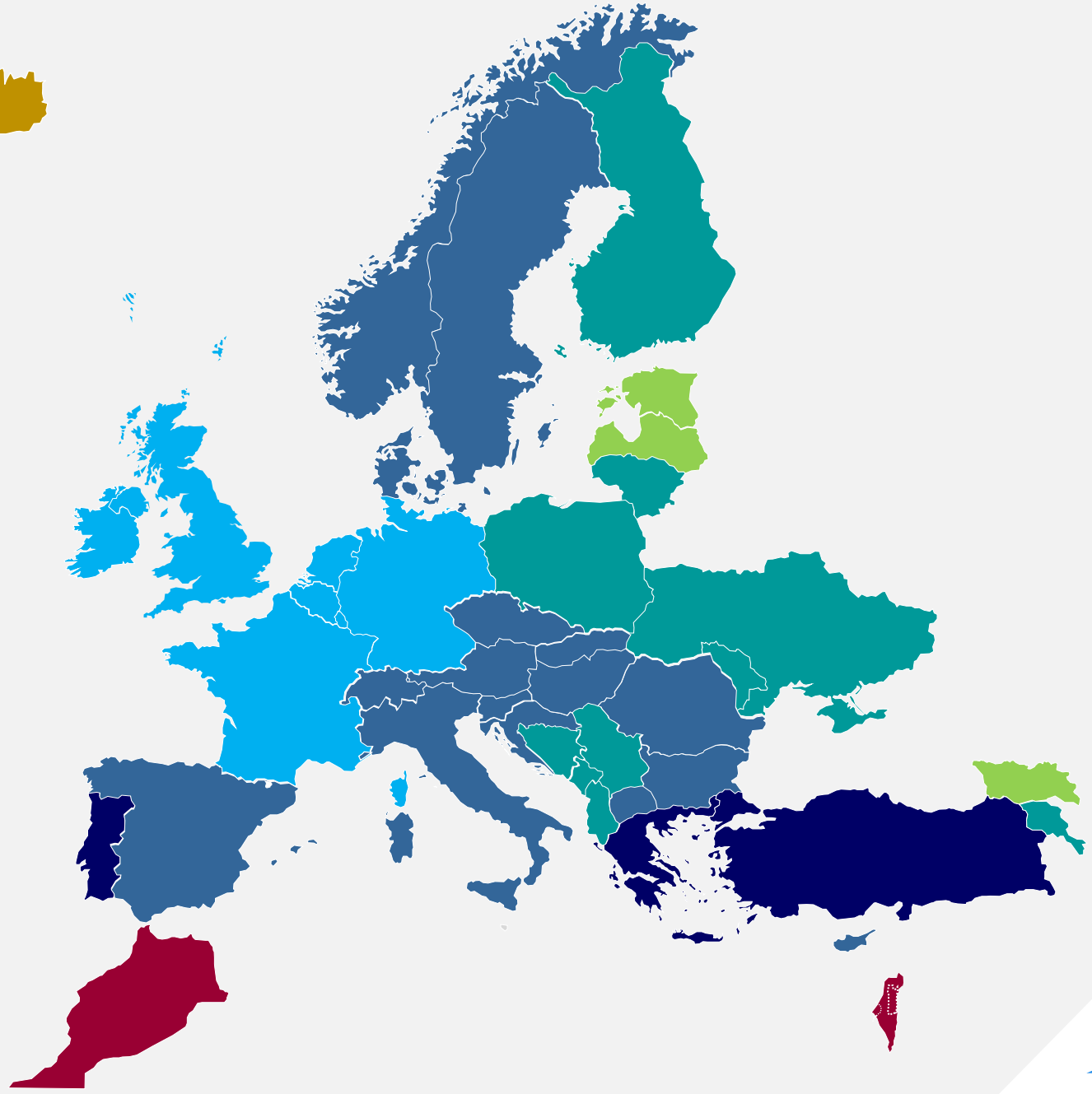
Patrick MANA

EUROCONTROL

EUROCONTROL is an inter-governmental, pan-European, civil-military organisation dedicated to supporting European aviation.

EUROCONTROL HISTORY

- 1960s
- 1980s
- 1990s
- 2000s
- 2010s
- 2025



2 ‘Comprehensive Agreement’ States: Morocco & Israel

EUROCONTROL

Building the Single European Sky !

Provide air traffic services in upper airspace
of Benelux & North-west of Germany

Manage the pan-European network

R&D => Deployment

Products

Collect route and
terminal charges

SUPPORTING
EUROPEAN
AVIATION

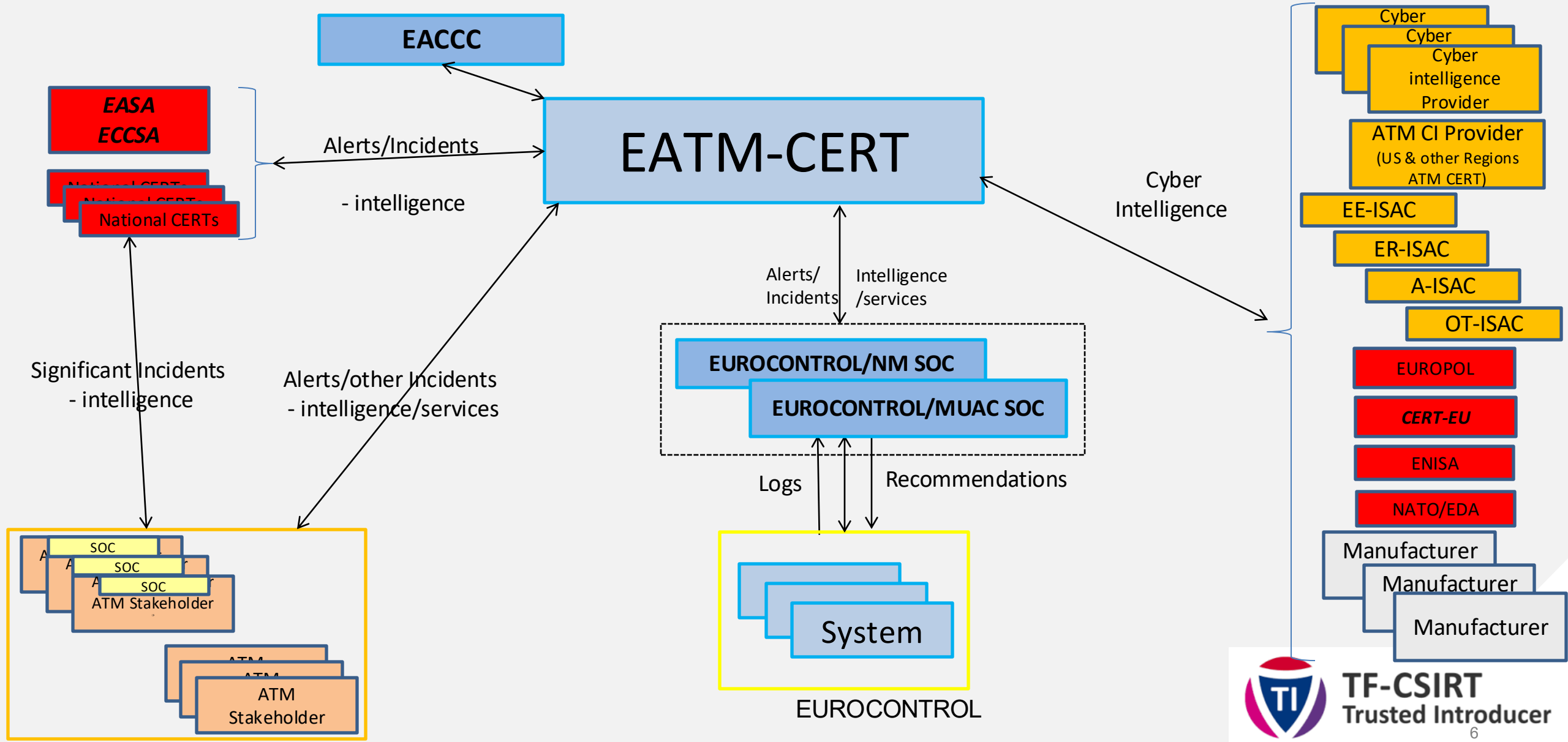
EUROCONTROL EATM-CERT

CONSORTIUM COORDINATOR sesar DEPLOYMENT MANAGER

FOUNDING MEMBER sesar JOINT UNDERTAKING

NETWORK MANAGER

Regional sectorial CERT: combine cyber and domain expertise



EATM-CERT services

1. Penetration test (EUROCONTROL services & products + Aviation stakeholders)
2. CRCO scams via email
3. Credentials leaks detection
4. Sensitive info leaks detection
5. Fraudulent websites (including takedown)
6. Cyber Threat Intelligence (CTI) and feeds for aviation
    1. Weekly briefing
    2. Quarterly cyber threat landscape report for senior management
    3. Annual report “cyber in aviation”
    4. TLP:CLEAR CTI tools – raising awareness - Cyber events map
    5. Alerts: MISP – cyber info sharing platform & email
7. Support to incident response / Artefacts analysis
8. Vulnerability scanning of Aviation Stakeholders
9. Training exercises (table-top & technical) - EATM-CERT CTF, Room42
10. Phishing awareness campaigns
11. Test of Anti-DDOS solutions

CTI – Weekly Briefings

EUROCONTROL

EATM-CERT

AVIATION CYBER THREAT BRIEFING - WEEK 14

18
Fraudulent websites impersonating airlines

4
Ransomware affecting aviation

6
Dark web incidents or events

BLUESKY

Aviation Cyber Threat News (in the media)

1. [EN] Anonymous Sudan claimed a series of attacks on Israeli airlines (EL-Al Airlines, Arkia Airlines, Israir, Ayeet Aviation and Cargo Aviation)

Israeli airlines was hit by a cyberattack and taken down by the hacker group Anonymous Sudan…Read the article.

2. [EN] Anonymous Sudan hackers group claims to have targeted Indian airport infrastructures.

Hacker group Anonymous Sudan made good on its threat to target Indian organizations.

BLUESKY

Aviation Cyber Threat News (in the media)

1. [EN] Anonymous Sudan claimed a series of attacks on Israeli airlines (EL-Al Airlines, Arkia Airlines, Israir, Ayeet Aviation and Cargo Aviation)

Israeli airlines was hit by a cyberattack and taken down by the hacker group Anonymous Sudan…Read the article.

2. [EN] Anonymous Sudan hackers group claims to have targeted Indian airport infrastructures.

Hacker group Anonymous Sudan made good on its threat to target Indian organizations.

After a DDoS attack on the Cochin International Airport's (CIAL) website over the weekend the threat group has listed six new targets…Read

Comment:

EATM-CERT has identified claims by the hacktivis distributed denial-of-service (DDoS) attacks targ airports and Israeli airlines.

The hacktivist "Anonymous Sudan" has launched for anti-Muslim activities and announced thes Palestinian conflict and Anti-Muslim Violence in In

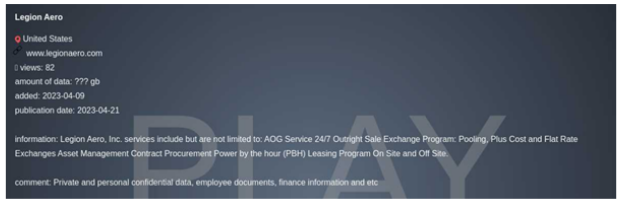
EATM-CERT cannot verify the validity of Anony attack occurred. We believe that the group's operations that align with Russian interests. EA situation for further developments.

DARKSKY

Detection of criminal activities on the Deep/Dark Web

TLP: AMBER

1. The operators of Play ransomware claimed to have compromised Legion Aero, an aircraft supply store in the US (legionaero.com).



CONFIDENCE: LOW

MITRE ATT&CK : T1486 - Data Encrypted for Impact

2. Aero Engine Solutions, a commercial aircraft parts, components, and accessories manufacturer in the US (aeroenginesolutions.com), and AV Industries, a provider of equipment and services to the airline industry in the US (avindustriesinc.com), was listed on the data leak site of RansomHouse.

KEY CYBER THREAT INDICATORS

Fraudulent websites impersonating airlines (IATA and A4E members)

Fraudulent websites impersonating aviation stakeholders

Publicly reported incidents/events (collected by EATM-CERT on the public internet)

Dark Web incidents/events (collected by EATM-CERT on the darkweb)

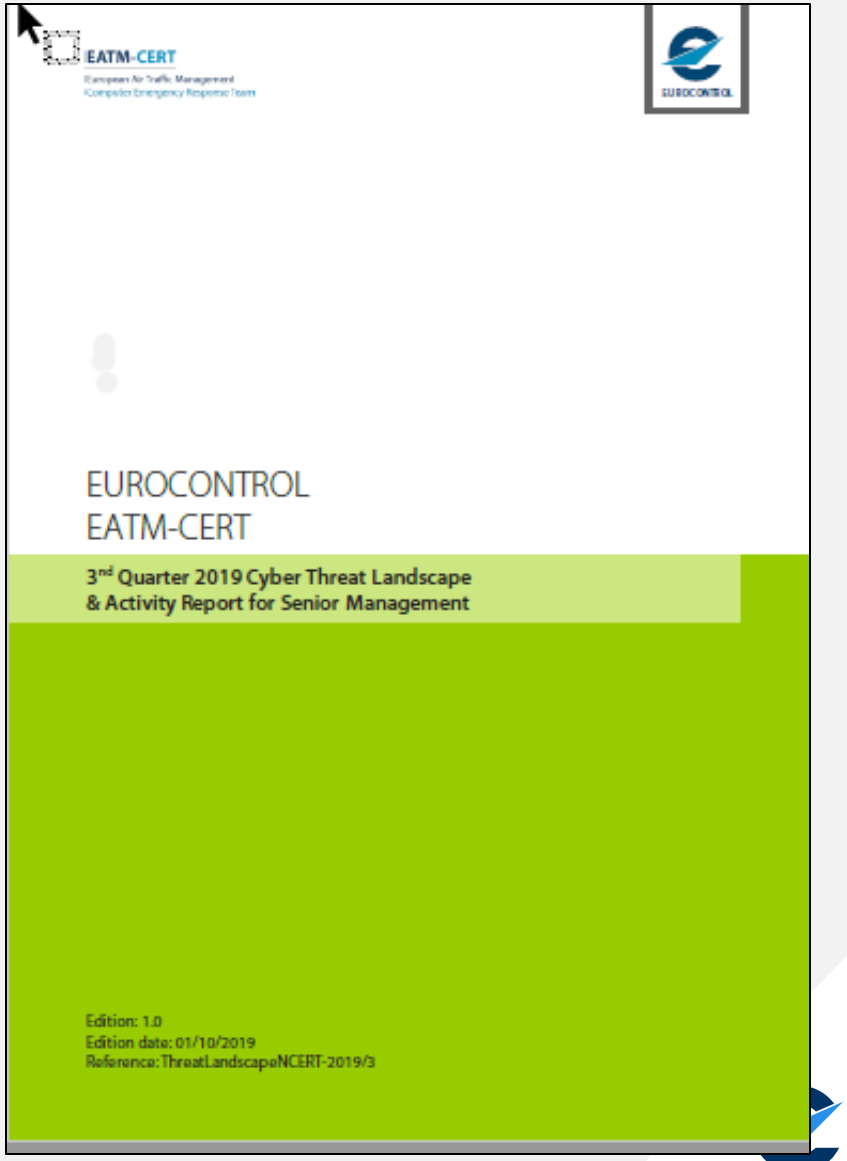
Ransomware affecting aviation (worldwide - Source: EATM-CERT)

EATM-CERT credential leak monitoring service users

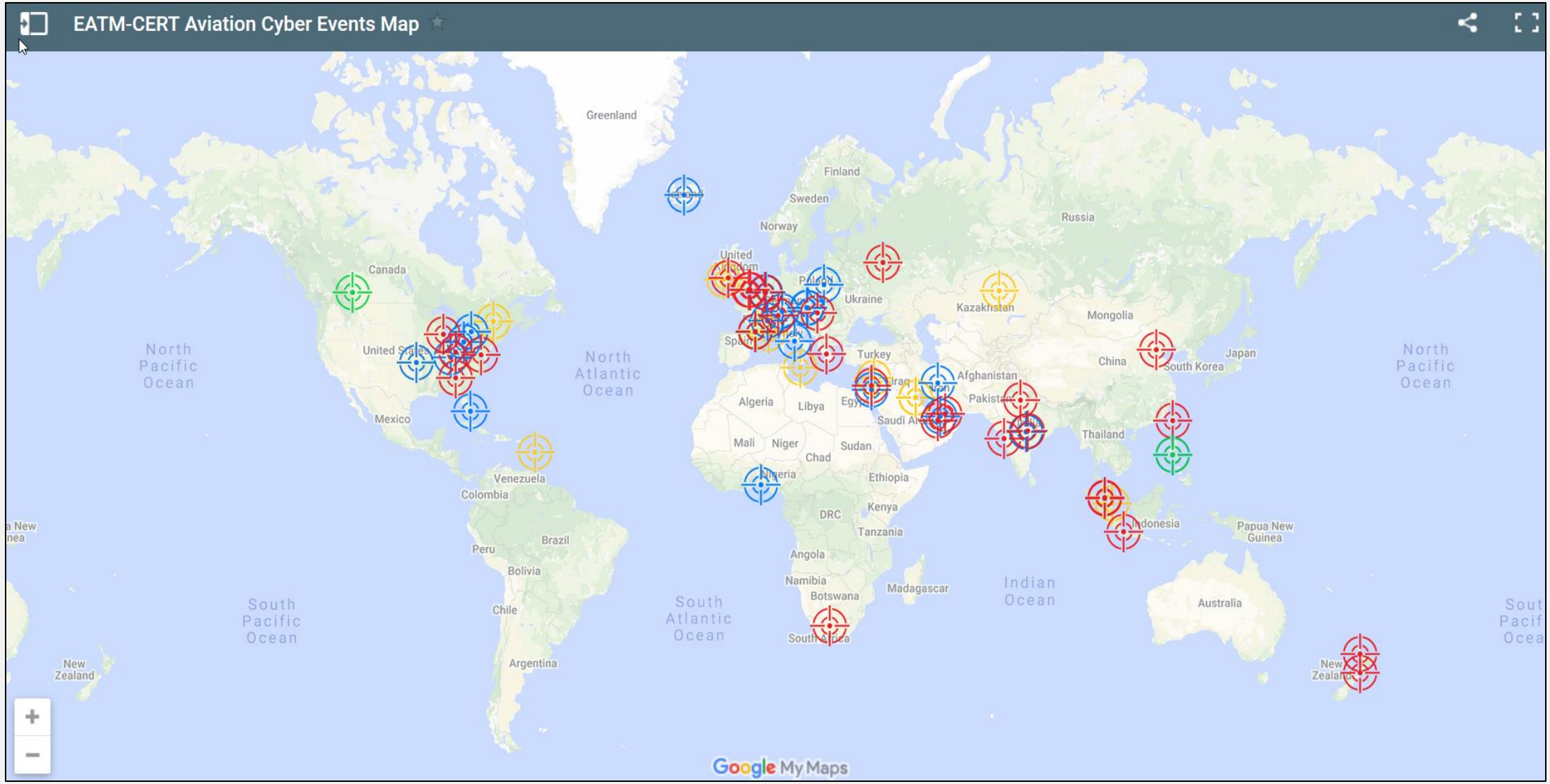
EATM-CERT Malware Information Sharing Platform (MISP) users

EATM-CERT vulnerability scanning service users

New
Total



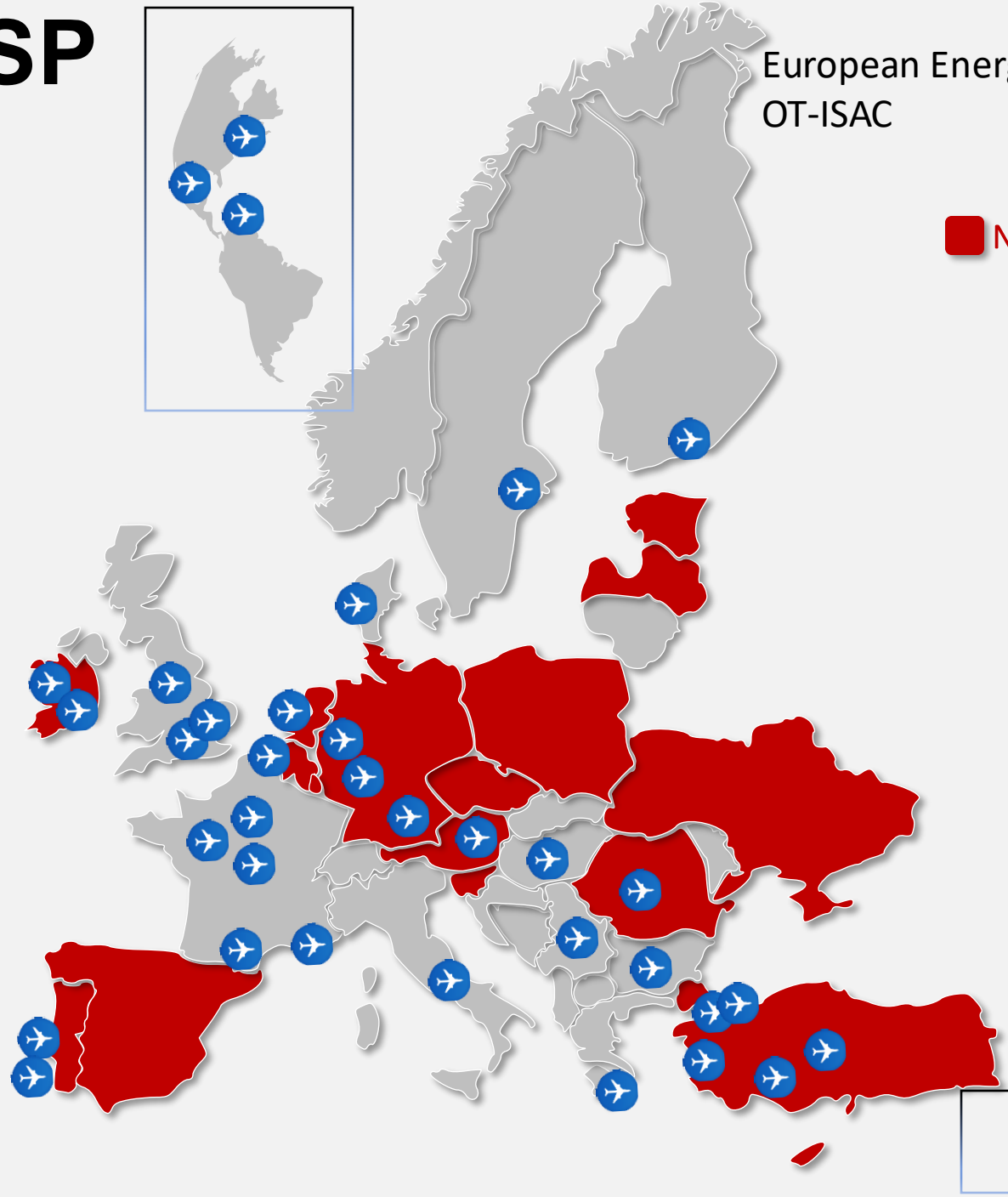
TLP:WHITE CTI tools – raising awareness



MISP

Aviation stakeholders

- Austria – Austrocontol (ANSP)
- Belgium – DHL
- Bulgaria - BULATSA (ANSP)
- Denmark - NAVIAIR (ANSP)
- Finland – Fintraffic (ANSP)
- France - CERT-AIRBUS A/C
- France - Groupe ADP
- France – DSNA
- France – Air France
- France – Air Caraïbes
- Germany - DLH – Lufthansa Group
- Germany - Frankfurt Airport
- Germany – Munich airport
- Greece - HANSP
- Hungary - HungaroControl (ANSP)
- International - IATA
- International – AMADEUS
- Ireland – Shannon airport
- Ireland – Dublin Airport
- Italy - Aeroporto Di Roma
- Mexico - Aero Mexico Airlines
- Netherlands - Schiphol Airport
- Portugal – ANA (airport)
- Portugal – SATA (airline)
- Romania - CAA-RO
- Serbia - SMATSA (ANSP)
- Sweden - Swedavia (airports)
- Turkey - CERT-THY (Turkish Airlines)
- Turkey - DHMI (ANSP)
- Turkey - IGA Istanbul Airport
- Turkey - Celebi Ground ops
- Turkey – SGIA Airport
- UK - British Airways
- UK - Heathrow Airport
- UK – Manchester Airport Group



European Energy ISAC
OT-ISAC

NATIONAL CERT/NCSC

- **Austria** (CERT.at)
- **Belgium (CERT.be)**
- **Cyprus (CSIRT-CY)**
- Czech republic (CSIRT.cz)
- **Europe .eu (CERT-EU)**
- **Estonia** (CERT-EE)
- **Germany** (CERT-Bund)
- **Ireland (CSIRT-IE)**
- **Israel (CERTGOVIL)**
- **Latvia (CERT.LV)**
- **Luxembourg** (CIRCL)
- **Netherlands** (NCSC-NL)
- **Poland** (CERT.GOV.PL)
- **Portugal** (CERT-PT)
- Romania (CERT-RO)
- **Slovenia** (SI-CERT)
- **Spain** (INCIBE-CERT)
- **Spain** (CCN-CERT)
- Turkey (TR-CERT)
- Ukraine (CERT-UA)

Israel

EUROCONTROL

EUROCONTROL

SUPPORTING
EUROPEAN
AVIATION

Aviation cyber threat landscape

CONSORTIUM COORDINATOR sesar DEPLOYMENT MANAGER

FOUNDING MEMBER sesar JOINT UNDERTAKING

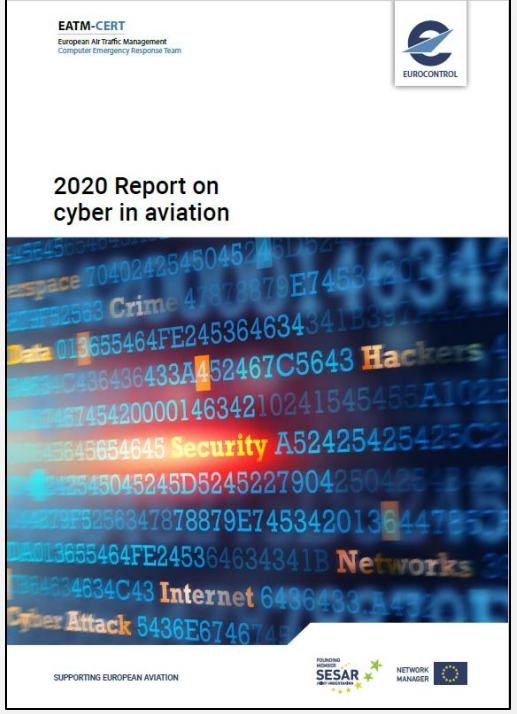
NETWORK MANAGER

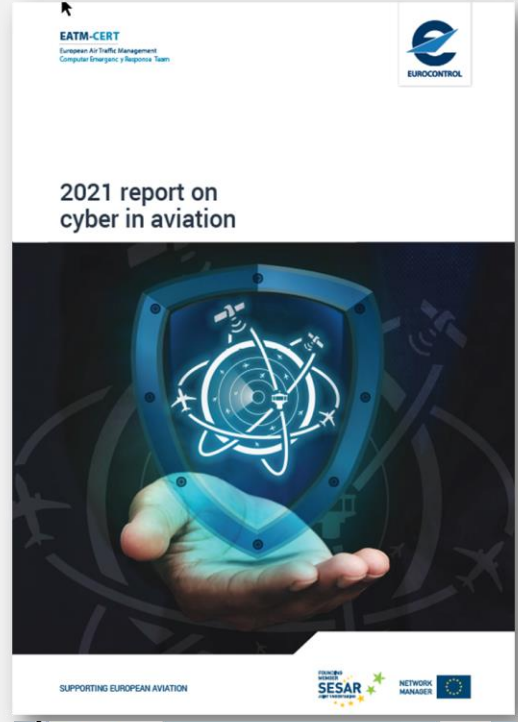
Report on cyber in aviation

- Annual Report on cyber in aviation
- Contributors from five continents
- More entities are contributing year after year
- Trusted and de-identified exchange of cyber events and attacks
- 8.630 **reported** events in 2024
- 6.320 **reported** events in 2023
- 2.700 **reported** events in 2022

EATM-CERT

TLP:GREEN





Overview – who is affected

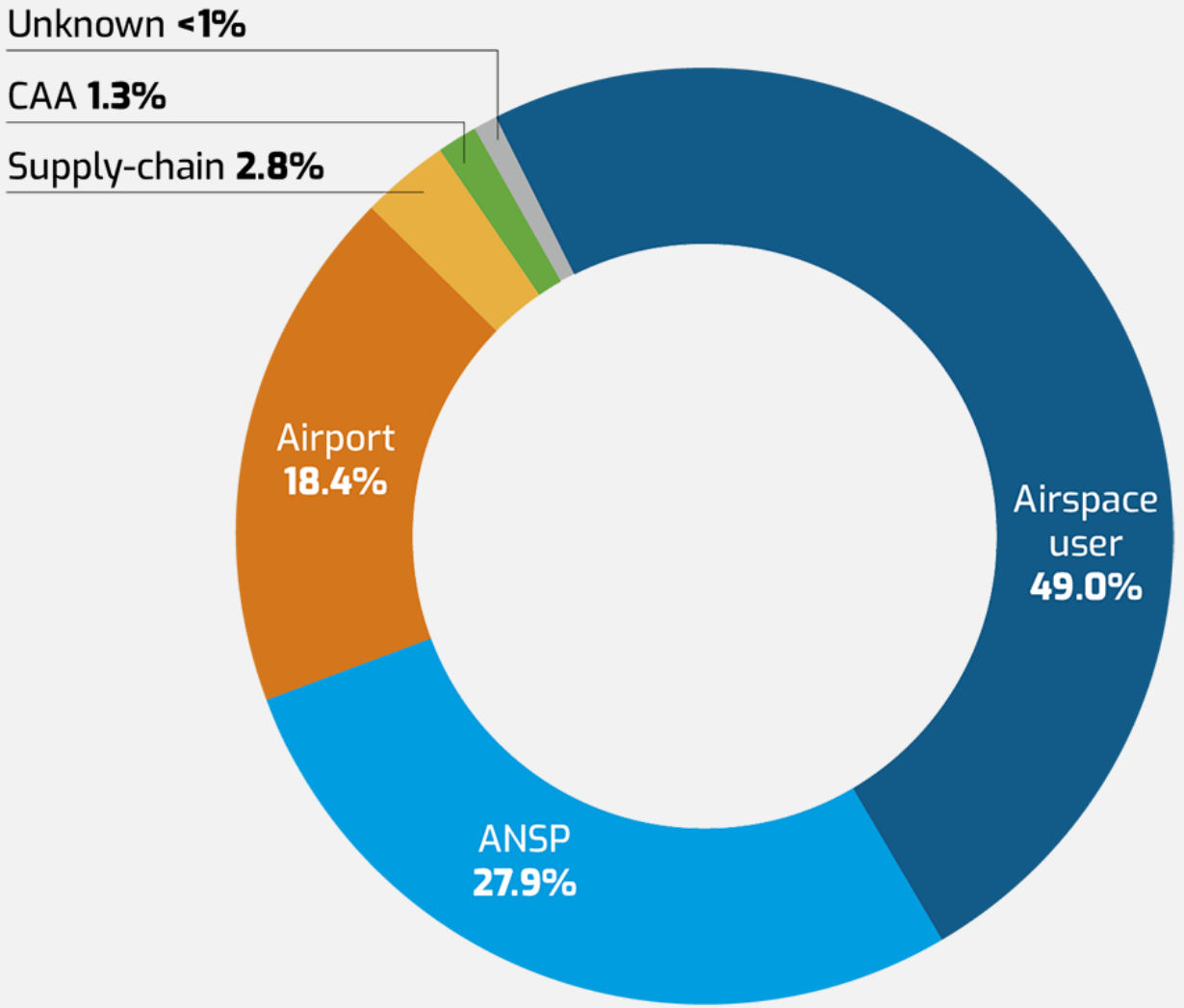


Figure 1: Global Aviation Threat Landscape - Victimology

Overview - why

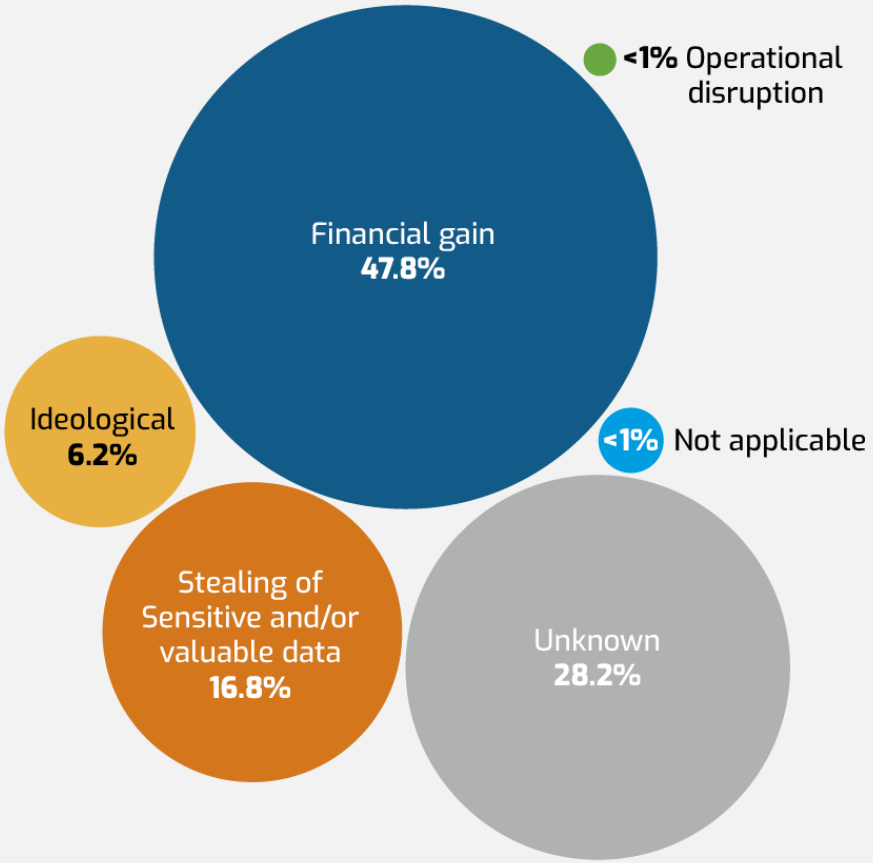


Figure 3: Global Aviation Threat Landscape - Motivation Distribution

EATM-CERT is not aware of any cyber incidents that compromised flight safety in 2024 (except due to GNSS RFIs)

TLP:GREEN

EUROCONTROL

Overview – by whom

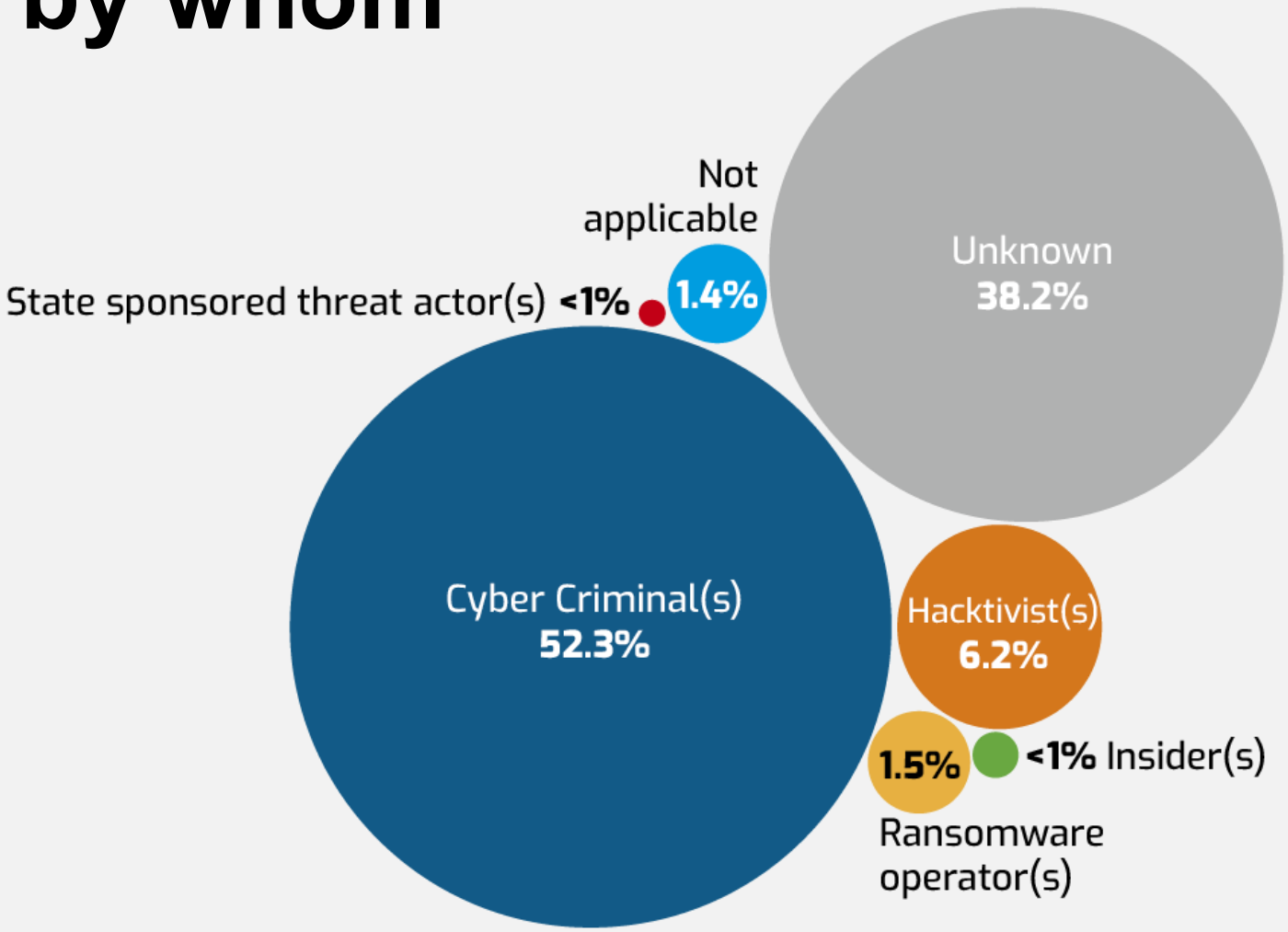


Figure 6: Global Aviation Threat Landscape - Threat Actor Distribution

Overview – how

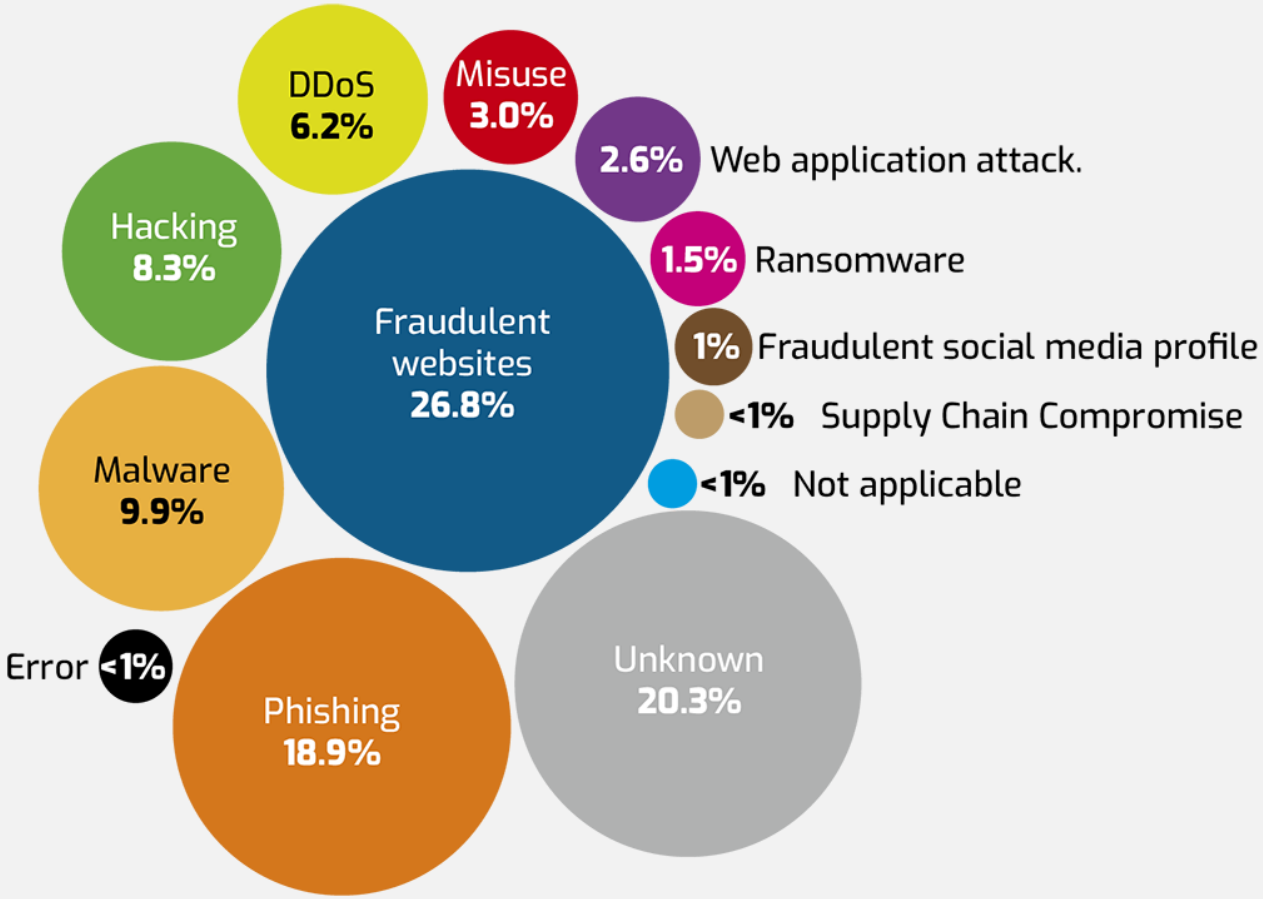
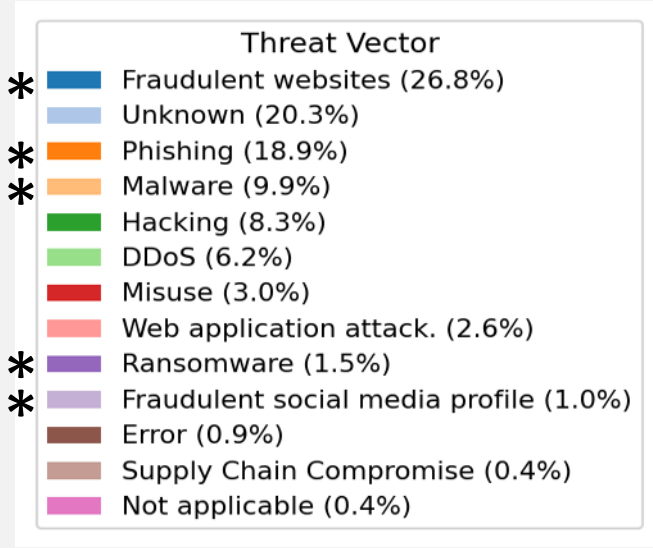


Figure 2: Global Aviation Threat Landscape - Threat Vector Distribution



*: augmented using AI

EUROCONTROL

Airspace users – by whom and why

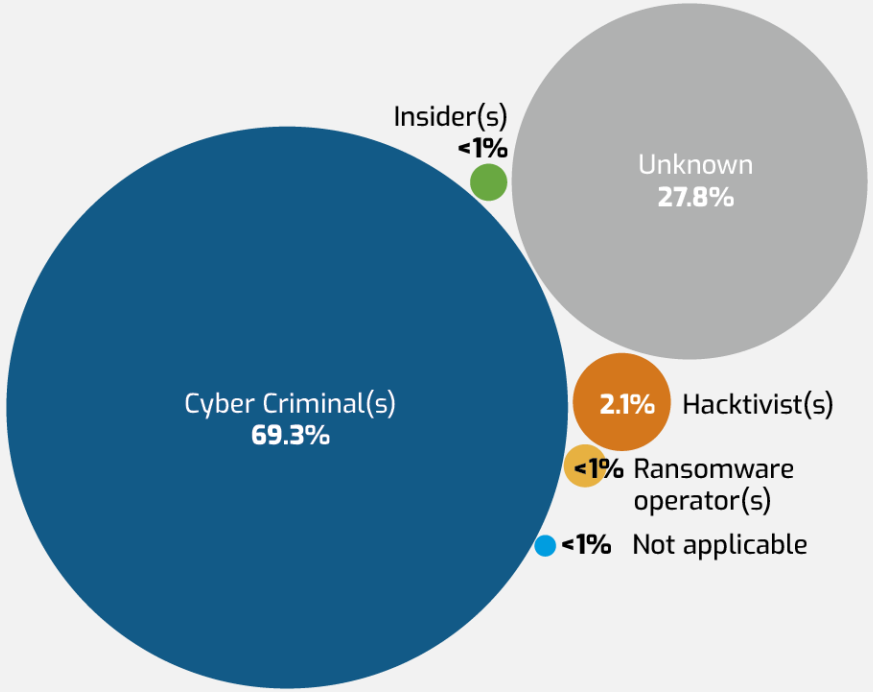


Figure 27: Attacks against Airspace users - Threat Actor distribution

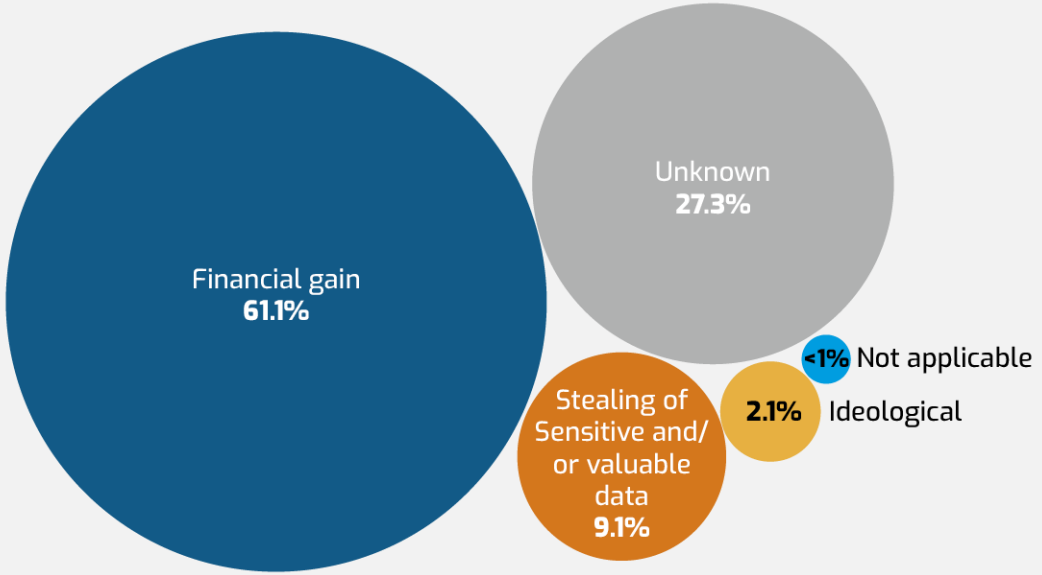


Figure 29: Attacks against Airspace users - Threat Vector distribution

Airspace Users – impact

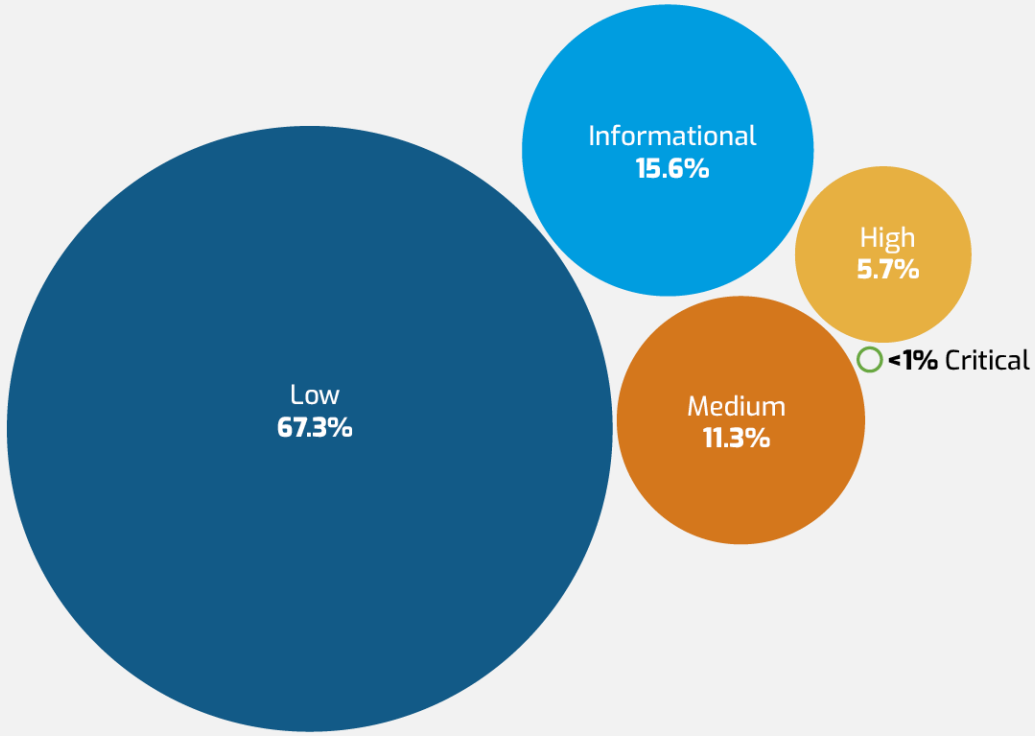


Figure 47: Attacks against Airspace users - Severity distribution

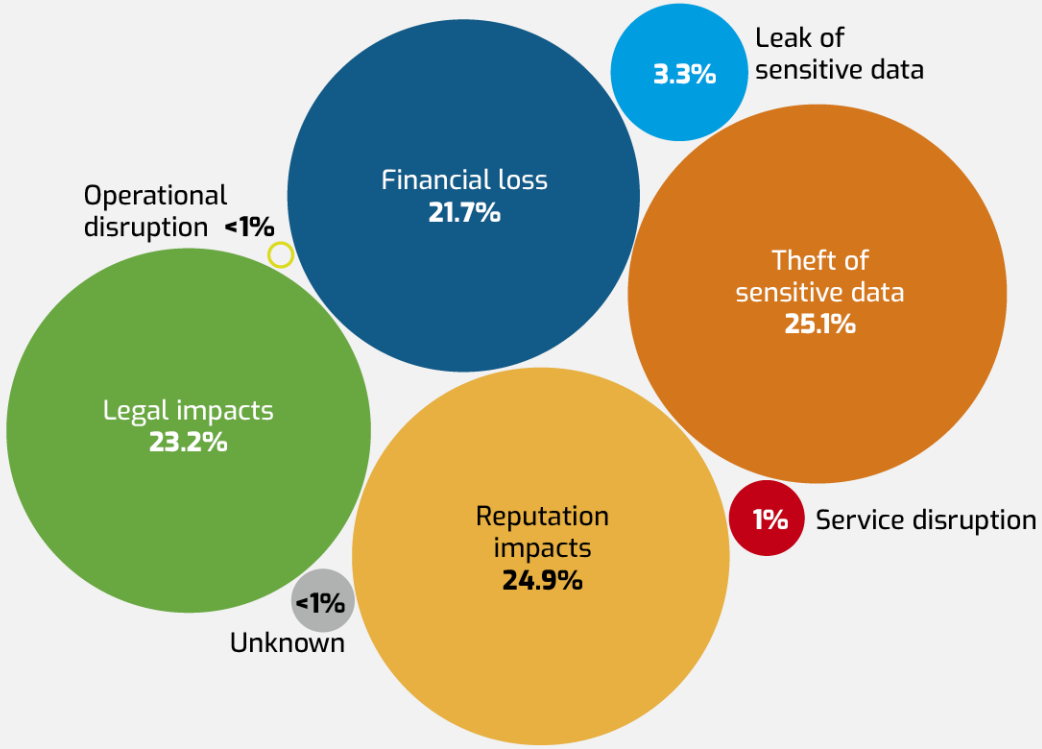


Figure 48: Attacks against Airspace users - Impact distribution

EUROCONTROL

Airspace Users – how

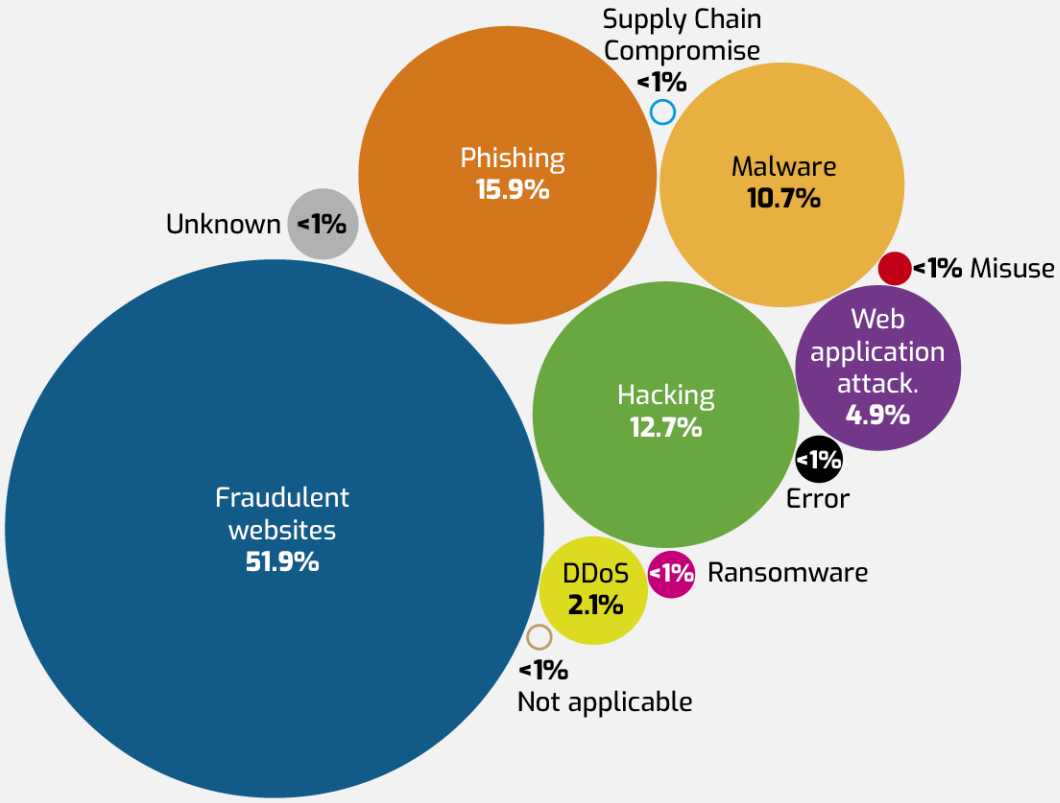


Figure 28: Attacks against Airspace users - Threat Vector distribution

What protection

- **Detection means** (MITRE ATT&CK)
  - **Application Log / Logon Session** (DS0015, DS0028) and **Command** (DS0017) – These offer deep visibility into system-level events, useful in identifying unusual access patterns or script-based automation.
  - **Network Traffic** (DS0029), **Process** (DS0009), and **Script** (DS0012) also stand out, reinforcing the importance of network and process telemetry in identifying both phishing payload execution and scripted reconnaissance.
  - **File-based detections** like File (DS0022) provide post-interaction insight, potentially flagging data exfiltration attempts.
- **Mitigation means** (MITRE ATT&CK)
  - **User Account Management** (M1018) and **User Training** (M1017) - Strengthening user provisioning and awareness could help reduce the likelihood of users falling for phishing or entering credentials on spoofed portals.
  - **Audit** (M1047) and **Multi-factor Authentication** (M1032) offer visibility and access control respectively important steps in reducing the success rate of identity-related attacks.
  - Additional entries like **Behavior Prevention on Endpoint** (M1040), **Update Software** (M1051), and **Execution Prevention** (M1038) indicate best practices in endpoint hygiene and hardening that could help prevent delivery or execution in more advanced cases.

EUROCONTROL

EUROCONTROL CRCO Impersonation Frauds

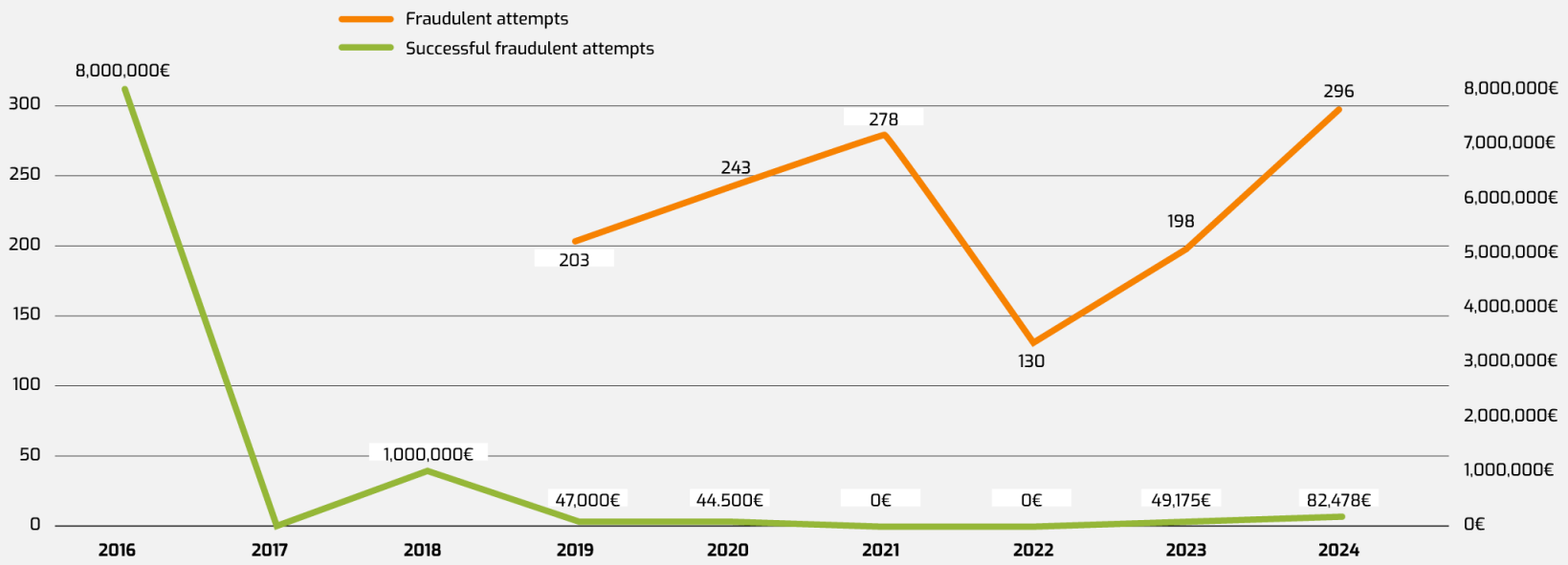


Figure 45 Annual losses reported by stakeholders due to scams impersonating EUROCONTROL.

```
Subject: Unpaid Invoices
To: me <r3.crco@eurocontrol.int>
From: r3.crco <r3.crco@eurocontrol.int>
Date: Sun, 06 Dec 2020 20:49:05 -0800
Reply-To: r3.crco <r3.crcoeurocontrol.ints@gmail.com>

You will not see this in a MIME-aware mail reader.
--===============0666264462==
Content-Type: text/plain; charset="iso-8859-1"
MIME-Version: 1.0
Content-Transfer-Encoding: quoted-printable
Content-Description: Mail message body

Dear Accounts Team,     Would you please let us know the status of your Oct=
ober November and December invoices. On review of your files,  We discovere=
d that these invoices are still in arrears.    Kindly please confirm the st=
atus of these invoices below.    501018200123 501028991020 501900189028    =
 Please let us know if payment has been paid or not. Provide the copy of th=
e proof of payment with Invoice number and amount.   So as to enable us rec=
oncile and update your account accordingly.   In order to make sure that th=
e bills you receive are authentic, please consult and download them from th=
e CRCO Extranet For Airspace users (CEFA): https://www.eurocontrol.int/tool=
/cefa Kindly send us a copy stamped by return mail from now on.   We have s=
ent out new invoices for your reference kindly notify us by return mail whe=
n you receive it.     Thanks once again for your understanding and cooperat=
ion.   Kind Regards, Nancy Coveliers Collection of Charges CECO/R4 EUROCONT=
ROL  96 Rue de la Fusee 1130 Brussels Email: r3.crco@eurocontrol.int Teleph=
one: +32 460 222 485
--===============0666264462==
```

TLP:GREEN

EUROCONTROL

EUROCONTROL CRCO Impersonation Frauds

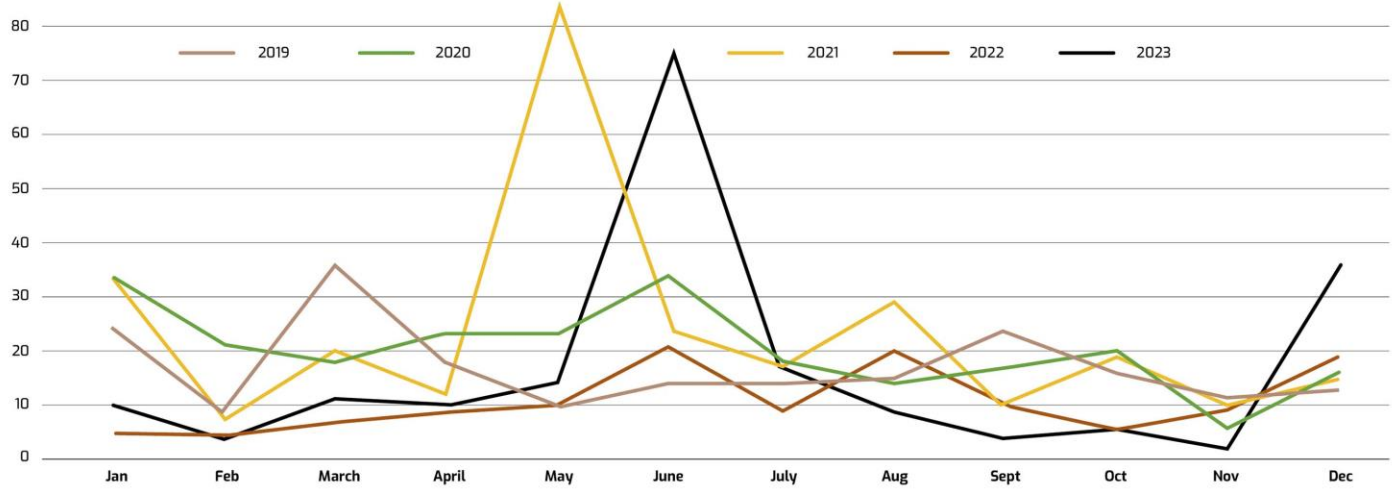


Figure 42: Scams Impersonating EUROCONTROL

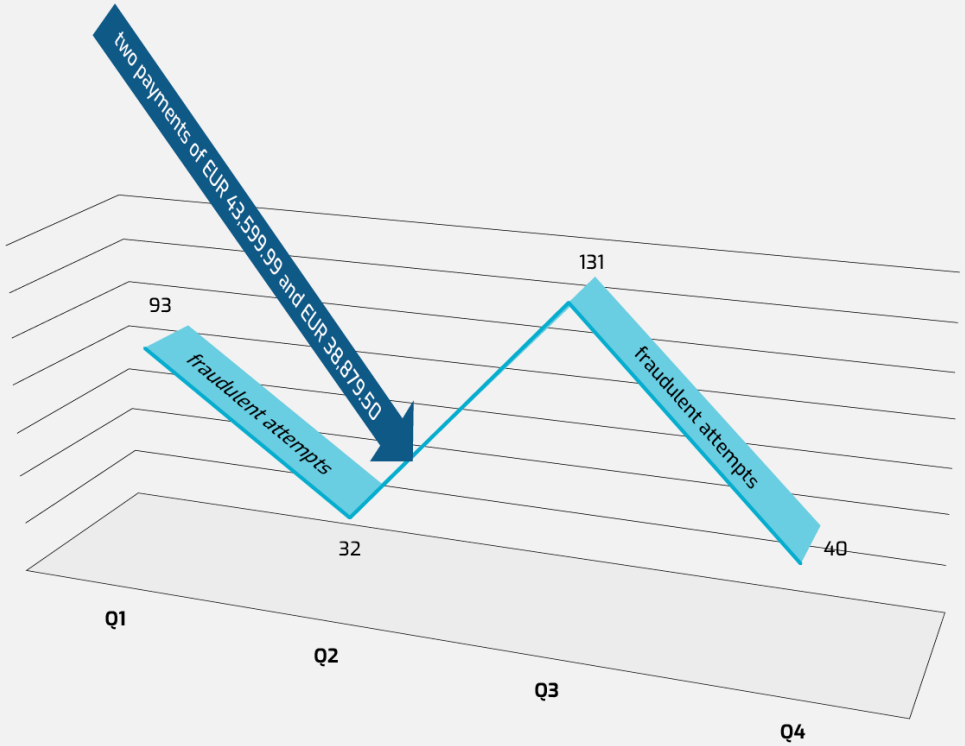


Figure 46: Increase in Fraudulent Attempts Following Each Successful Attack

TLP:GREEN

EUROCONTROL

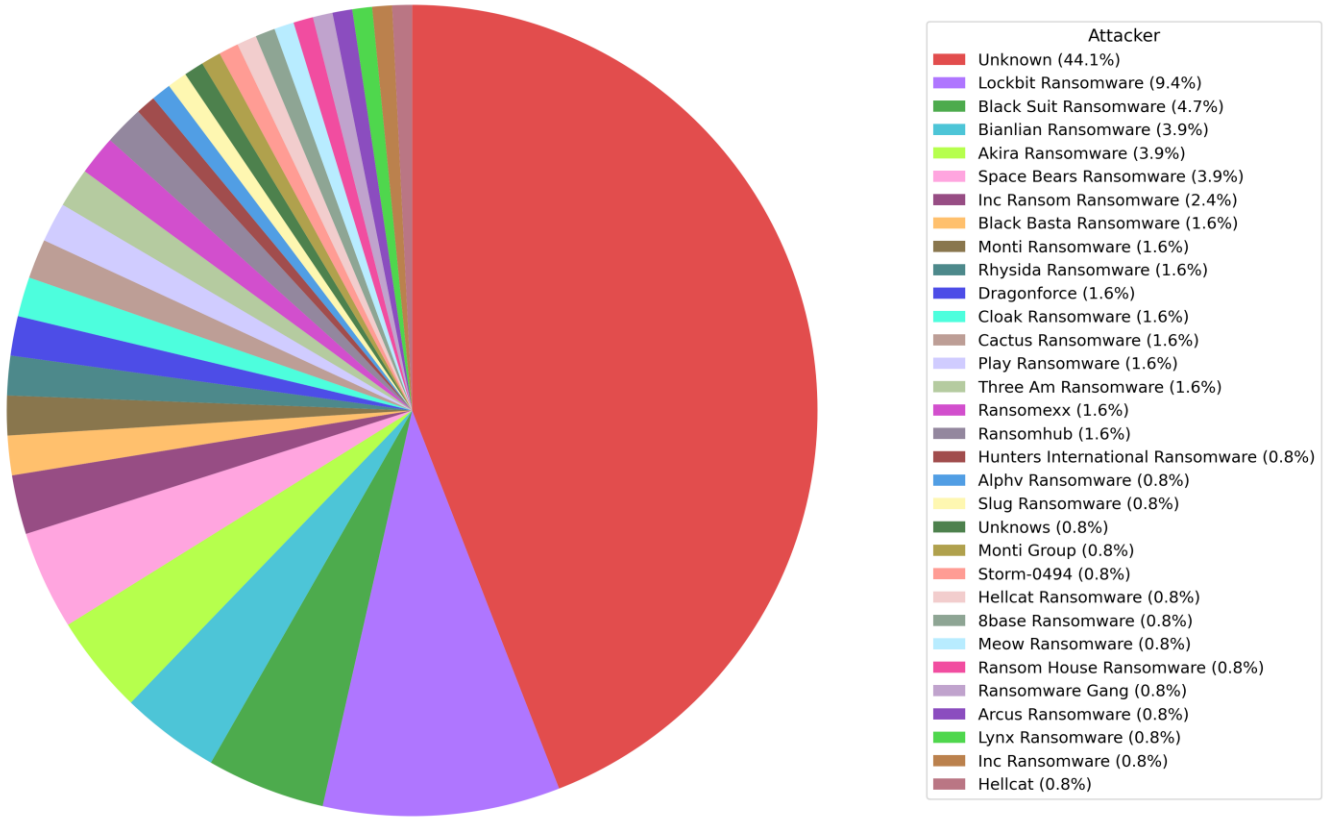
Ransomware on aviation

2024: 127

2023: 108

2022: 97

2021: 119



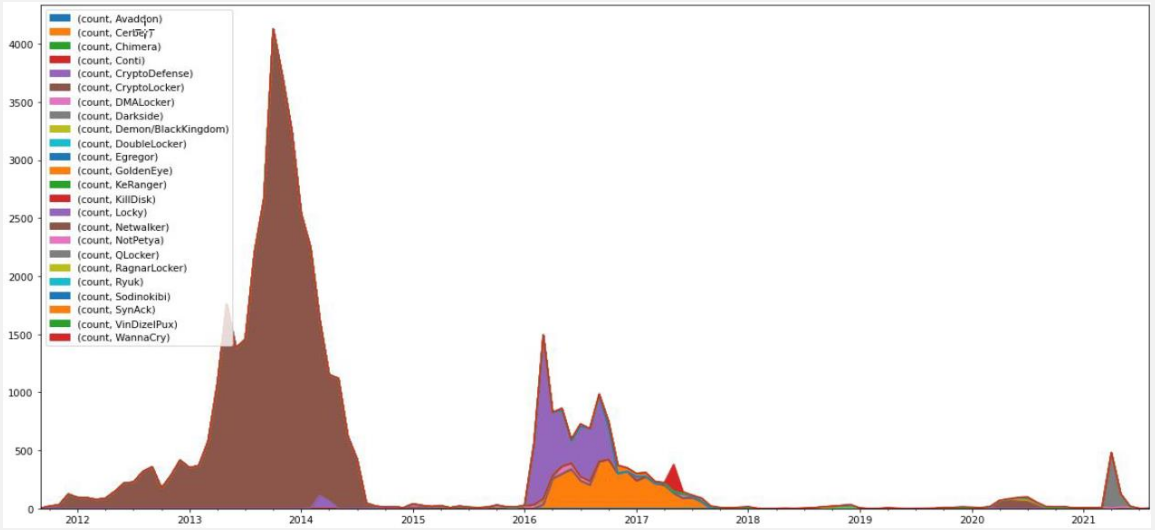
Main initial vectors:
- Spearphishing
- Stolen credentials

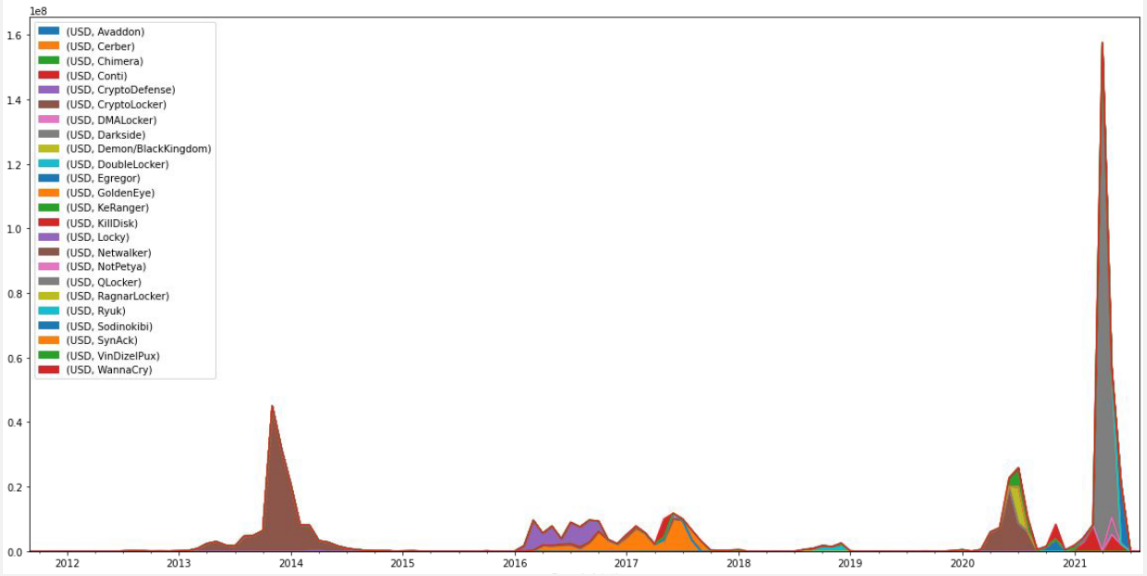
Double and even triple extorsion

TLP:GREEN

Ransomware (all sectors)

Number of ransoms paid monthly
(source Eireann LEVERETT – Waratah)

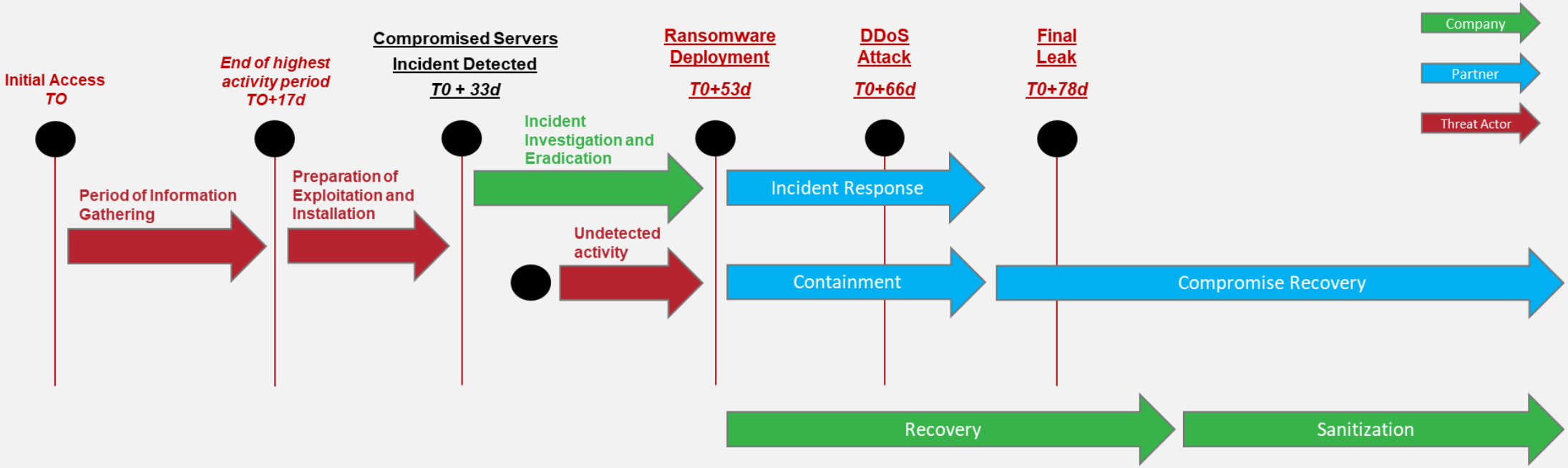




Amount of money earned monthly
(source Eireann LEVERETT – Waratah))

Big Game Hunting

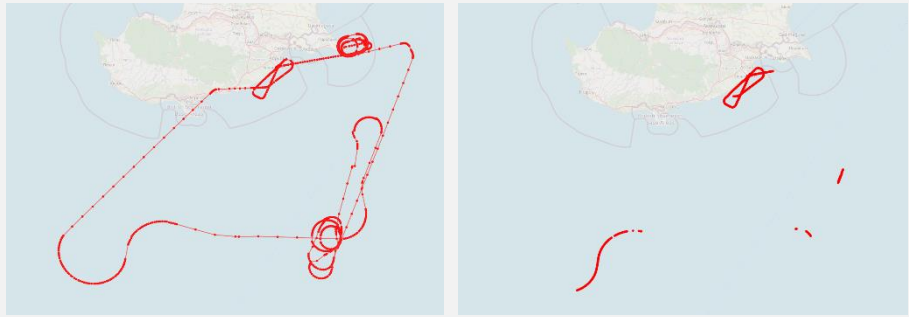
Ransomware – a real case

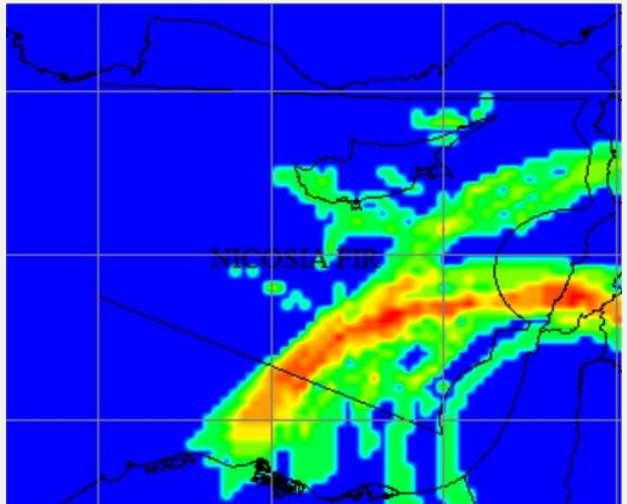


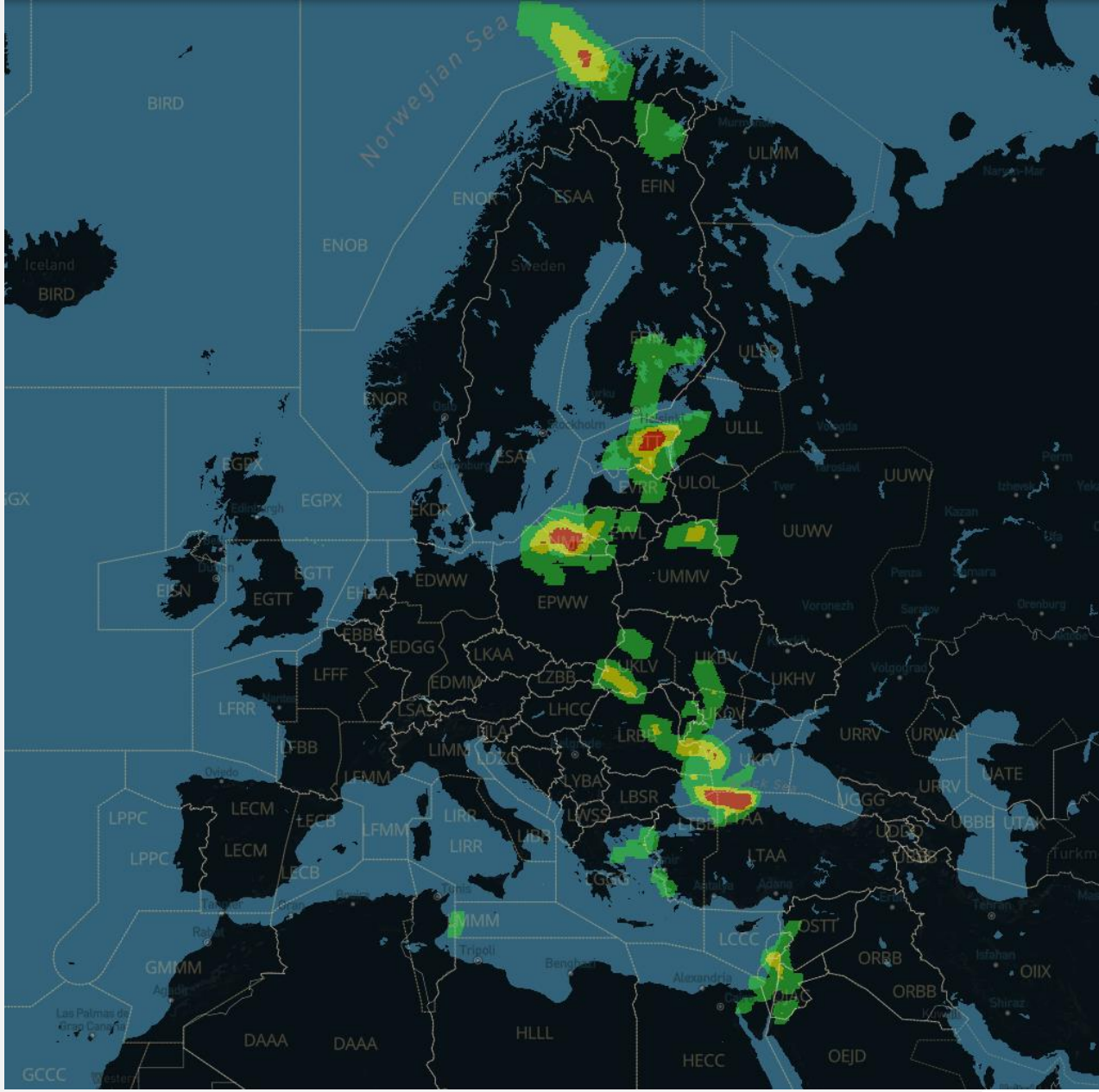
What happened:	Immediate actions:
• Compromised servers detected and addressed – T0 • Incident investigation and eradication ongoing • Ransomware detected and mitigated – T0+53d • No operational impact but several servers were encrypted • DDoS attack mitigated – T0+66d	• Focus on initial containment • Engaged a Partner for incident response, containment and recovery • Critical services and applications recovery from backups • Crisis committee setup • Incident reported • Internal and external communication

GNSS Interferences

Between early 2004 and August 2024, civil airliners were experiencing up to 1,500 cases of "spoofing" per day, primarily in and around conflict zones







TLP:GREEN

EUROCONTROL

SUPPORTING
EUROPEAN
AVIATION

AI & cyber

CONSORTIUM COORDINATOR sesar DEPLOYMENT MANAGER

FOUNDING MEMBER sesar JOINT UNDERTAKING

NETWORK MANAGER

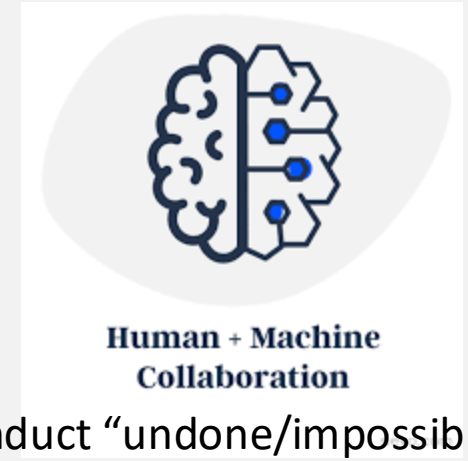
AI for cyber and other domains

Increase productivity

Save resources

Focus on adding value

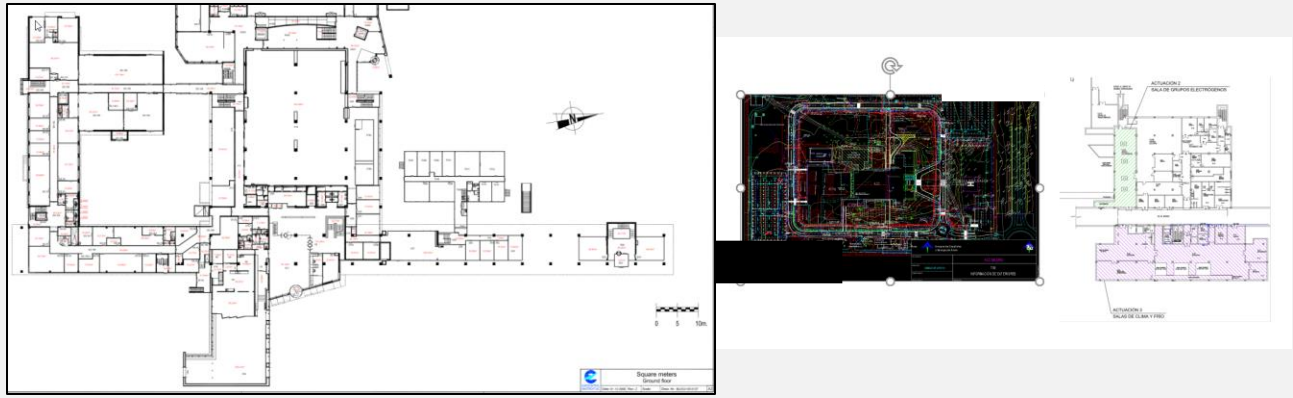
Challenge completeness



Conduct “undone/impossible” analyses

Dedicated and protected knowledge database

Document leaks



Very limited risk as it runs on an isolated PC (docs to be analysed can be corrupted)

Our AI App (LSD)

98% efficient

Total number of matches during the proof of concept

01/01/2019 to 25/06/2019

Live Monitoring

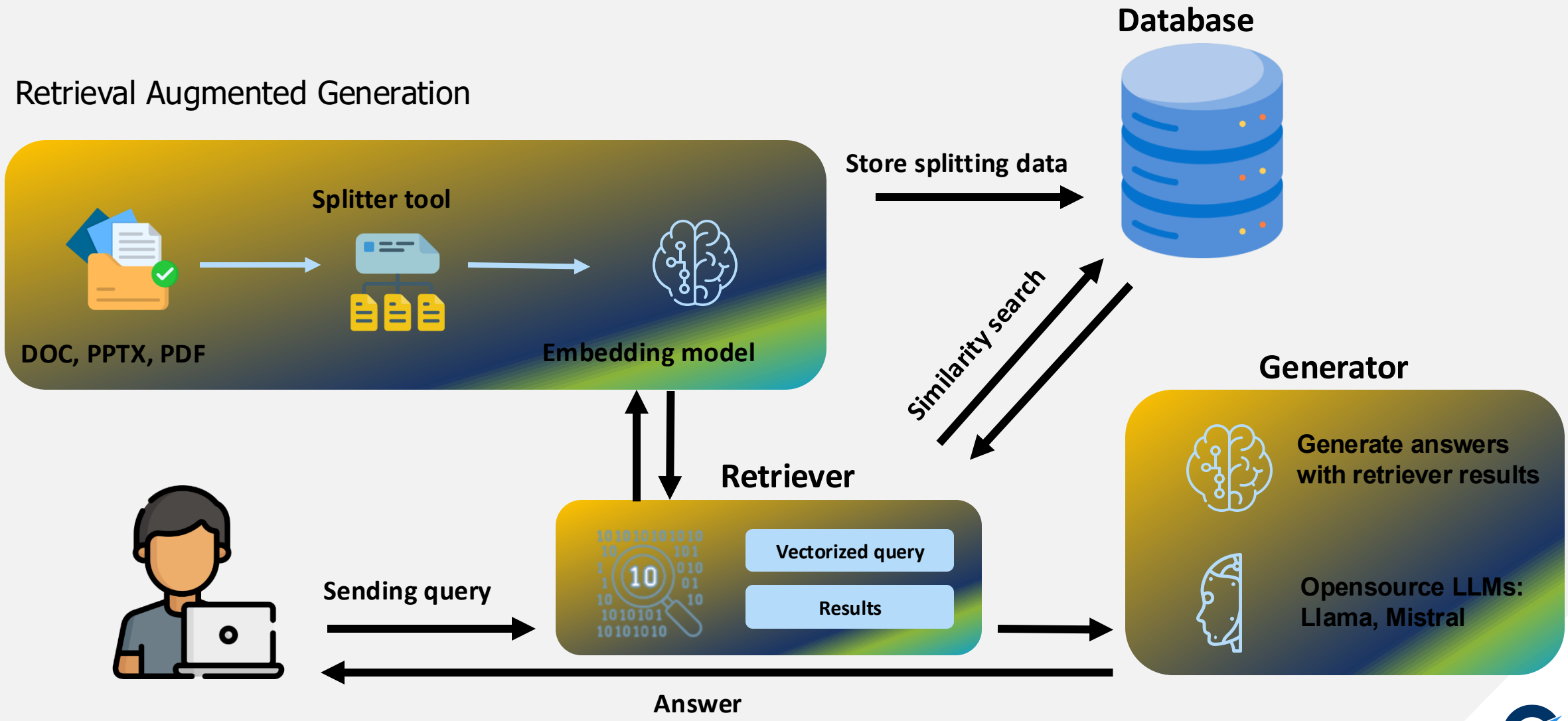
	Connected storage	Dark & Deep Web	Clear Web
Number of **matches**	+2.800.000		
Number of **AI filtered data**	~33.000	~14.000	~8.000
Number of **relevant and qualified incidents**	16	15	2

LSD lessons learned

- Service which can be provided only if AI app available
- App dev:
  - 9 man-month effort
  - 90% time
    - Data prep
    - Find/create artefacts (distorted logos, docs in 6 ICAO languages, “all aviation”, “bad” docs) to train the model
    - (re)Train model
- Initial performance with 30,000 docs: 95% … unusable
- Increase to 300,000 docs to reach 98% perfo

... Then came LLM

RAG: LLM on a local protected knowledge database

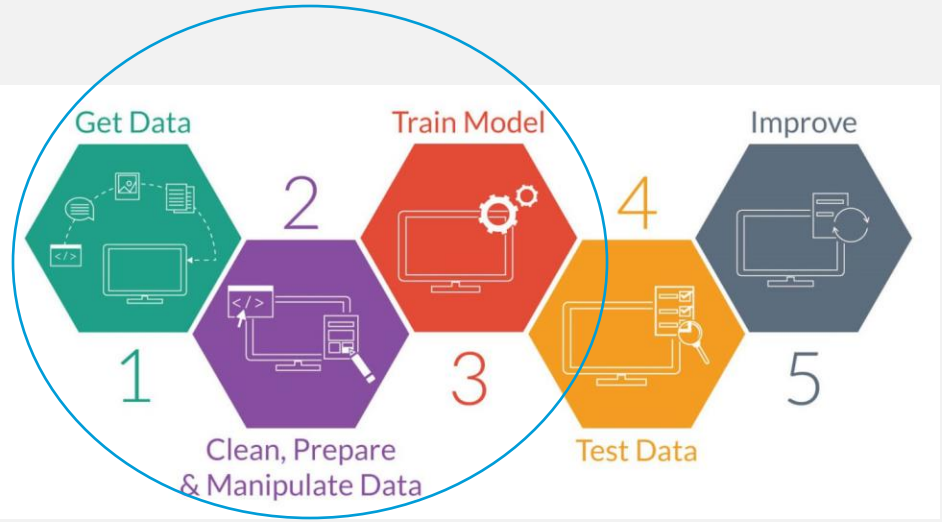


AI = yes, however, some challenges

Sensitivity
Corruption
+
Vulnerability as any app

Biased view

Don’t trust blindly

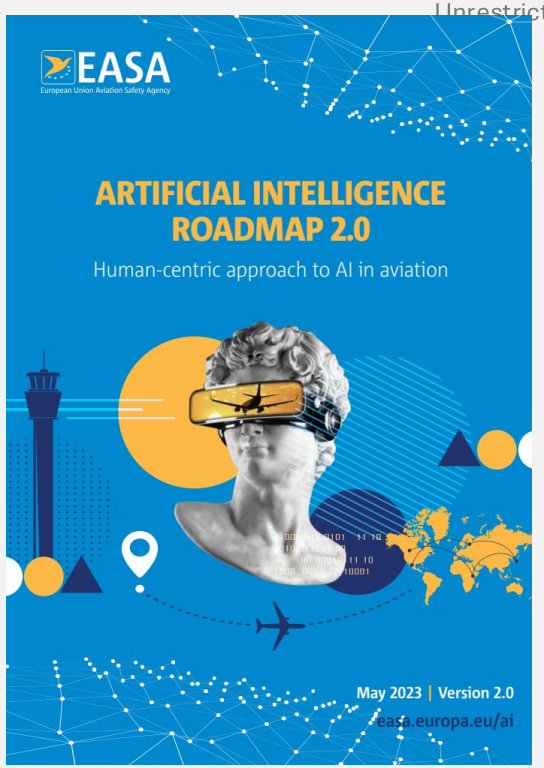


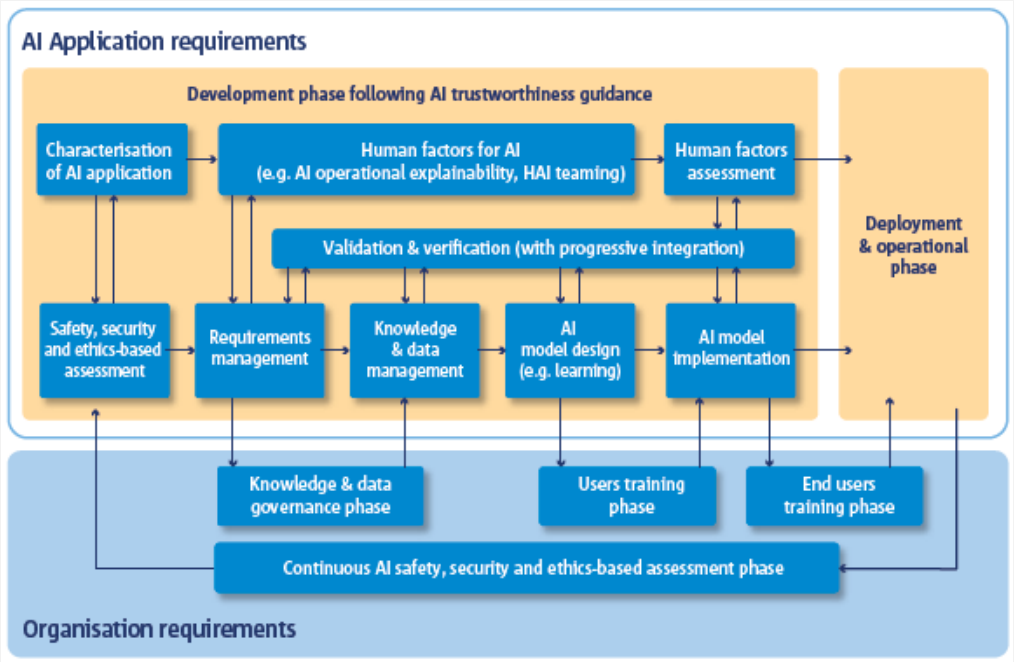
Amount and variety of data to train models

Data sharing

EASA - Regulatory approach

- Create a framework for AI trustworthiness and for enabling readiness for the use of AI in aviation





Level 1 AI: assistance to human	Level 2 AI: human-AI teaming	Level 3 AI: advanced automation
• Level 1A: Human augmentation • Level 1B: Human cognitive assistance in decision-making and action selection	• Level 2A: Human and AI-based system cooperation • Level 2B: Human and AI-based system collaboration	• Level 3A: The AI-based system performs decisions and actions that are overridable by the human. • Level 3B: The AI-based system performs non-overridable decisions and actions (e.g. to support safety upon loss of human oversight).

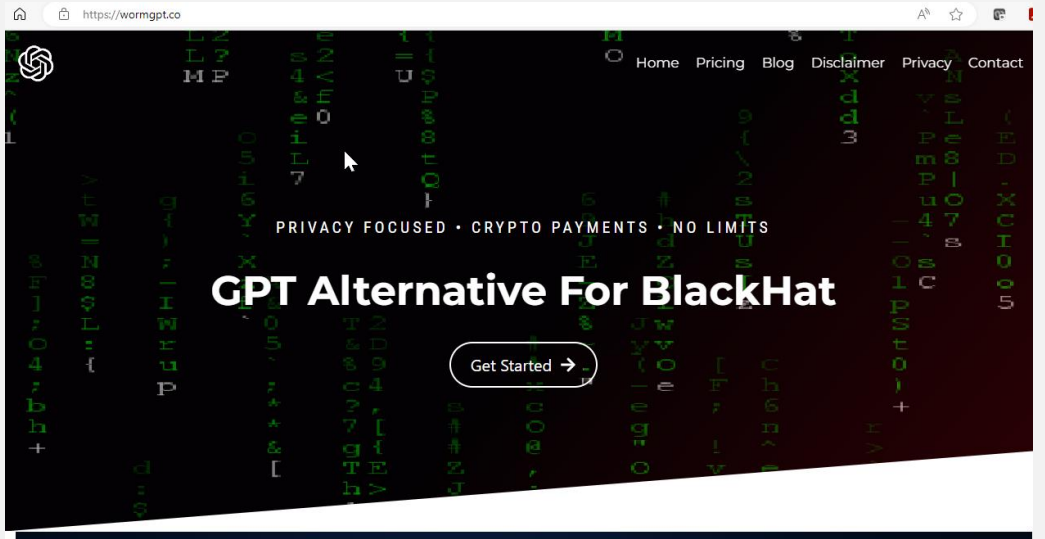
EUROCONTROL

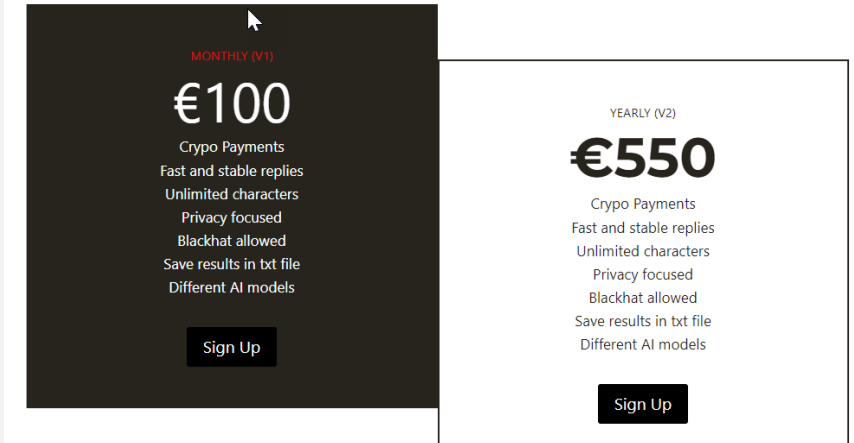
AI for cyber: also a threat

- More sophisticated attacks
- Reduced cost to produce a cyber-attack
- More accessible

… and it’s only the beginning

😢





SUPPORTING
EUROPEAN
AVIATION

Cloud secure by default

CONSORTIUM COORDINATOR sesar DEPLOYMENT MANAGER

FOUNDING MEMBER sesar JOINT UNDERTAKING

NETWORK MANAGER

Status

- Website: www.securitybydefault.org
  - Supportive community
  - Manifesto
  - Publications
- Manifesto can still be signed

- Microsoft
  - Set of default settings shared with Microsoft (Azure and M365) – based on users' input
- AWS & GCP
  - Default settings under development – input welcome

Next steps

- Microsoft implementation of default settings

- Finalise default settings for AWS and Google GCP
- Push other cloud service providers to adopt a similar approach

THANK YOU

eatm-cert@eurocontrol.int
patrick.mana@eurocontrol.int

SUPPORTING
EUROCONTROL
AVIATION

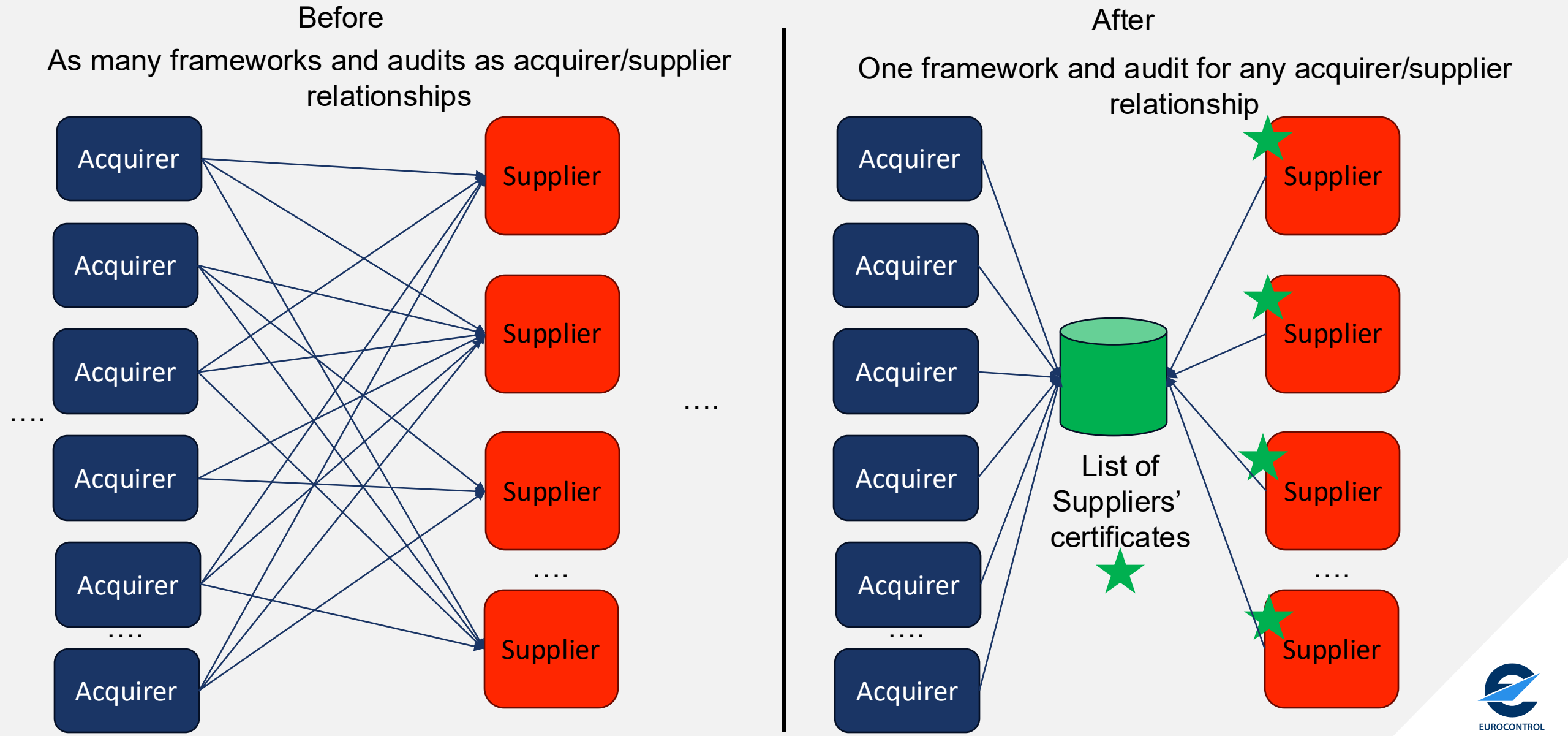
Supply chain cyber maturity

CONSORTIUM COORDINATOR sesar DEPLOYMENT MANAGER

FOUNDING MEMBER sesar JOINT UNDERTAKING

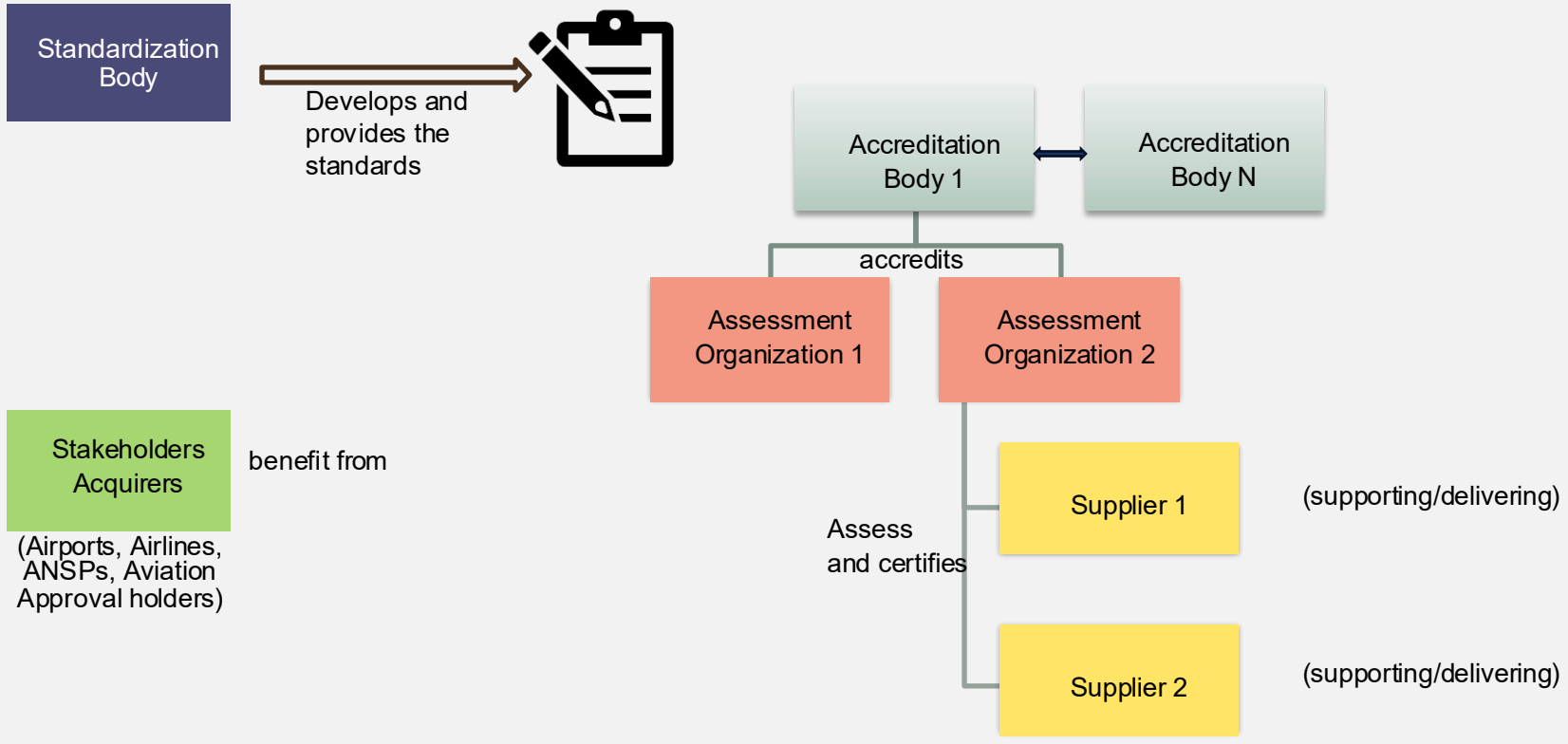
NETWORK MANAGER

The problem – a solution



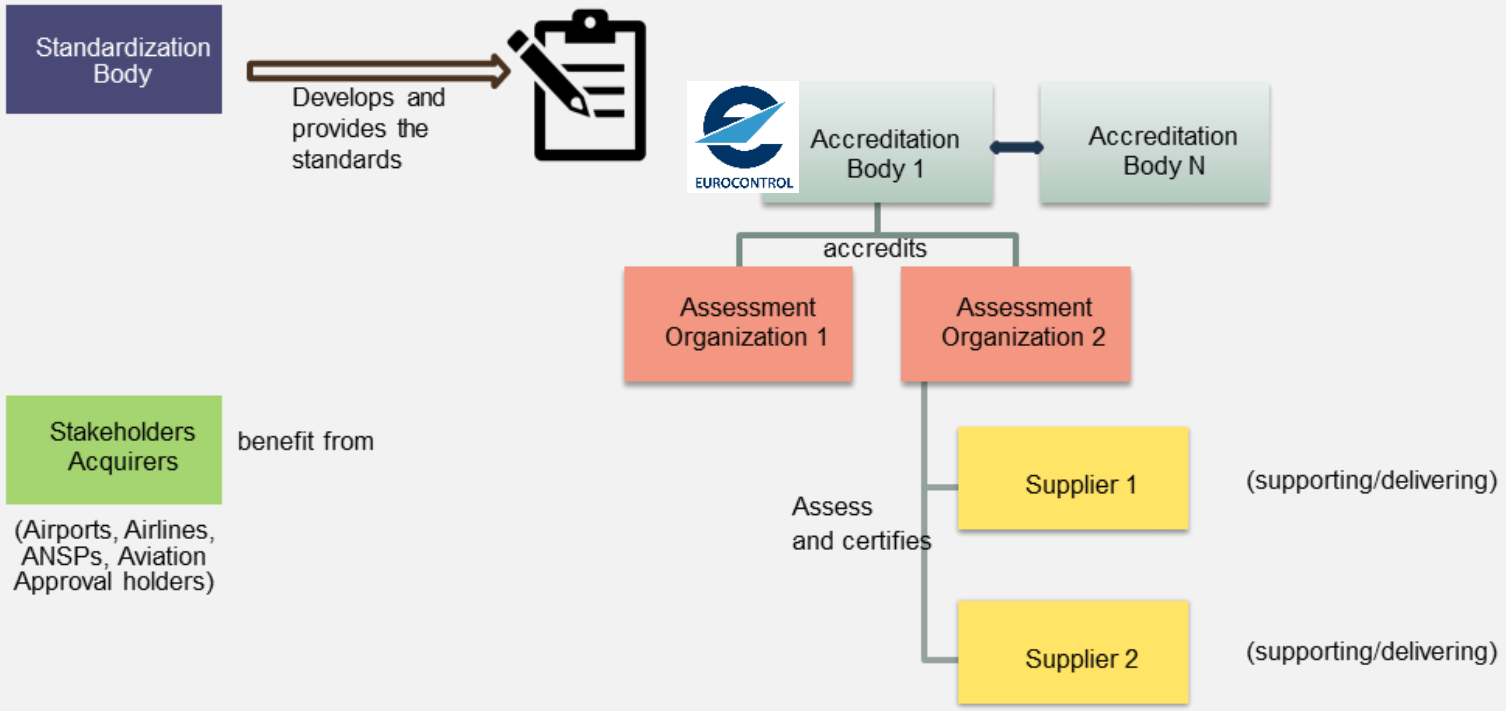
Cybersecurity supply chain assessment framework

- A group has been working in how to implement the supply chain assessment framework based on this use case (based on AirCyber as a standard):



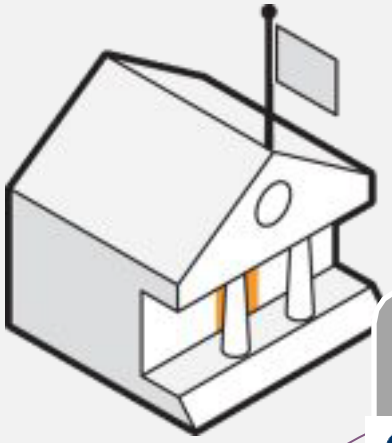
Cybersecurity supply chain assessment framework - EUROCONTROL Role

- **The idea is EUROCONTROL would act as the European/Regional (or more) accreditation body which:**
  - Select/validate the standards that assessment organizations will use to evaluate the cybersecurity maturity level of suppliers.
  - Defines the procedures, methodologies, qualifications for conducting cybersecurity assessments and issuing assessments results
  - Accredits and oversees assessment organizations
  - Issue certifications based on the compliance and maturity level of the suppliers.
  - Maintain the repository with the list of accredited assessment organisations and the results of the assessments.



Roles

Standardization body



Accredit assessors

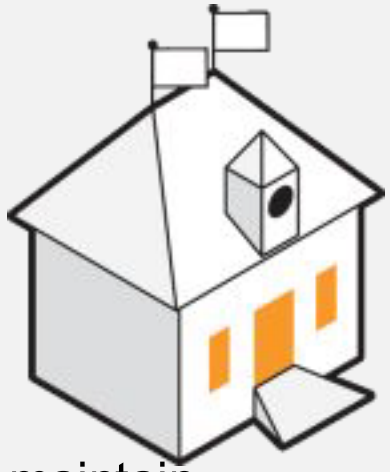
Regional Accreditation Body

EUROCONTROL

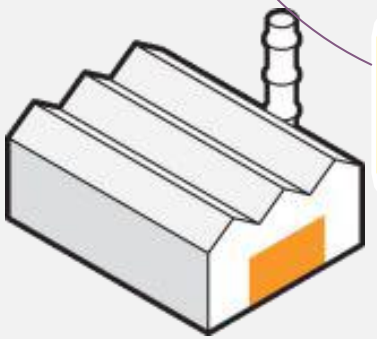
Acquirers/ Stakeholders
(Airports, Airlines, ANSPs, Aviation Approval holders)

Accredited assessment organization

Assess Supplier Maturity



Develop and maintain the framework



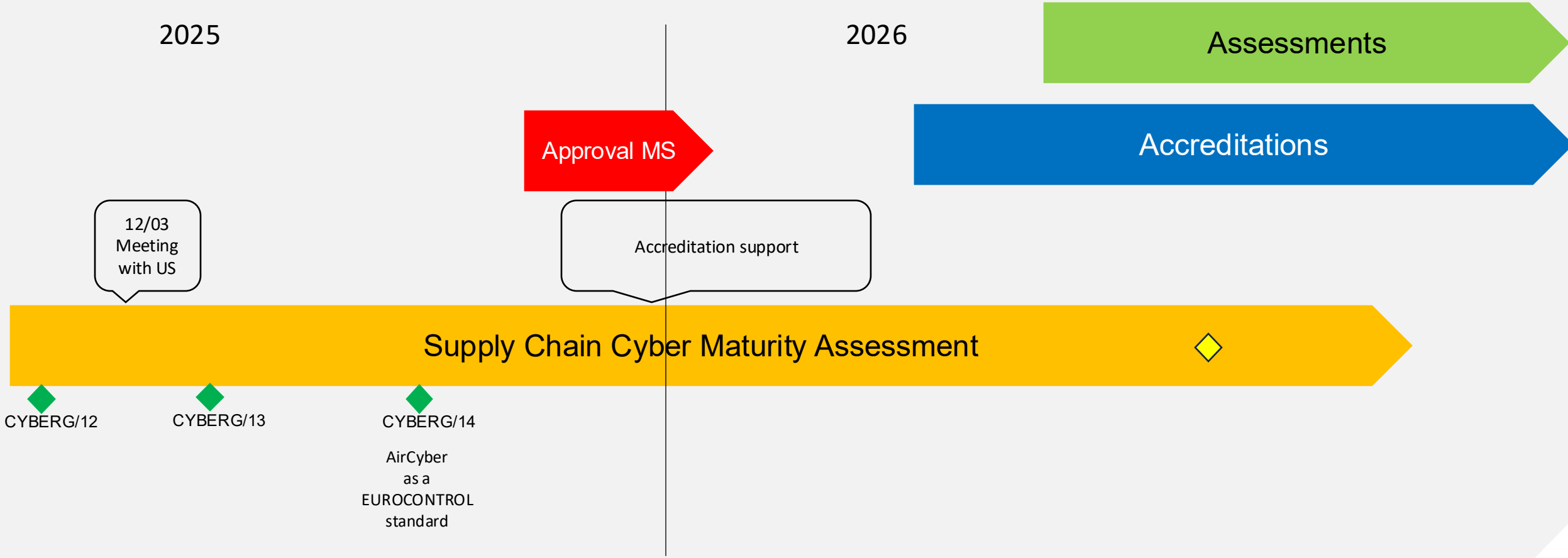
Suppliers
(supporting/delivering the Stakeholders)

Choose its Assessment Organisation

Benefits from the certificates

EUROCONTROL

Roadmap


2025
2026
Assessments
Approval MS
Accreditations
12/03
Meeting
with US
Accreditation support
Supply Chain Cyber Maturity Assessment
CYBERG/12
CYBERG/13
CYBERG/14
AirCyber
as a
EUROCONTROL
standard