



SUPPORTING
EUROPEAN
AVIATION

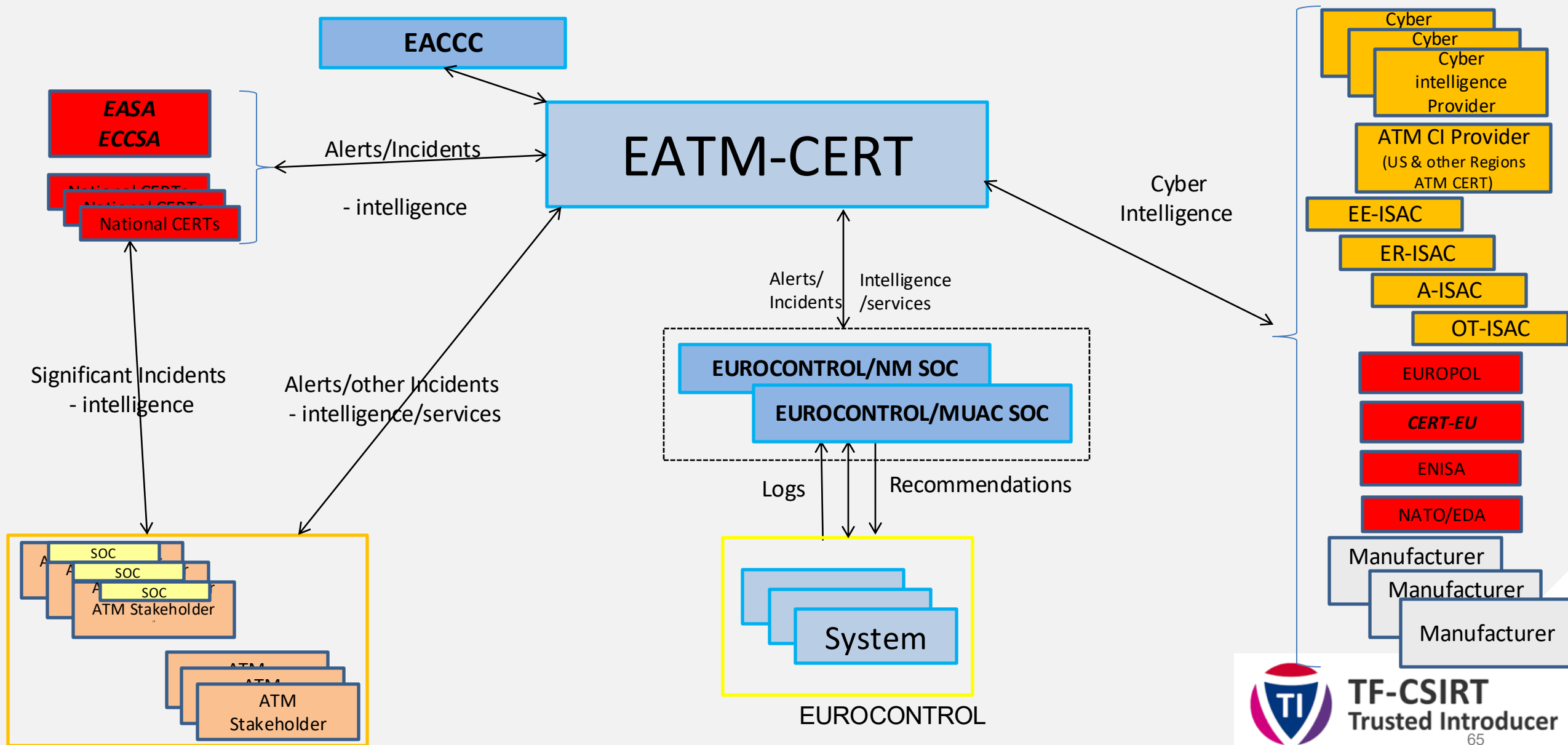
Aviation Cyber Threat Landscape

ICAO NACC/SAM Seminar

Patrick MANA

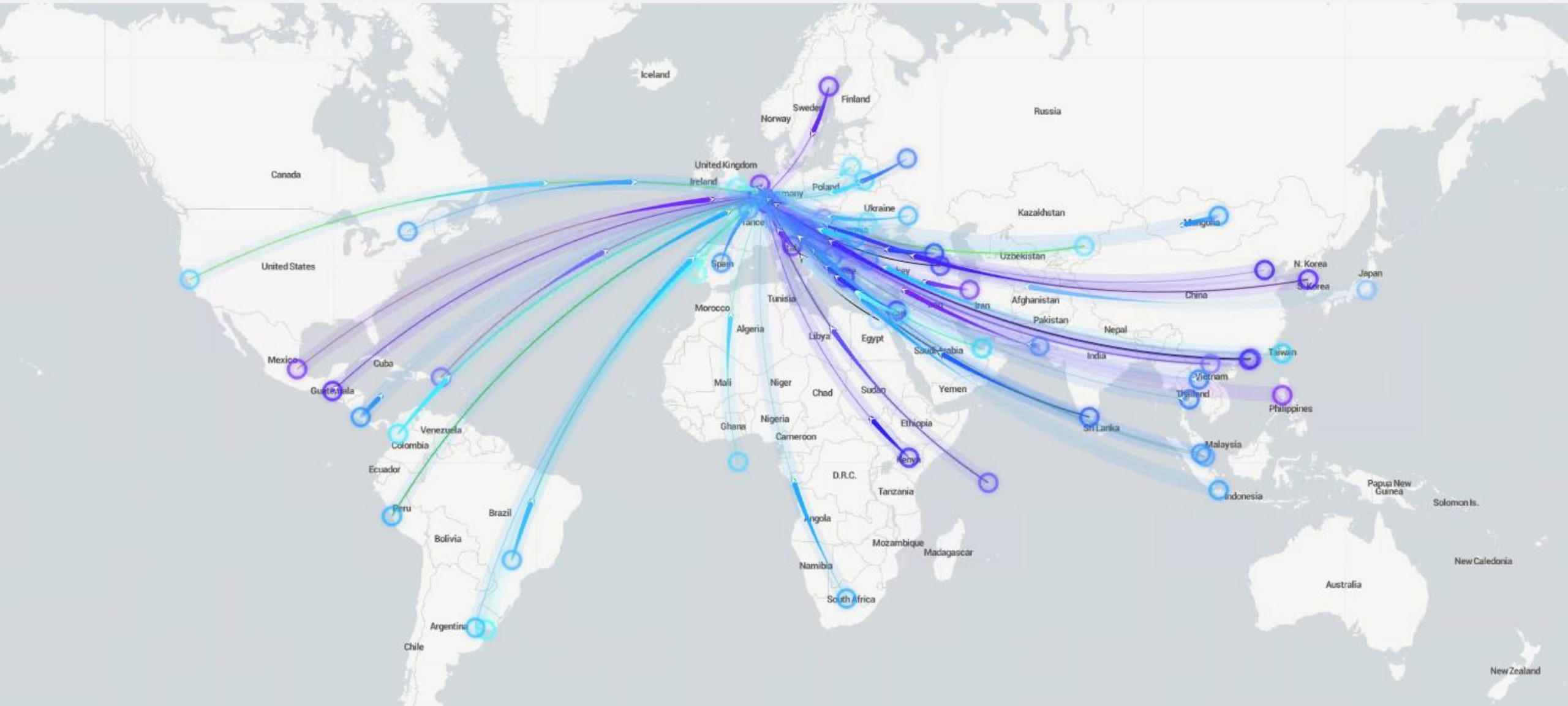


Regional sectorial CERT: combine cyber and domain expertise



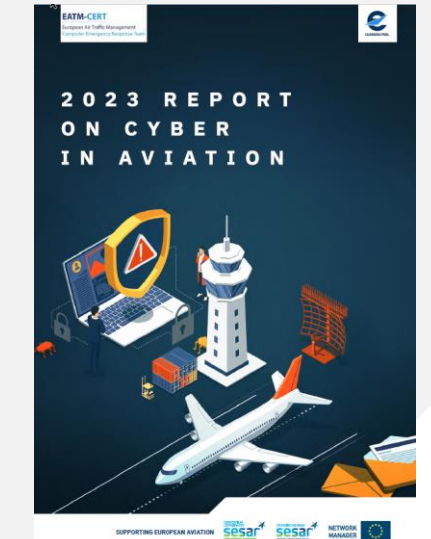
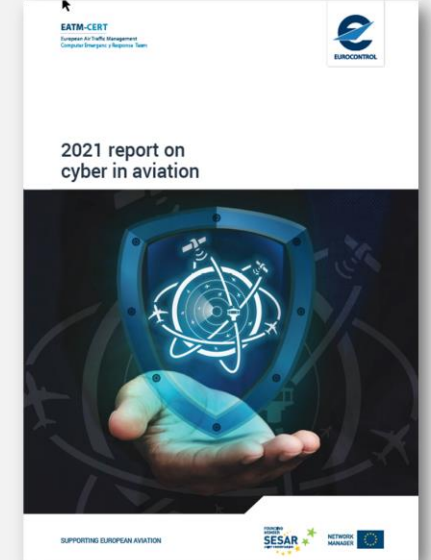
EATM-CERT services

1. Penetration test (EUROCONTROL services & products + Aviation stakeholders)
2. Bank transfer scams via email
3. Credentials leaks detection
4. Sensitive info leaks detection
5. 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
6. Support to incident response / Artefacts analysis
7. Vulnerability scanning of Aviation Stakeholders
8. Training exercises (table-top & technical) - EATM-CERT CTF, Room42
9. Phishing awareness campaigns
10. Test of Anti-DDOS solutions





The report is
TLP:GREEN



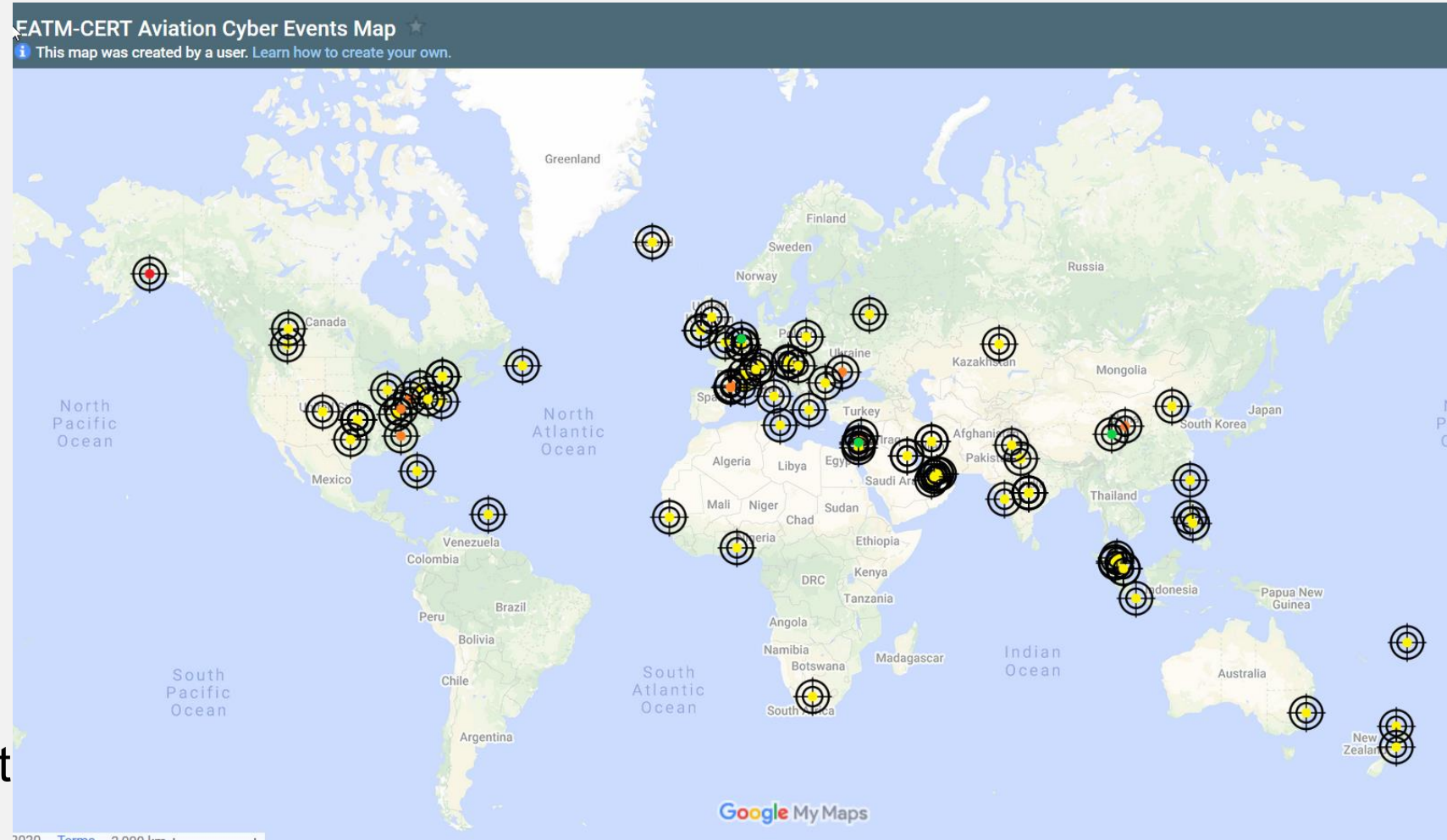
Dataset - Year 2023

6.320 incidents/events

- EUROCONTROL/EATM-CERT services
- Aviation stakeholders
- Publicly reported events (90)

2024: collection phase completed by end of March

- Equivalent number of input
- Analysis on-going



6.320 events – worldwide aviation

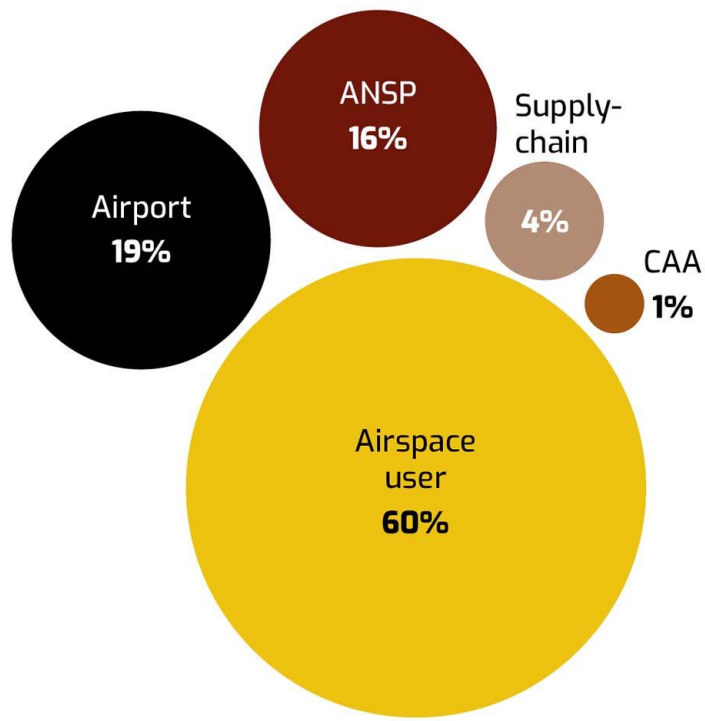


Figure 1: 2023 Attack surface

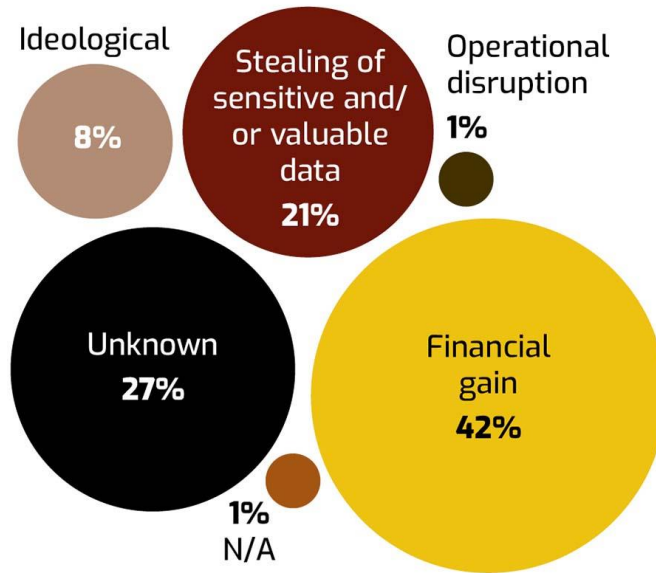


Figure 2: Threat actor motivation

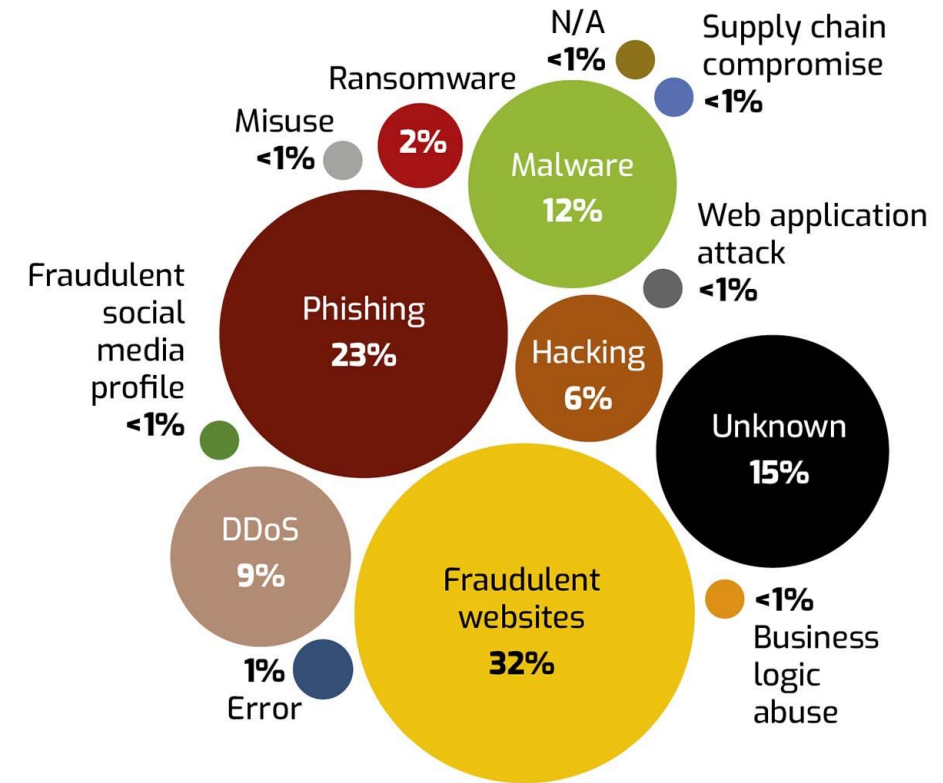


Figure 3: 2023 Adversaries Threat Vector

Figure 4: Threat Actors categories observed in 2023.

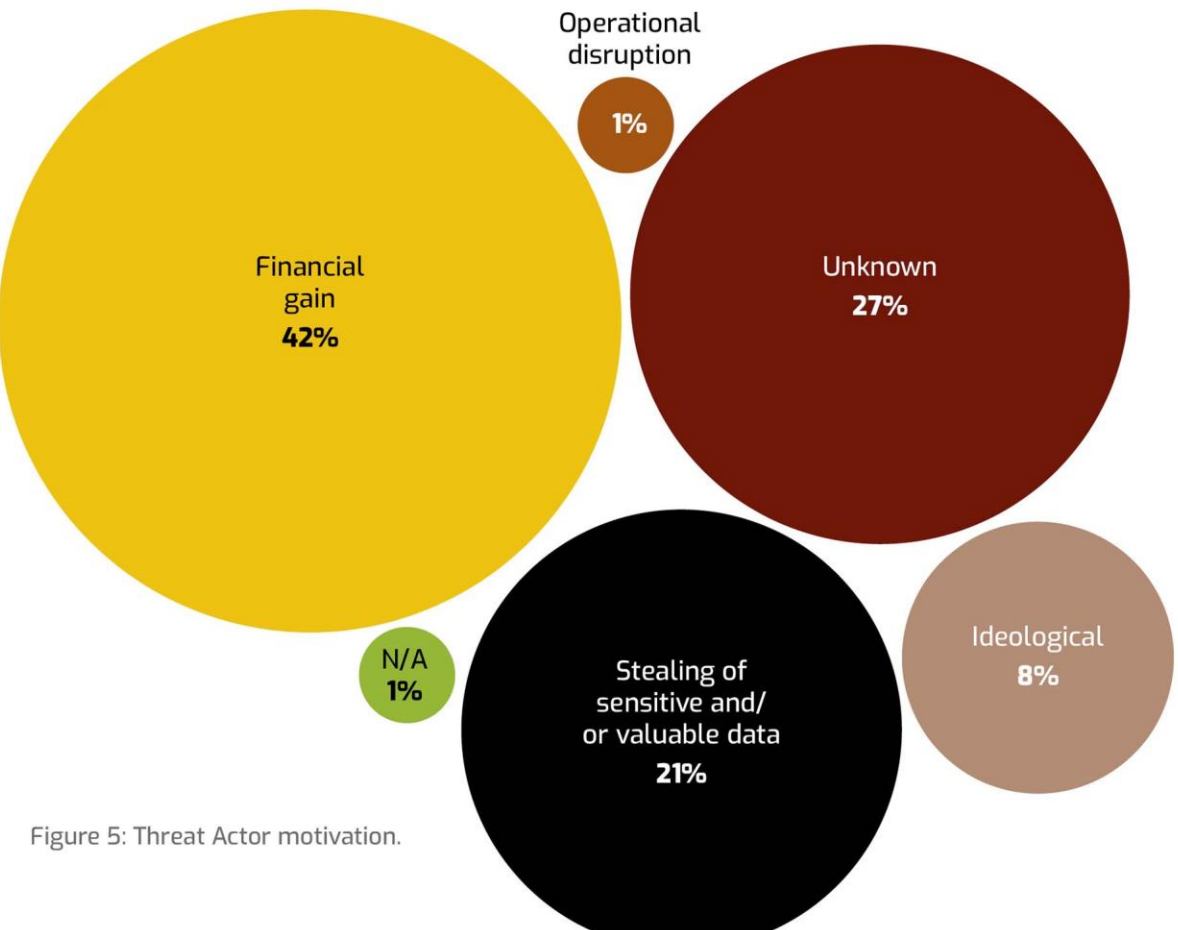
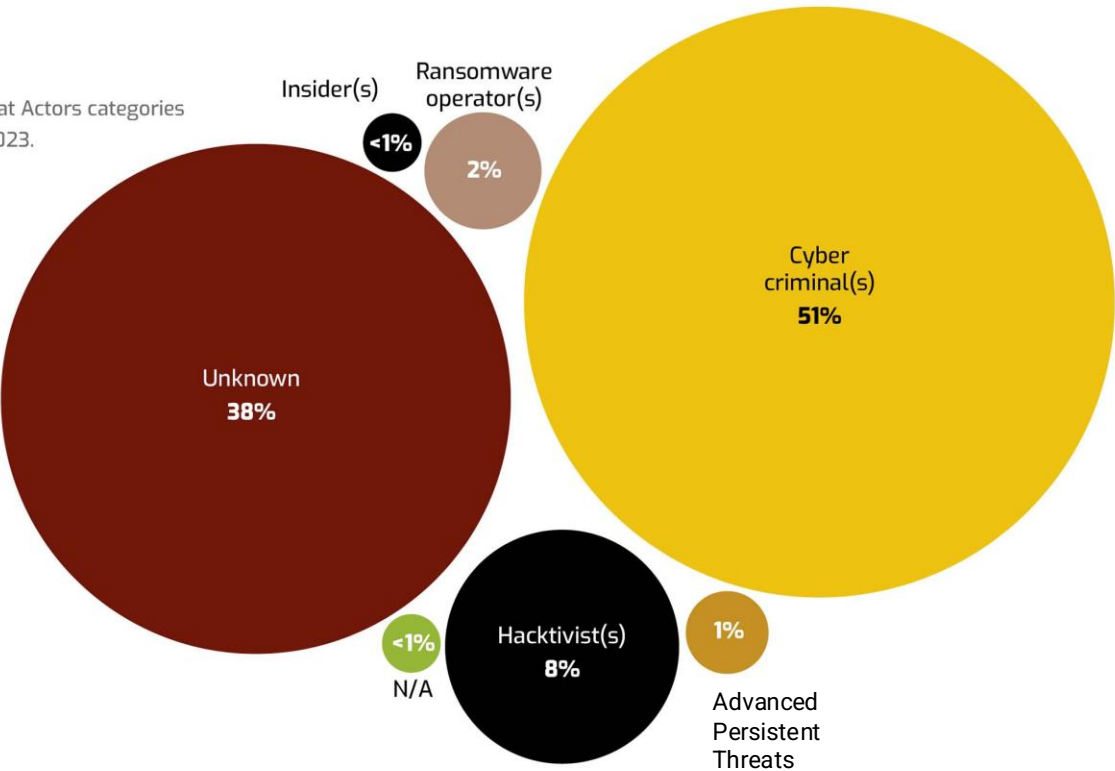


Figure 5: Threat Actor motivation.

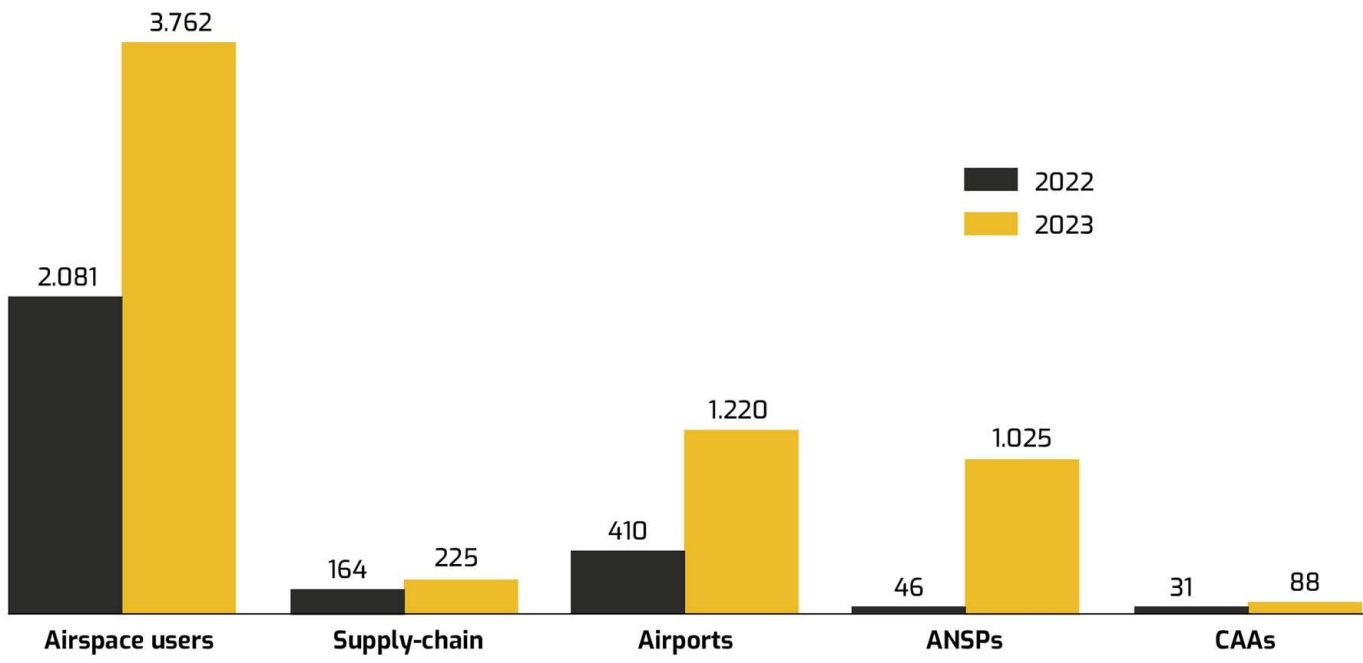


Figure 7: 2022 and 2023 threat attack surface comparison

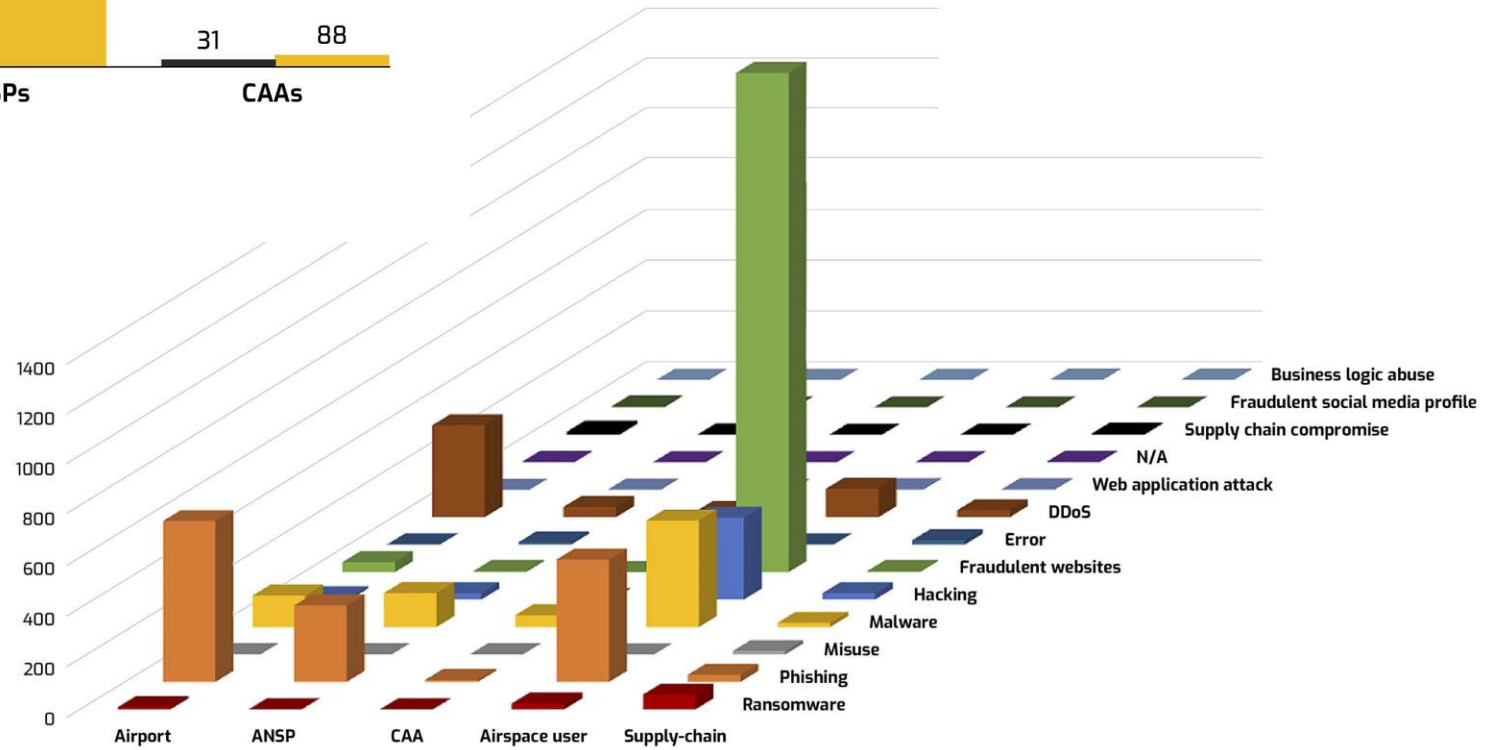


Figure 8: 2023 Attack type distribution

Motivation and Cost to Compromise Cybercrime

Malware Products

Account Stealer	\$ 32 - \$ 324
Bank Trojan	\$ 1,273 - \$ 3,956
Basic Malware Kit	\$ 323 \$ 97 /month \$ 258 /year
Advanced Malware Kit	\$ 450 /week \$ 1,800 /month
Custom Kit	\$ 323 - \$ 8,075
Malware vs AV checks	\$ 20
Zero-day money back guarantee	+10%

Command & Control Rental

Bulletproof VPN	\$ 25 /month
Bulletproof hosting	\$ 50 /month
Bulletproof domains/fast flux	\$ 50 /month
Custom C&C	\$ 1000 -

DDOS Services

DDOS kit rental	1 month	\$ 81
	6 months	\$ 161
	1 year	\$ 258
DDOS service / day	1 GB	\$ 16
	10 GB	\$ 161
	DNS server	\$ 323

Compromised Hosts

Asia	1000	\$ 20
NA/EU	1000	\$ 200 - \$ 270
Mix	1000	\$ 35
Handpicked		\$...

Stolen Data Products

Credit Card US	\$ 4 - 8
Credit Card EU / Asia	\$ 12 - 18
Credit Card + stripe data	\$ 19- 28
US Fullz (ID, SSN, address, ...)	\$ 25
EU Fullz (ID, SSN, address, ...)	\$ 30 - 40
Bank Account + credentials (\$70k+)	\$ 20 - 300

Professional Services

Doxing / Targeting	1 person	\$ 25 - 1000
Fake bank site		\$ 81 - 1000
File Cracking	zip, xls, ..	\$ 45
Hacking	Personal email	\$ 47
	Corporate email	\$ 81 - ...
	Website	\$ 100 - \$ 300
Coordinator / remote support		\$ 50 / hour
Zero Day exploit		\$ 500 - 250,000

Ransomware on aviation

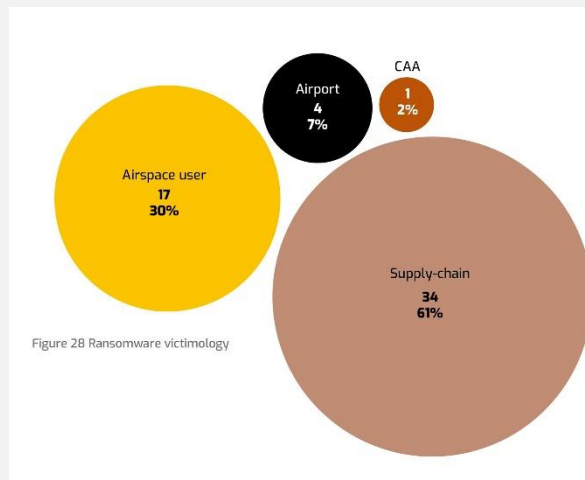
2024: ~42

2023: 108

2022: 97

2021: 119

Mostly Supply Chain



Main initial vectors:

- Spearphishing
- Stolen credentials

Double and even triple extortion

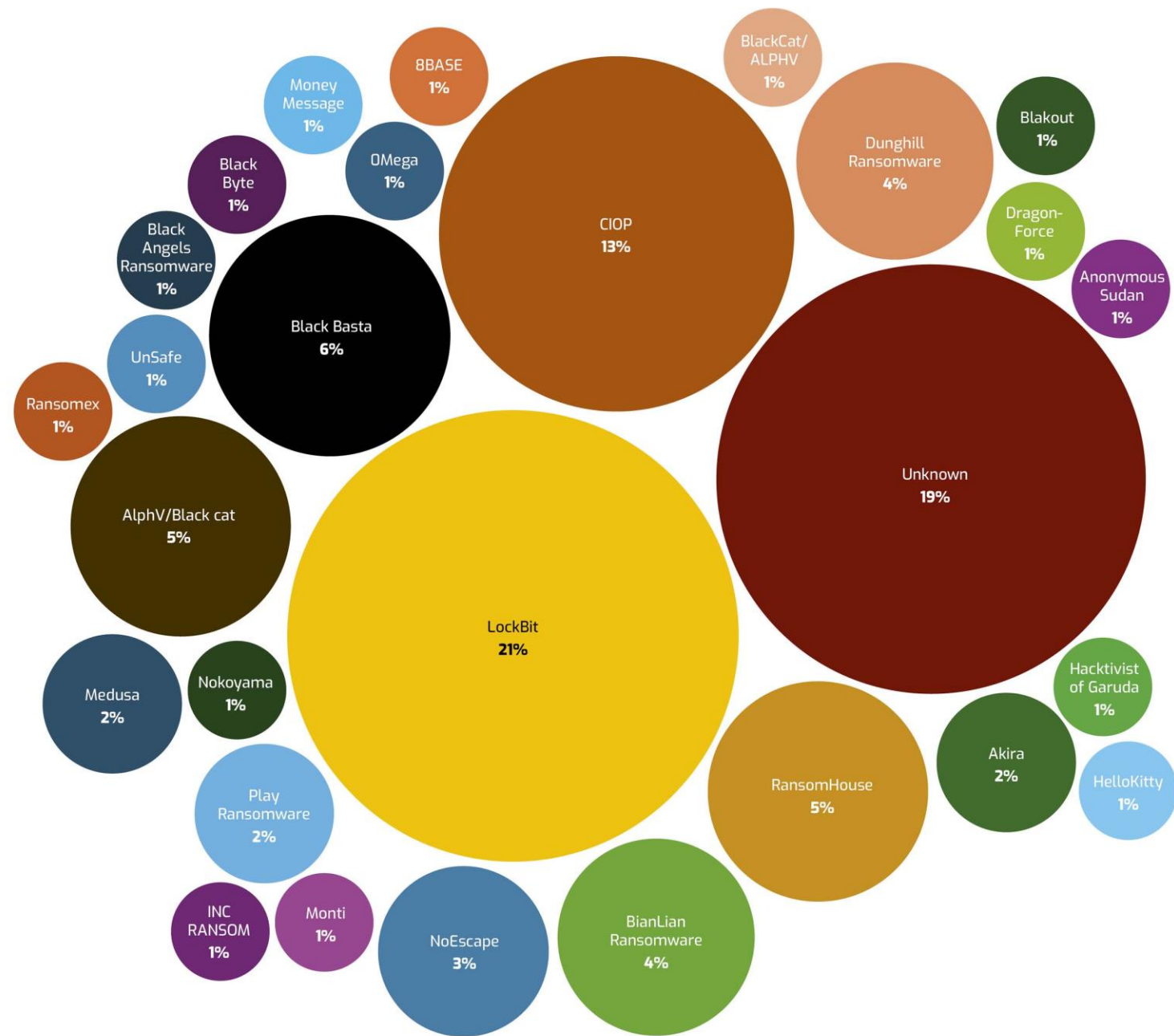


Figure 6: Ransomware groups in 2023

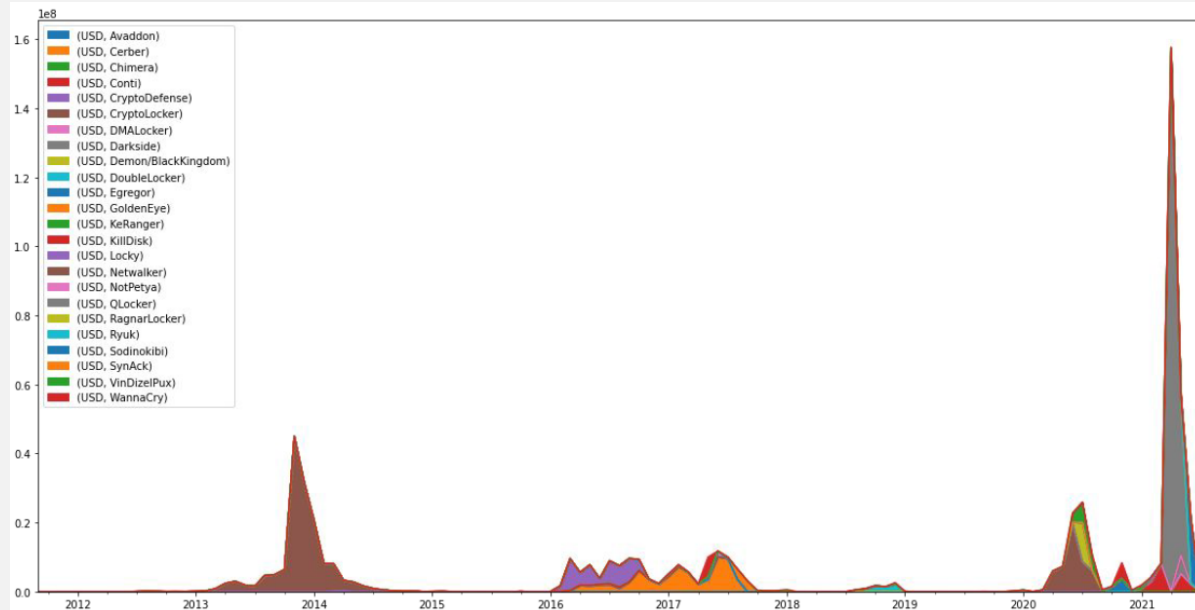
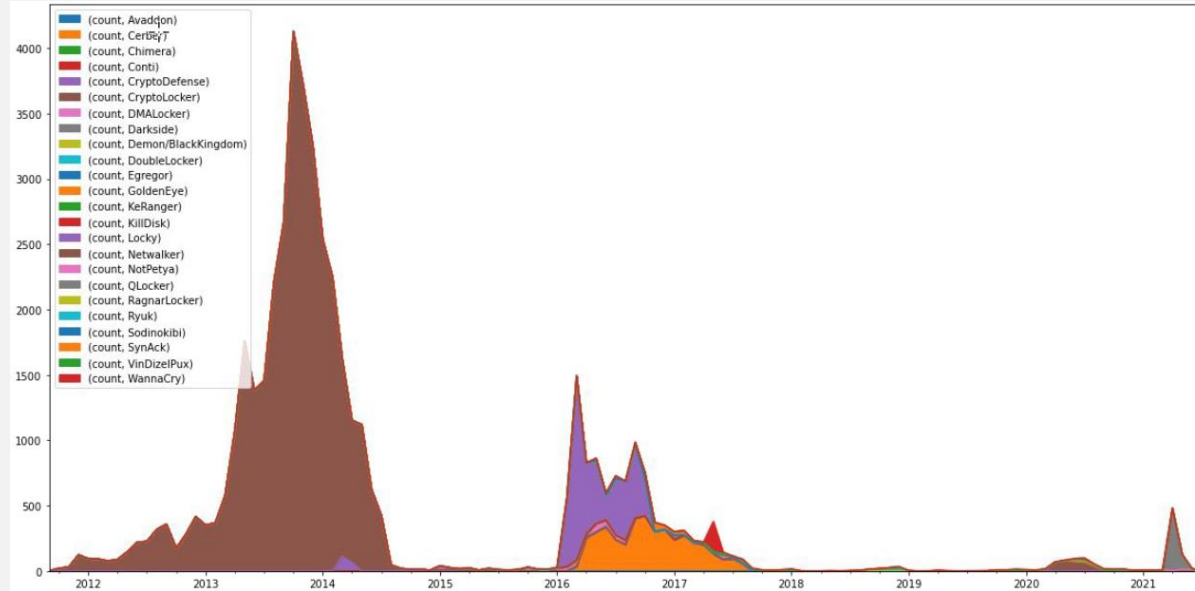
Ransomware affecting aviation

(worldwide - Source: EATM-CERT)



Ransomware (all sectors)

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



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



Number of DDoS attacks on aviation in:


- 2021: few (~10s)
- 2022: 318
- 2023: 528 (64% on airports)
- 2024: ~500

Surge of DDoS attacks associated to conflicts/wars.

Distribution of DDoS attacks against aviation in 2022/month

State of occurrence

DDoS as a Service



ПРАЙС

ГЛАВНАЯ / ПРАЙС

Синий
\$3/д
1 день
1 атака
120 секунд атаки
216Gbps TN
Layer 4: SSYN, OVX, DNS, NTP SSDP
Layer 7: GET, POST
Купить

Голубой
\$6/мес
1 месяц
1 атака
300 секунд атаки
216Gbps TN
Layer 4: SSYN, OVX, DNS, NTP SSDP
Layer 7: GET, POST
Купить

Зеленый
\$10/мес
1 месяц
1 атака
600 секунд атаки
216Gbps TN
Layer 4: SSYN, OVX, DNS, NTP SSDP
Layer 7: GET, POST
Купить

PLANS

Plan length and concurrents are fully customizable when purchasing.

<div>PLAN 1</div> <div>\$5/mo</div> <div>1 Concurrent Attack</div> <div>300 Second Attack Time</div> <div>PURCHASE</div>	<div>PLAN 2</div> <div>\$10/mo</div> <div>1 Concurrent Attack</div> <div>600 Second Attack Time</div> <div>PURCHASE</div>	<div>PLAN 3</div> <div>\$15/mo</div> <div>1 Concurrent Attack</div> <div>1200 Second Attack Time</div> <div>PURCHASE</div>
<div>PLAN 4</div> <div>\$25/mo</div> <div>1 Concurrent Attack</div> <div>3600 Second Attack Time</div> <div>PURCHASE</div>	<div>PLAN 5</div> <div>\$45/mo</div> <div>1 Concurrent Attack</div> <div>7200 Second Attack Time</div> <div>PURCHASE</div>	<div>PLAN 6</div> <div>\$60/mo</div> <div>1 Concurrent Attack</div> <div>10800 Second Attack Time</div> <div>PURCHASE</div>

Aviation MITRE ATT&CK Heatmap

6.320 events

+

APT10	APT39	HEXANE	UNC2420
APT15	APT41	Ke3chang	UNC2565
APT18	Axiom	LazyScripter	UNC2589
APT2	Chimera	Leafminer	UNC3318
APT27	Cleaver	Leviathan	UNC3810
APT28	Conference Crew	Molerats	UNC4214
APT29	Dragonfly	MuddyWater	UNC4697
APT3	Equation	Roaming Tiger	UNC4705
APT33	FIN6	TA2541	UNC4713
APT35	FIN7	Tropic Trooper	UNC4841
APT37	FIN11	UNC1543	UNC5111

Table 1: APT groups attacking aviation

Figure 44 Aviation Heatmap



Aviation MITRE ATT&CK Heatmap

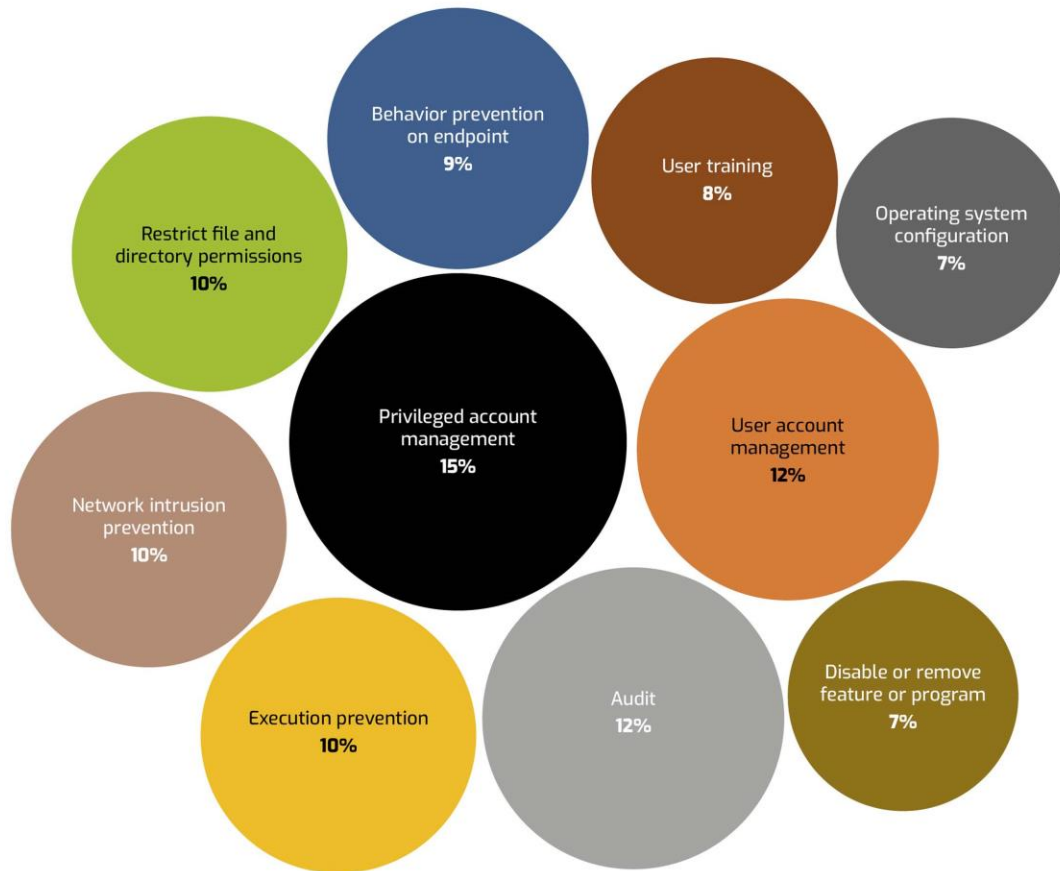


Figure 45: Identified mitigations

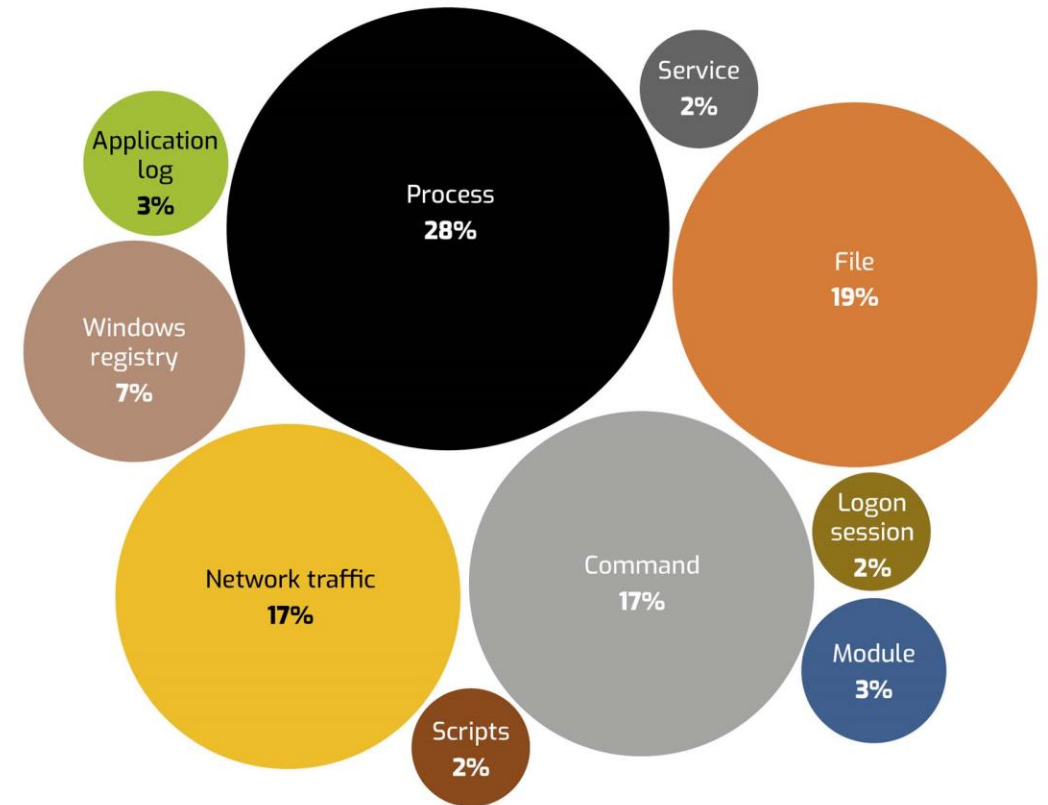


Figure 46: identified detections

Aviation MITRE ATT&CK Heatmap

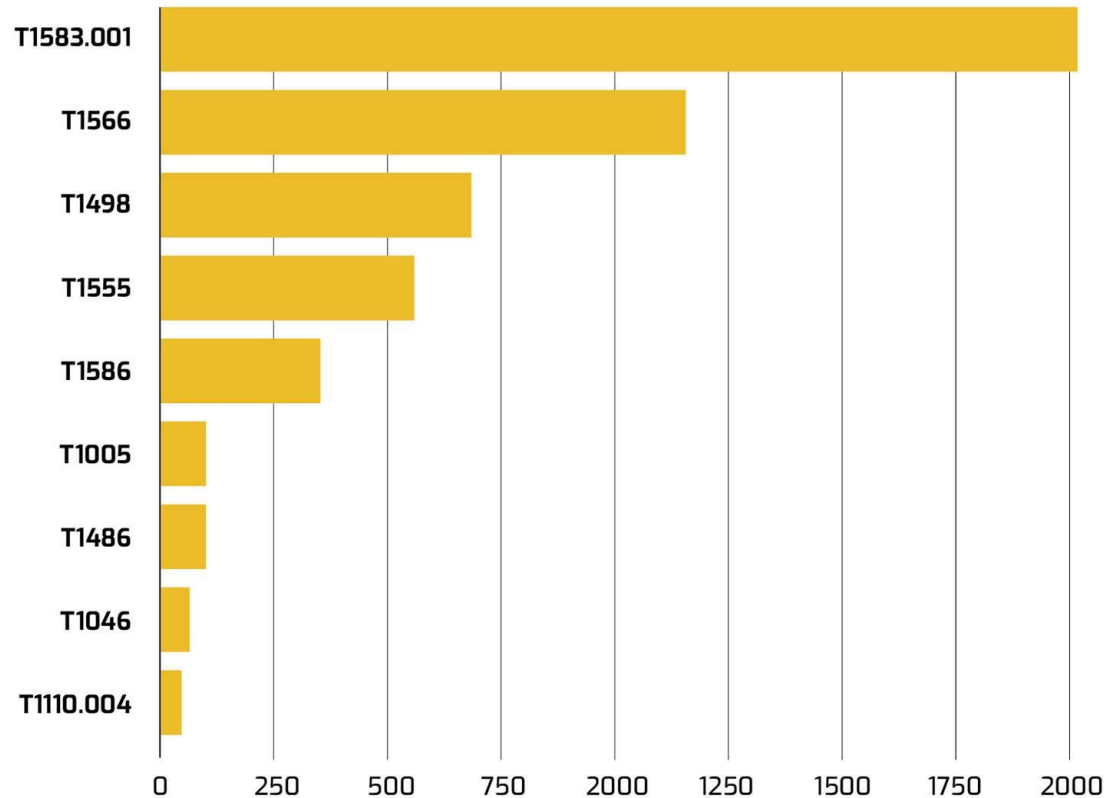


Figure 47: Top 10 techniques used by adversaries

Compromise Infrastructure: Domains (T1583.001)

Phishing (T1566)

Network Denial of Service (T1498)

Credentials from Password Stores (T1555)

Compromise Accounts (T1586)

Exploitation for Credential Access (T1212)

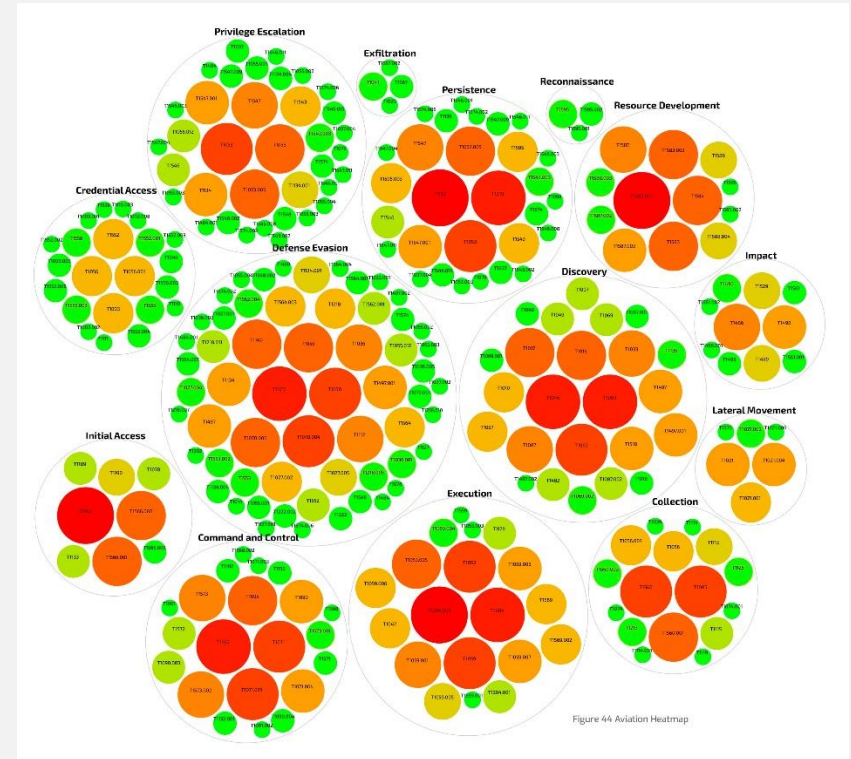
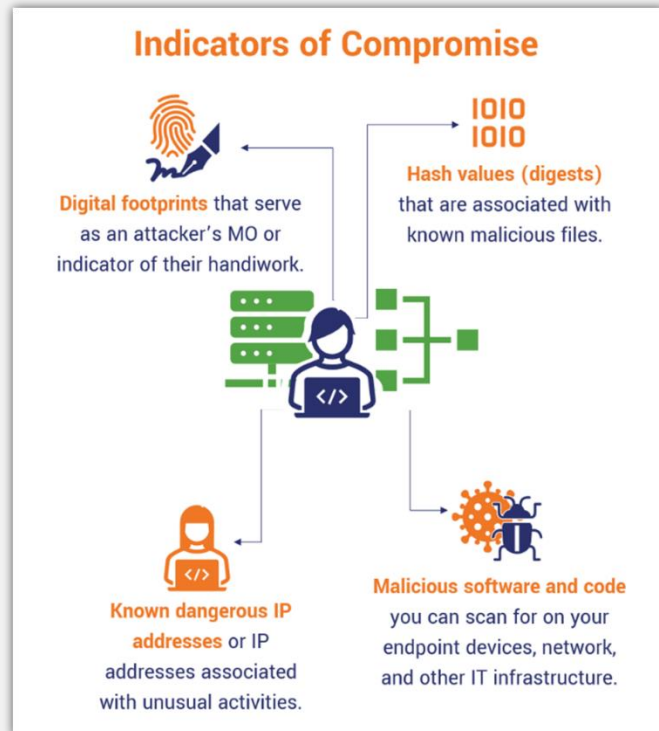
Valid Accounts (T1078)

Command and Scripting Interpreter: PowerShell (T1059.001)

Account Manipulation (T1098)

Windows Management Instrumentation (T1047)

From IOCs driven to TTPs driven SOC





SUPPORTING
EUROPEAN
AVIATION

Thank you!

patrick.mana@eurocontrol.int

eatm-cert@eurocontrol.int

eacp@eurocontrol.int

CONSORTIUM
COORDINATOR
sesar
DEPLOYMENT MANAGER

FOUNDING MEMBER
sesar
JOINT UNDERTAKING

NETWORK
MANAGER

