Supporting
European
Aviation

EUROCONTROL

EUROCONTROL/EATM-CERT views on cyber in aviation

Patrick MANA
EATM-CERT Manager

FOUNDING MEMBER SESAR JOINT UNDERTAKING

NETWORK MANAGER

EUROCONTROL

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

EUROCONTROL HISTORY

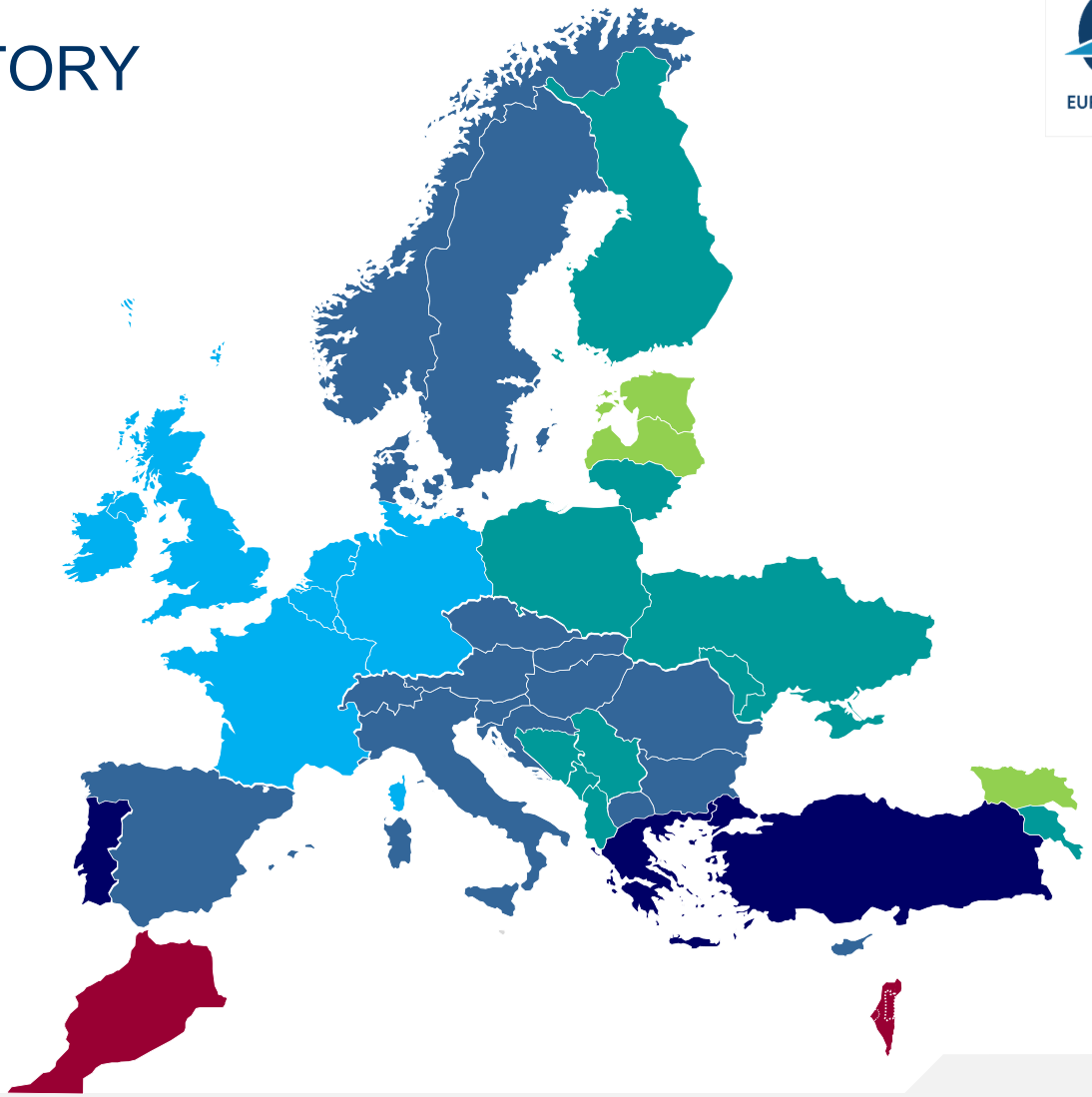
1960s

1980s

1990s

2000s

2010s



41 Member States &
the European Union

2 ‘Comprehensive Agreement’
States: Morocco & Israel

Building the Single European Sky !

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

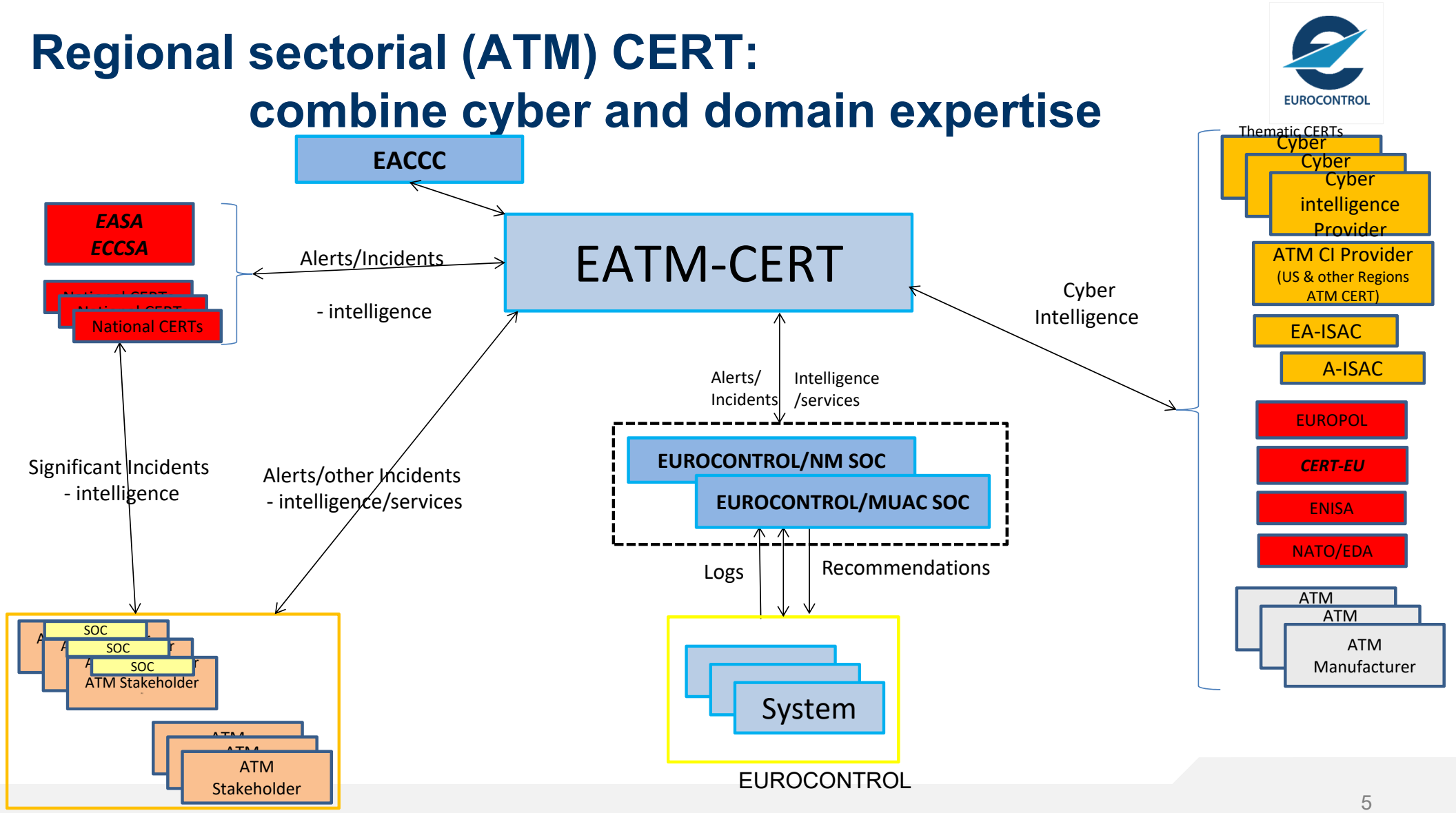
Manage the pan-European network

R&D => Deployment

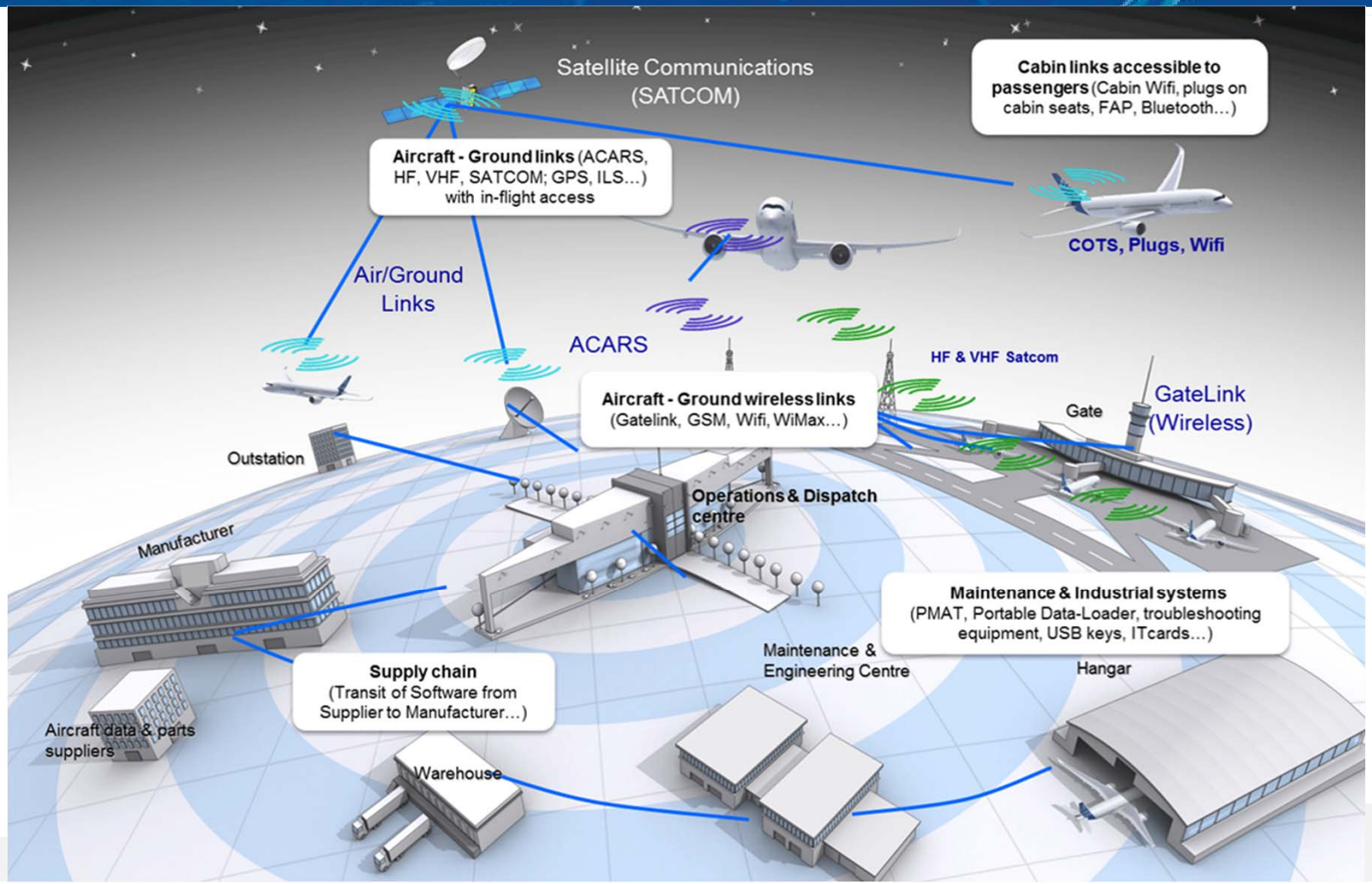
Products

Collect route and terminal charges

Regional sectorial (ATM) CERT: combine cyber and domain expertise

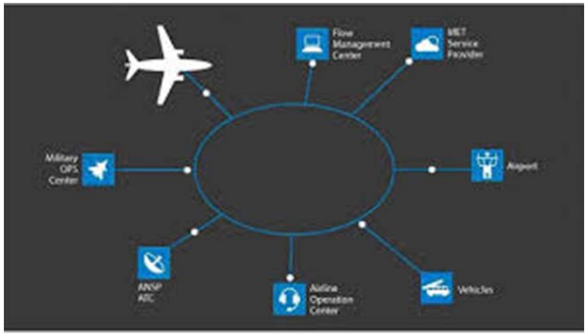


Complexity of Securing the Aviation Ecosystem



Evolution of ATM – towards digitalization

=>



Supporting
European
Aviation

EUROCONTROL

Threat actors

FOUNDING MEMBER SESAR JOINT UNDERTAKING

NETWORK MANAGER

Threat actors

- State-sponsored groups (23% - all sectors – DBIR Verizon)
- Cyber-crime organisations (39% - all sectors – DBIR Verizon)
- Hacktivists

- APTs (Advanced Persistent Threats) in 2019:
  - Main objective:
    - Cyber espionage
    - Service disruption
  - Groups:
    - **APT33** - a suspected Iranian threat group that has carried out operations since at least 2013. The group has targeted organisations in many industries in the United States, Saudi Arabia, and South Korea; they have a particular interest in the aviation and energy sectors.
    - **APT26** – a suspected Chinese threat group. The group has targeted defence, aerospace and manufacturing sectors since 2014.
    - **Fxmsp** - a suspected Russian hacking group. The group focuses mainly on gaining and selling access to different industries, including air transport.

State-sponsored / Geo-political

Cyber-crime …

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

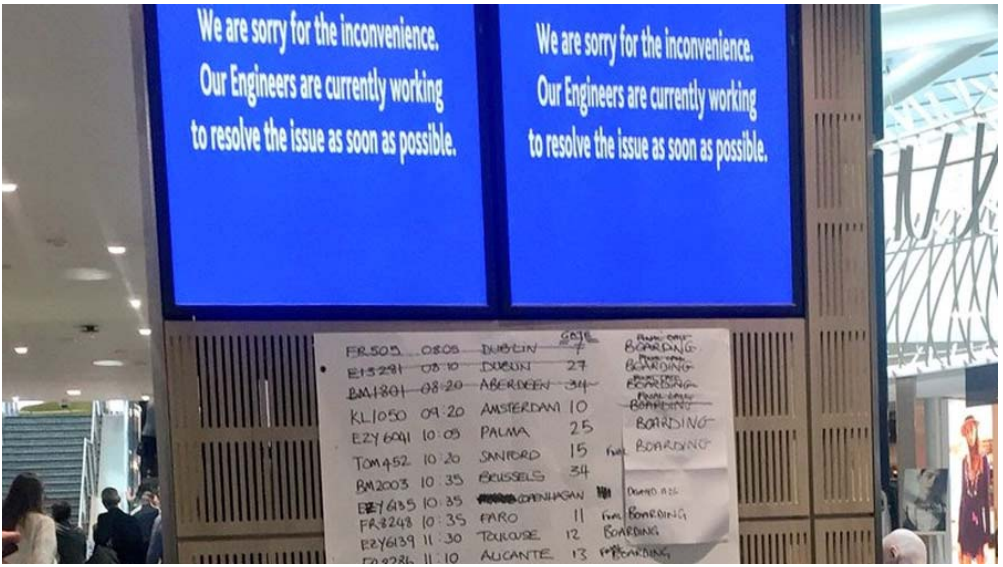
Doxing / Targeting	1 person	$ 25 - 1000
Fake bank site		$ 81 - 1000
File Cracking	zip, xls, ..	$ 45
Hacking	Personal email	$ 47
	Corporate email	$ 81 - ...
	Website	$ 100 - $ 300
Coordinator / remote support		$ 50 / hour
Zero Day exploit		$ 500 – 250,000

Source: RAND, Forbes, Verizon, TrendMicro

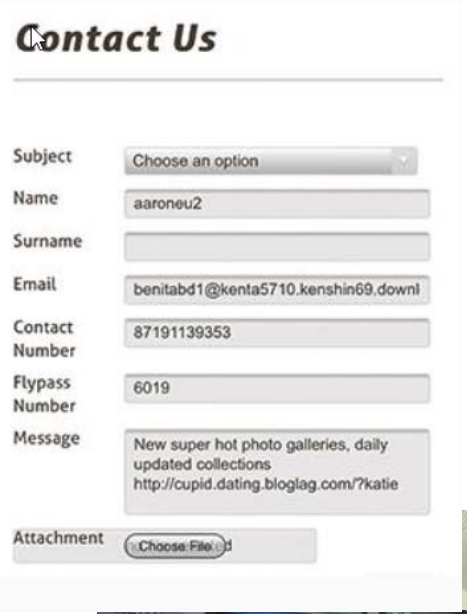
8

… it’s an industry

Cyber-crime e.g. ransomware



Bristol but also Atlanta, Cleveland, Albany, SFO, …



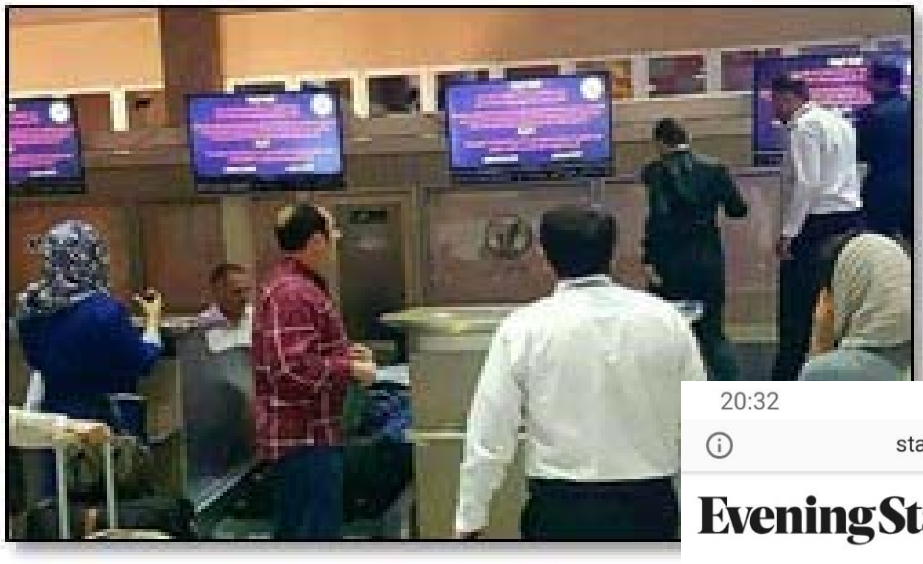
RavnAir ALASKA

???

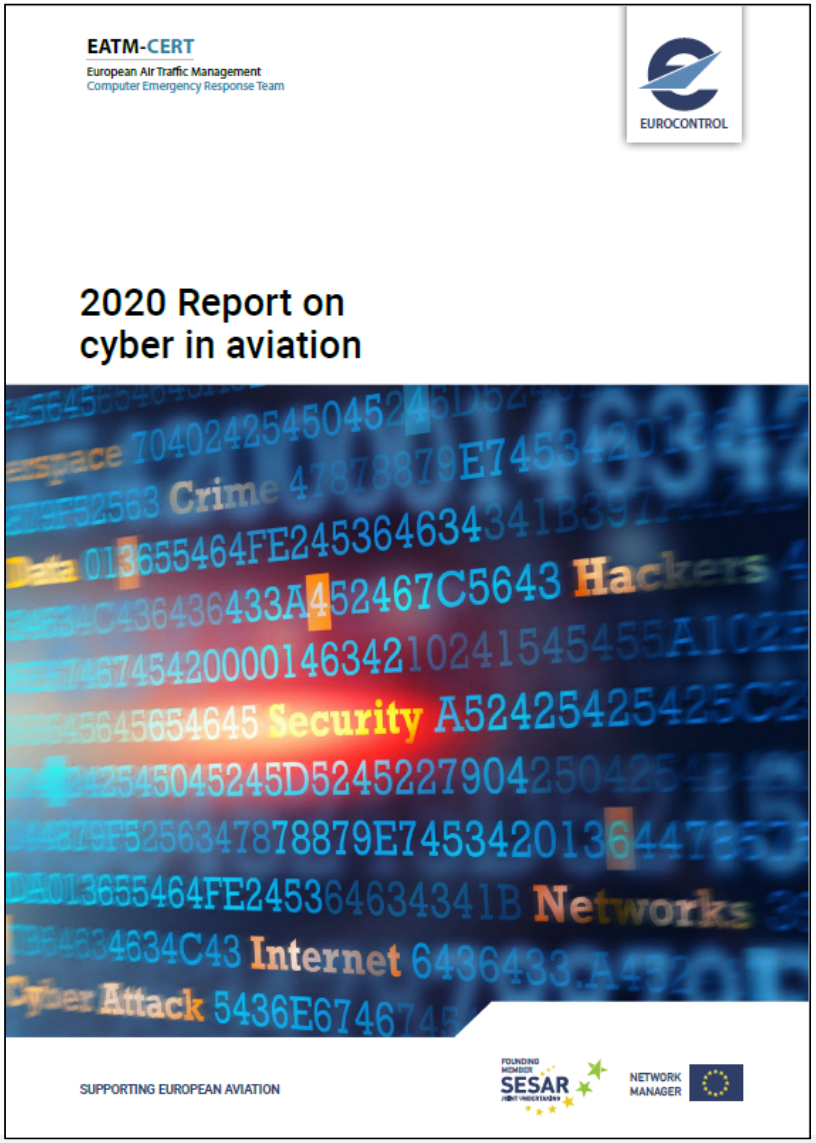
Hacktivists

- Eco-hacktivism
- Not only cyber (physical as well)
- COVID-19 impact on (eco) hacktivism ?

Hacktivism more and more e.g. environmentalists



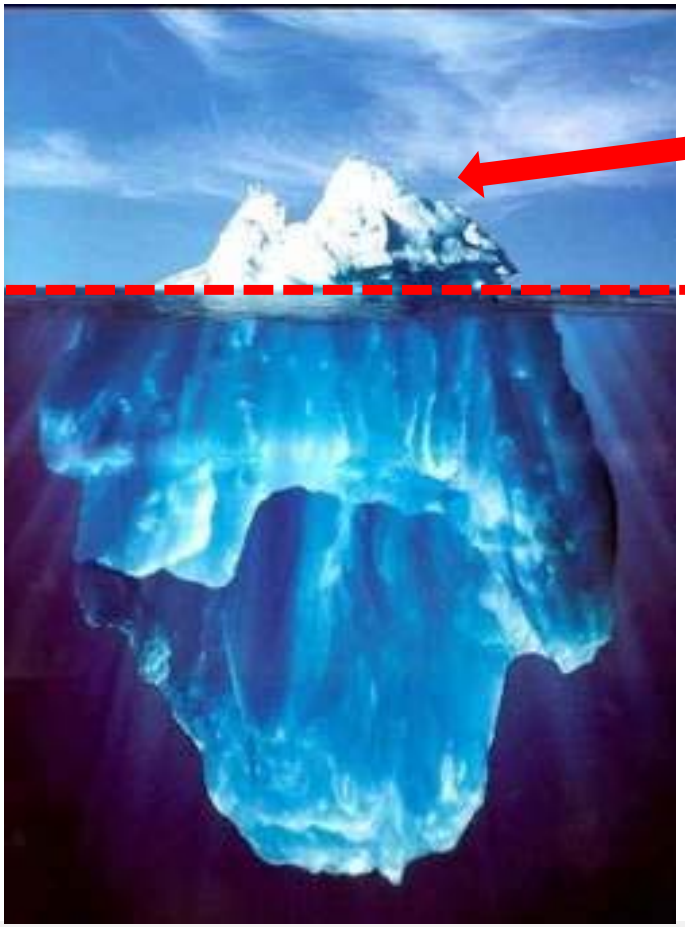
Report is TLP:GREEN



EUROCONTROL

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

Context and limitations



Our dataset

No detection means (e.g. SOC)

Misuse of TLP

Company sharing culture

De-identification

Legal framework to share

Lack of maturity

National regulation

Trust

Supporting
European
Aviation

EUROCONTROL

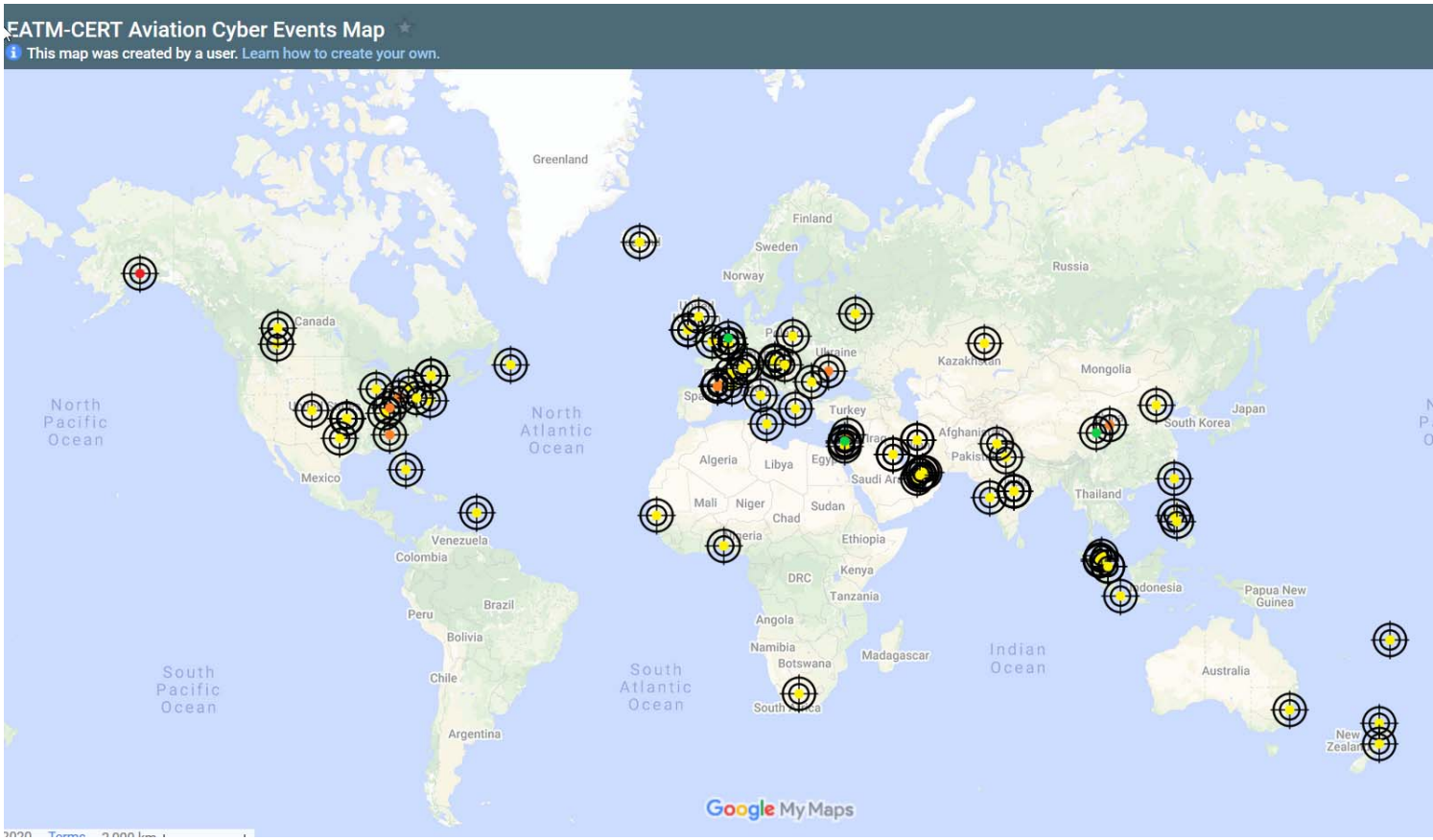
Data set

FOUNDING MEMBER SESAR JOINT UNDERTAKING

NETWORK MANAGER

Dataset

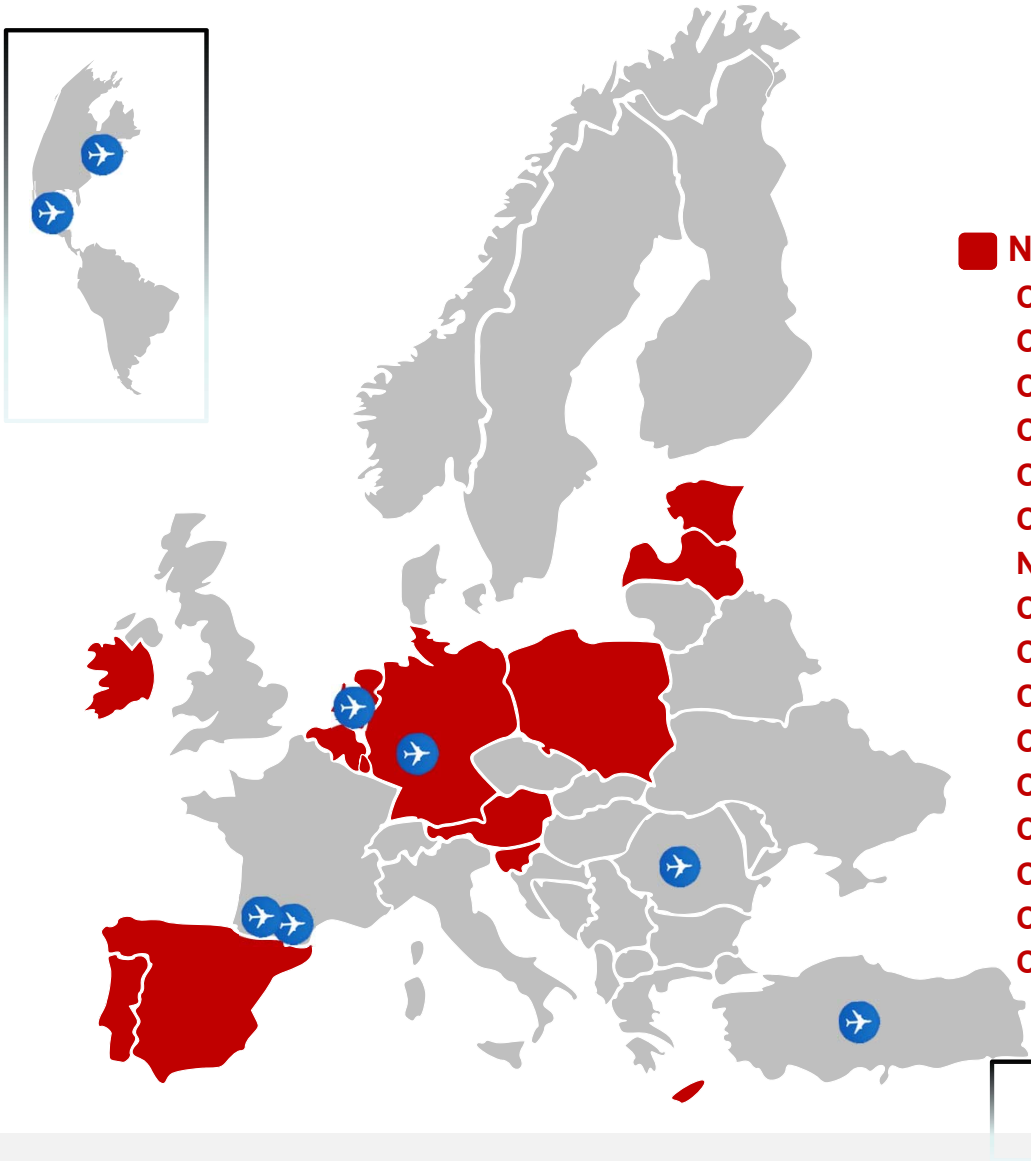
- ~200 incidents/events
- Publicly reported events
- EUROCONTROL/EATM -CERT services
- Aviation stakeholders
- Cyber “clubs”
- National CERTs
- CTI vendors



TLP marking

COLOUR	MEANING	EXAMPLE
RED	Not for disclosure, restricted to participants only. Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.	Information shared with people in a meeting; direct email.
AMBER	Limited disclosure, restricted to participants' organizations. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.	Sharing of Indicators of Compromise (IoCs) to an organisation's CSIRT. These could be forwarded to the SOC for further action.
GREEN	Limited disclosure, restricted to the community. Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.	Sharing of a malware analysis with a specific industry sector.
WHITE	Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.	Public security advisory.

MISP



Aviation PARTNERS

- CERT-AIRBUS A/C
- DLH-DE –Lufthansa Group
- ECCSA (test)
- IATA (by 3rd party CTI platform)
- Airport 1
- SOC of an airport
- Schiphol Airport – Netherlands
- CERT-IST – Thales
- CERT-THY – Turkish Airlines
- CAA-RO - Romanian CAA
- Aero Mexico

National CERT

- Cert-AT – Austria
- Cert-EE – Estonia
- Cert-EU – Europe *.eu
- Cert-Bund – Germany
- Cert-LV – Latvia
- CIRL.LU – Luxembourg
- NCSC-NL – Netherlands
- CERT-PL – Poland
- CERT-PT – Portugal
- CERT-SI – Slovenia
- CERT-IL – Israel
- CERT-BE – Belgium
- CSIRT-IE – Ireland
- CERT-CY-Cyprus
- CERT- INCIBE – Spain
- CERT-CCN – Spain

Israel

Supporting
European
Aviation

EUROCONTROL

Cyber at the time of the COVID-19 crisis

FOUNDING MEMBER SESAR JOINT UNDERTAKING

NETWORK MANAGER

Cyber during COVID-19

Attackers have no ethics!
Attackers never rest!

Issues:

- Budget cuts
- Resource availability
- Systems update
- New abnormal vs normal thresholds
- Videoconferencing
- Remote connections

Recommendations

Developing an approach and action plan to address the cyber challenges of recovering operations including the following areas:

- Security aspects of Returning to Operations, including:
  - Performing an assessment of Security updates and patches, across all systems;
  - Verification and validation of Interface status and reconnection requirements;
  - Verification and Validation of System access permissions, either thought local or remote, if applicable, access;
  - Performing Vulnerability scanning, Security risk assessment and implementing as required security patches and updates;
  - Verification and validation of Certificates in use and respective lifecycle as applicable;
  - Performing security assessment of systems and which are not in normal operation;
  - Perform security verification and validation prior to reconnect professional computers to corporate networks, specifically if they were used to perform remote work;

Recommendations

- Cyber Security Impact of the risk of budget reduction
- **Human resources Impact**
- Engaging and promote a dialog with their National Aviation Competent Authority as well as their National Cyber Security Authority to include a cyber approach in their recovery to normal operations.
- Considering to update the security controls especially for those IT systems which were not or poorly or differently used during this period
- Considering the use of tools and techniques that allow to detect infected and compromised files and systems
- Fine-tuning cyber detection means (e.g. SOC) in accordance with new information exchanges patterns and what is “abnormal vs normal”.
- Perform an information security risk impact analysis identifying the KPA´s impacted
- Consider the inclusion of information security requirements in the Project/Product/system lifecycle management and in new projects and in the process of modernization or upgrade of existing ones.

Supporting
European
Aviation

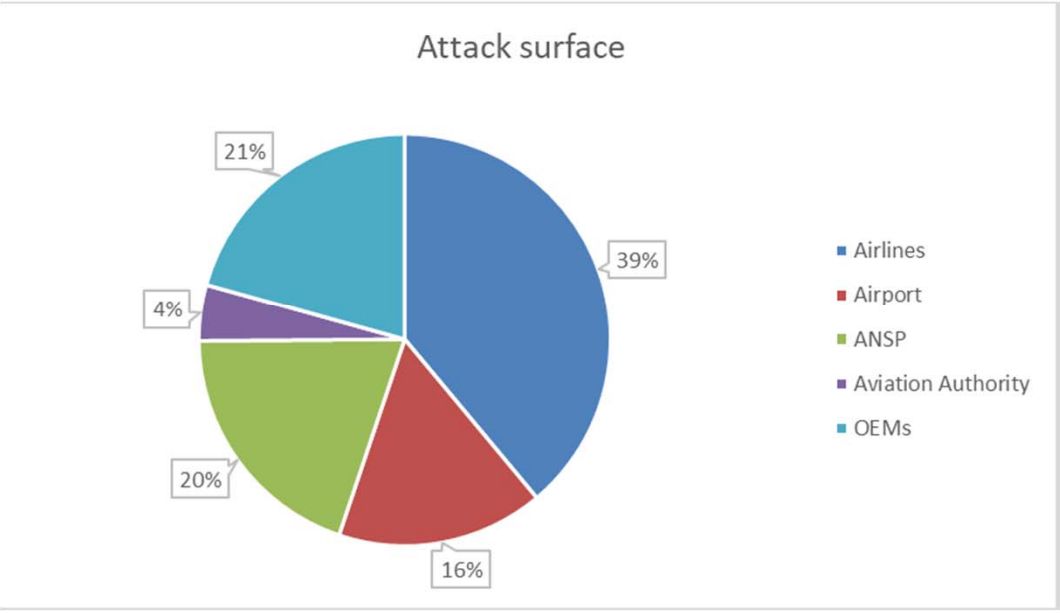
EUROCONTROL

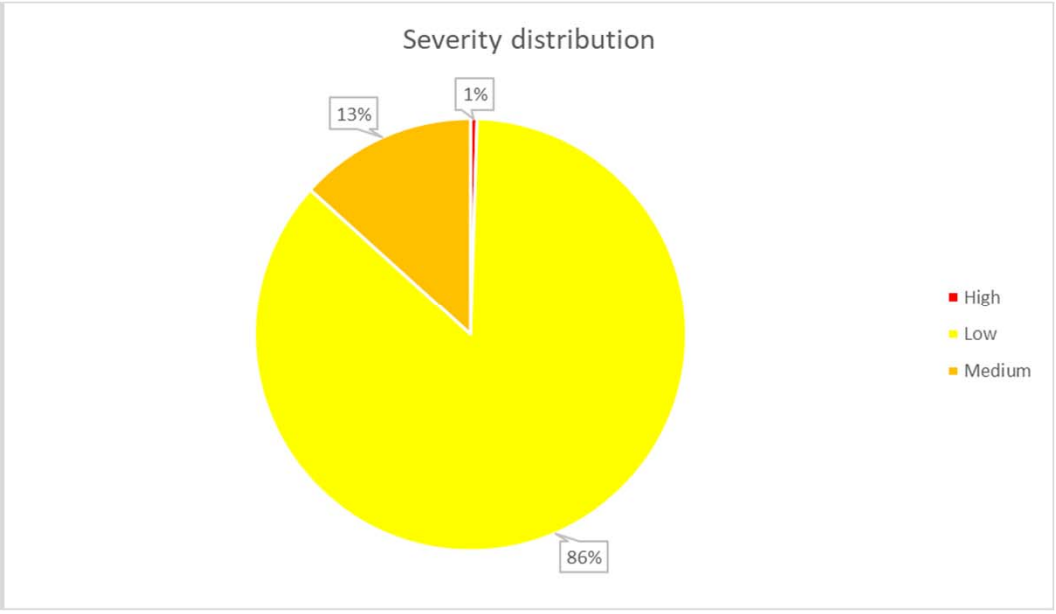
Threat landscape

FOUNDING MEMBER SESAR JOINT UNDERTAKING

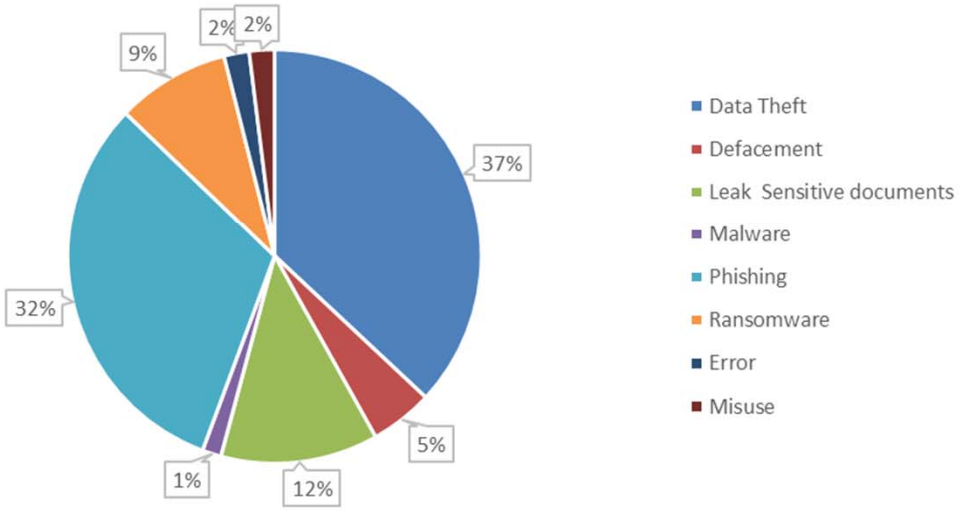
NETWORK MANAGER

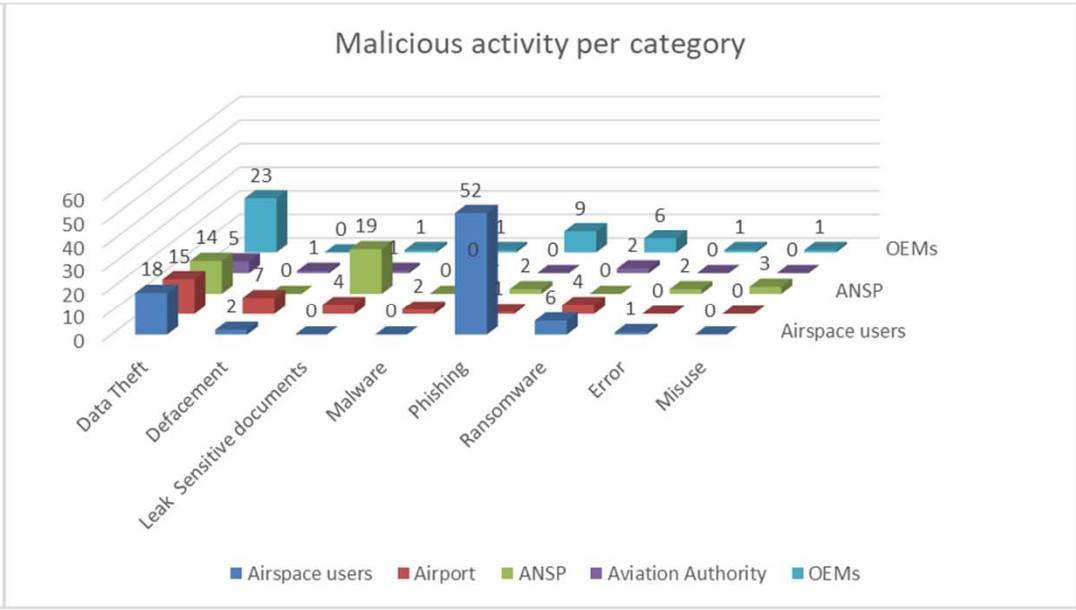
Aviation threat landscape





Aviation – attack types





Supporting
European
Aviation

EUROCONTROL

Threat characteristics

FOUNDING MEMBER SESAR JOINT UNDERTAKING

NETWORK MANAGER

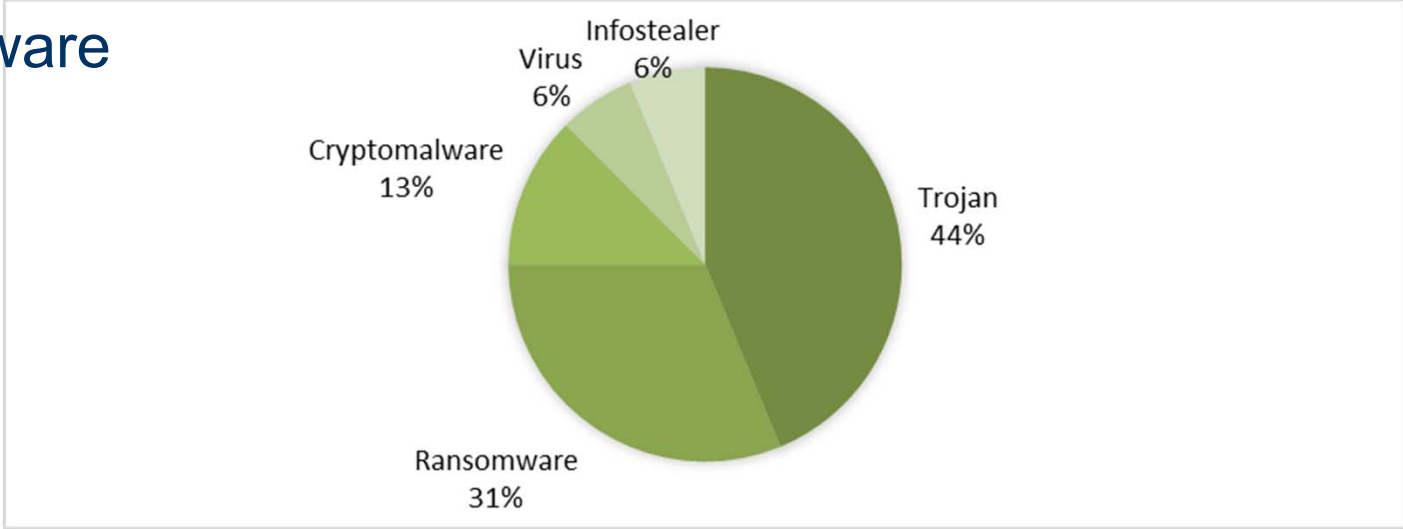
Threat characteristics

- Aviation is not so different from other sectors:
  - Some standard IT also ! (e.g. corporate/office/web)
  - Some ICS (e.g. power supply)

- No safety impact … reported (very sensitive information)

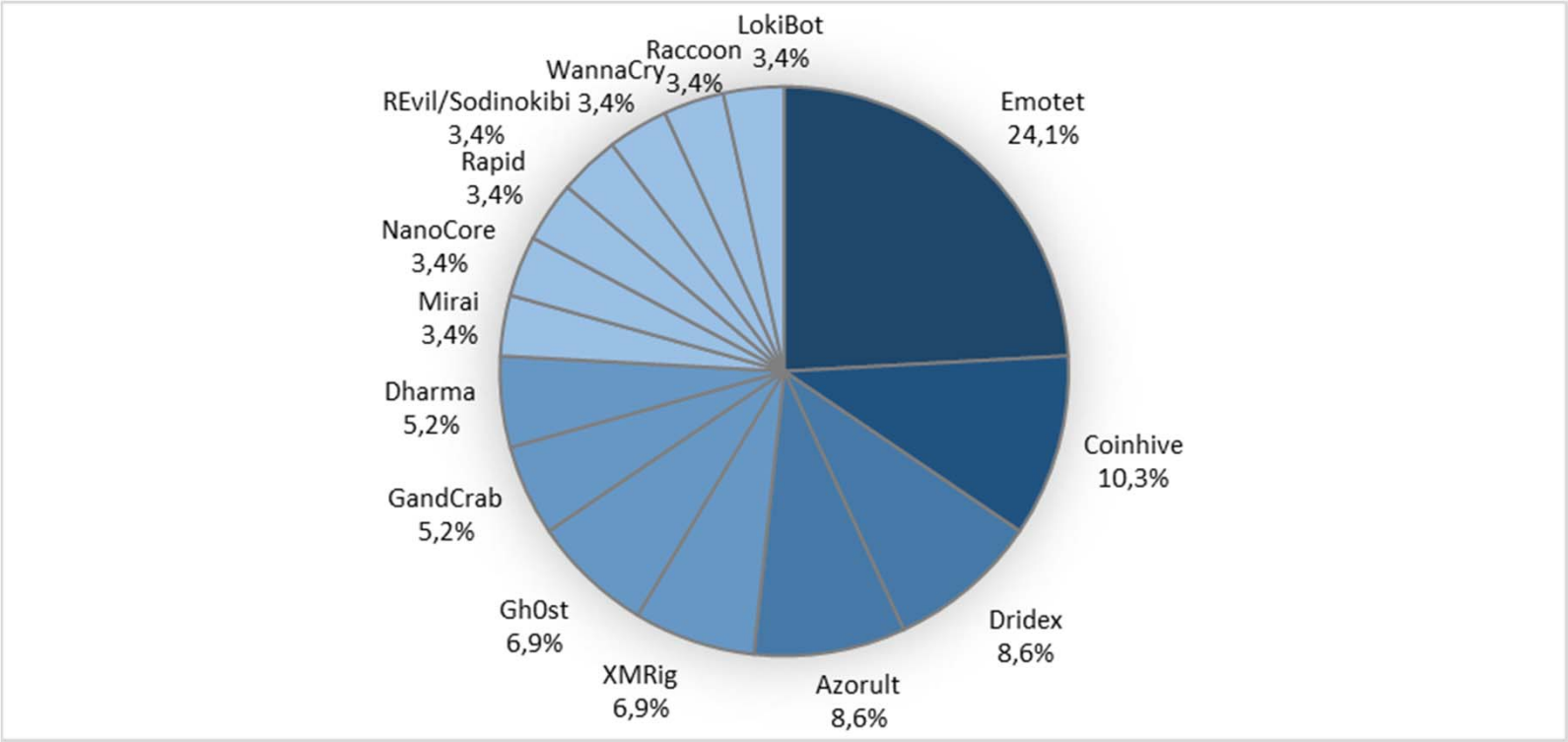
- Malware
- Credential leaks / Compromised accounts
- Scams impersonating EUROCONTROL staff
- Sensitive document leaks
- Fraudulent activities

Top malware

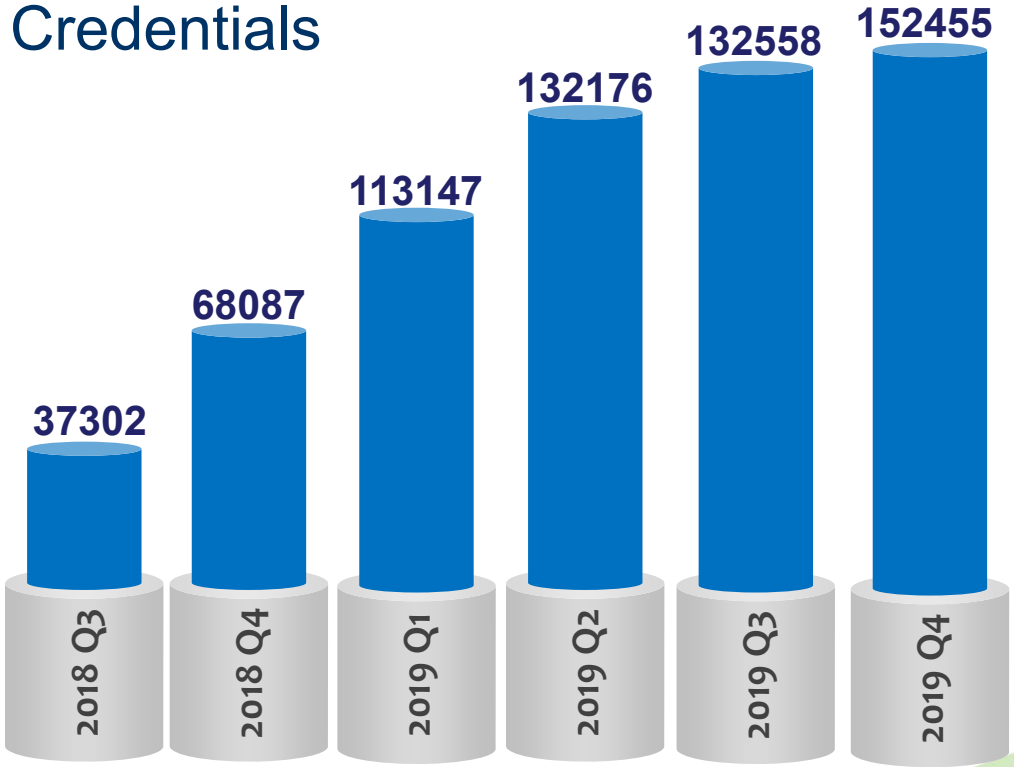


Trojan	Ransomware	crypto miners	Virus	Info stealer
Azorult	Dharma	Coinhive	Mirai	Racoon
Dridex	GandCrab	XMRig		
Emotet	Rapid			
Gh0st	REvil/Sodinokibi			
LokiBot	WannaCry			
NanoCore				
Smokeloader				

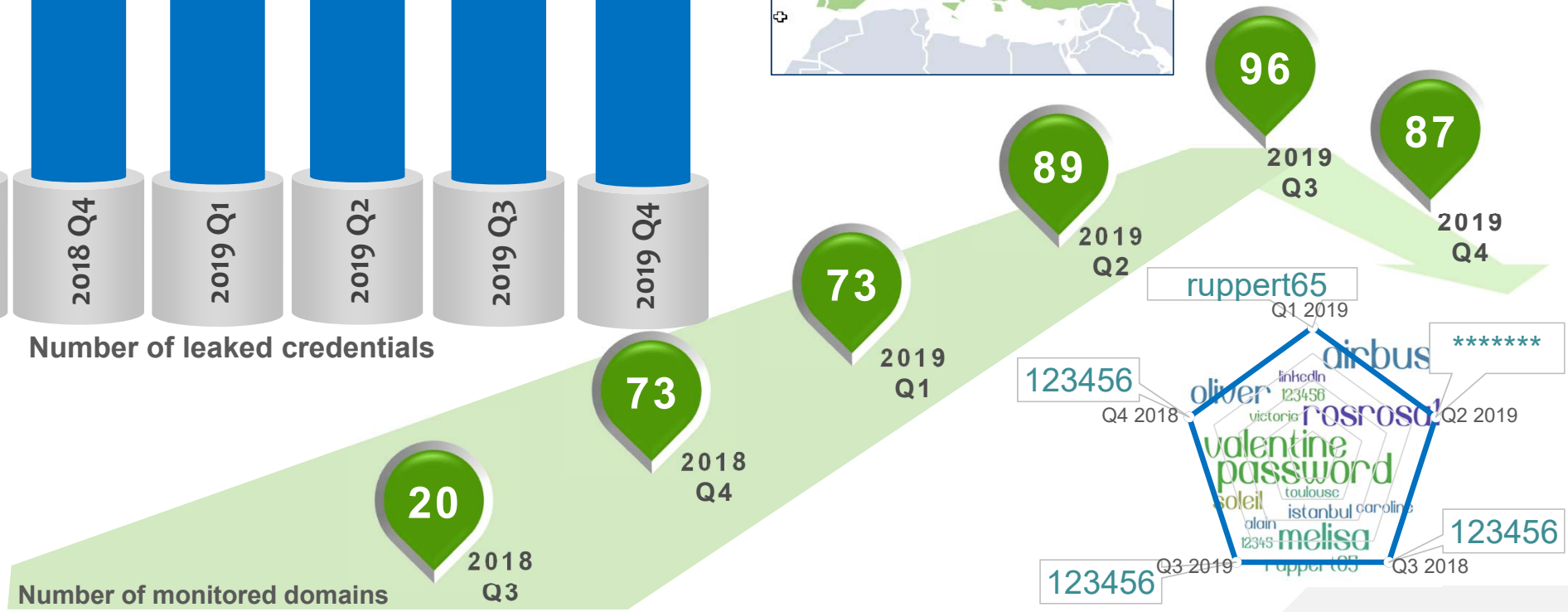
Top Malware


LokiBot 3,4%
Raccoon 3,4%
WannaCry 3,4%
REvil/Sodinokibi 3,4%
Rapid 3,4%
NanoCore 3,4%
Mirai 3,4%
Dharma 5,2%
GandCrab 5,2%
Gh0st 6,9%
XMRig 6,9%
Azorult 8,6%
Dridex 8,6%
Coinhive 10,3%
Emotet 24,1%

Credentials



Number of leaked credentials



Number of monitored domains

Scams impersonating EUROCONTROL Staff

Dear Julian,

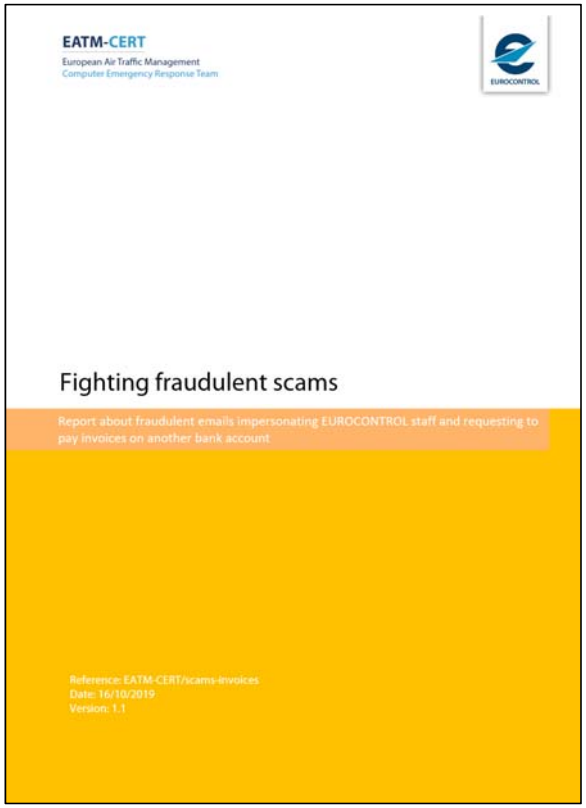
We hereby advise you of the change in our banking details due to the present slight logistics problem we are facing with our regular account, to avoid a failure or return on the arrival of your payment, we also ask you to inform us of your schedule date of payment on the outstanding invoices to enable us provide you the new banking details for the wire transfer.

We are waiting for your reply.

Kind Regards,

Alberto Varano

Financial Director
Accounts Receivable
Collection of Charges
EUROCONTROL-CRCO-R4
Rue de la Fusee 96
1130 Brussees, Belgium



Scams impersonating EUROCONTROL Staff

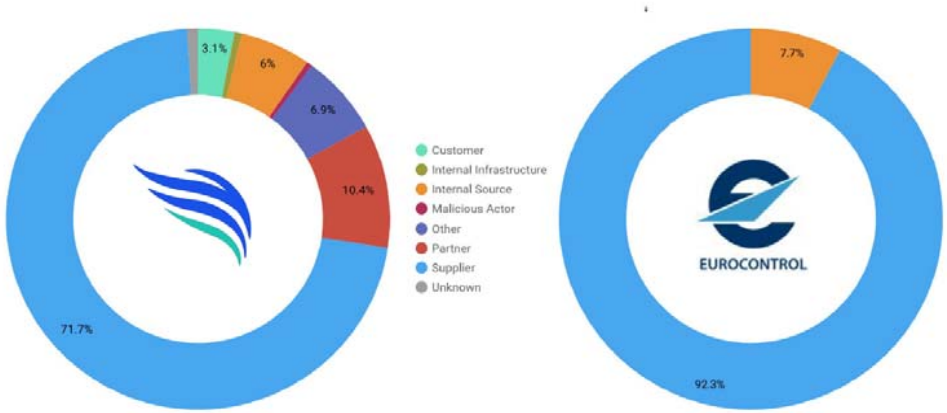
20 domain names suspended upon 2020 report on cyber in aviation request , another **3** suspensions requested:

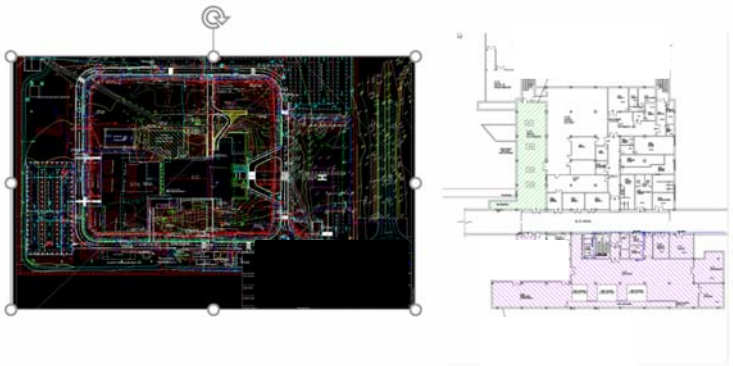
eurocontrolint.net
eurcontrol.int
eurocontroint.in
eurocontolint.net
eurocontrol.int.net
eurocontrols.net
mail-eurocontrol.com
eurocontrolt.net
eurocontrotint.net
euro-control.net
eurocontrol-intl.net
euro-control-int.org
eurcontrolint.net
eurocontrolin.int
eurocontrolint.eu.com
eurocontrolintl.net
eurocontrolinc.com
euro-control-int.net
euro-controlint.net
eurocontroladmin.net
eu-control.info
eurocontrols.org
eurocontrolx.net
eurocontroladmincentre.net
eurocontrolcrco4.com
eurocontrolintl.in
euro-control.net
euro-control.eu
euro-control.org
eurocontroint.net
eurocontrol.com
eurocontrolintl.int
eurocontrolint.in
eurocontroint.in
eurocontrolints.net
eurocontroladmin.in
eurocontrolunits.net
eurocontrolaudits.net
eurocontrolaudit.net
eurocontrolintl.com
int-eurocontrol.com
euro-control-int.com
eurocontrolunit.net
eurocontroll.int

Sensitive document leaks

Origin of the leaks

Your suppliers are the n°1 cause of data leaks





Fraudulent websites impersonating airlines

Ryanair

https://c.golddiggergames.be/9661/61283

easyJet

http://www.easyonefly.com

American Airlines

http://www.aa.com-flightus.com

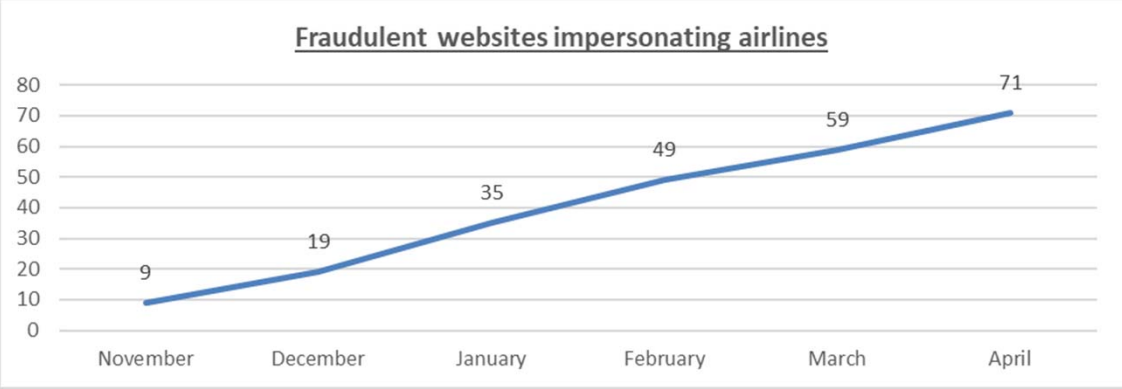
Singapore Airlines

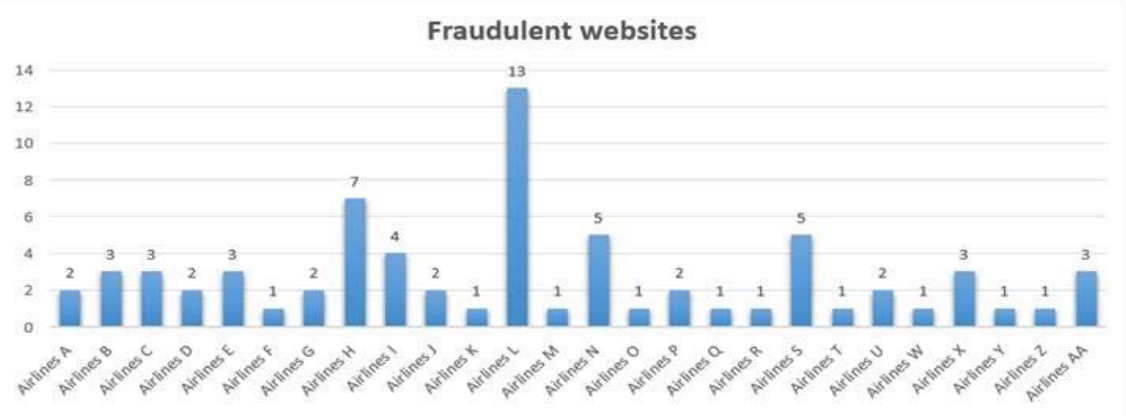
http://www.singaporeair.com/free-tickets/

Qantas Airlines

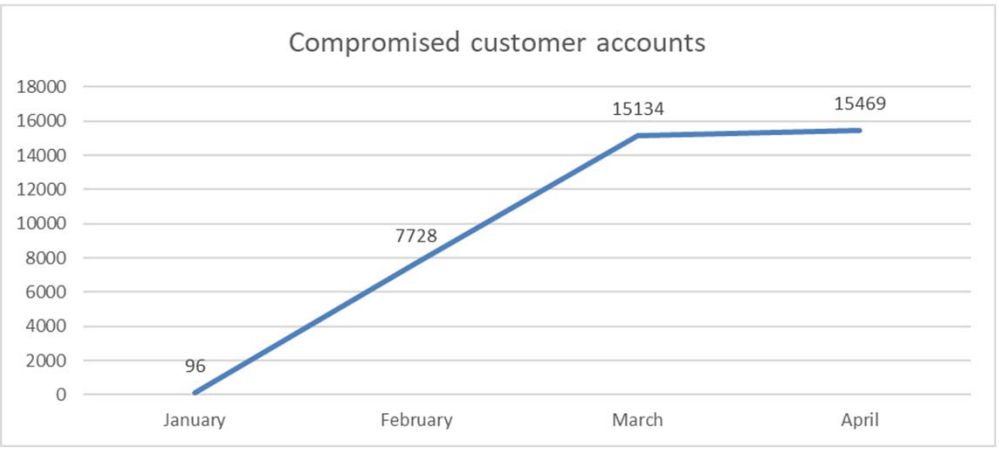
http://www.com-cana.com/?Anniversary-dUMwH

Fraudulent websites impersonating airlines





Compromised customers accounts (loyalty programs)



Supporting
European
Aviation

EUROCONTROL

Attacks, Mitigation and Detection Means

FOUNDING MEMBER SESAR JOINT UNDERTAKING

NETWORK MANAGER

MITRE ATT&CK : Techniques most commonly used to attack aviation

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
Spearphishing Attachment	Command-Line Interface	Registry Run Keys / Startup Folder	Scheduled Task	Obfuscated Files or Information	Credential Dumping	System Network Configuration Discovery	Remote Desktop Protocol	Input Capture	Remote File Copy	Data Compressed	Data Encrypted for Impact
Valid Accounts	Scripting	Scheduled Task	Valid Accounts	Scripting	Input Capture	Process Discovery	Remote File Copy	Data from Local System	Commonly Used Port	Data Encrypted	Disk Structure Wipe
Drive-by Compromise	PowerShell	Valid Accounts	Process Injection	Valid Accounts	Brute Force	Account Discovery	Pass the Ticket	Data Staged	Standard Application Layer Protocol	Data Transfer Size Limits	Resource Hijacking
External Remote Services	Scheduled Task	New Service	New Service	Code Signing	Credentials in Files	File and Directory Discovery	Remote Services	Email Collection	Connection Proxy	Exfiltration Over Command and Control Channel	System Shutdown/Reboot
Spearphishing Link	Exploitation for Client Execution	External Remote Services	Accessibility Features	Deobfuscate/Decode Files or Information	Credentials from Web Browsers	Network Service Scanning	Windows Admin Shares	Audio Capture	Web Service	Exfiltration Over Alternative Protocol	
Exploit Public-Facing Application	User Execution	Create Account	Bypass User Account Control	File Deletion	Network Sniffing	Remote System Discovery	Windows Remote Management	Automated Collection	Custom Command and Control Protocol		
Supply Chain Compromise	Windows Management Instrumentation	Redundant Access	Web Shell	Masquerading	Account Manipulation	System Information Discovery	Component Object Model and Distributed COM	Data from Information Repositories	Multi-Stage Channels		
Trusted Relationship	Dynamic Data Exchange	Web Shell	Exploitation for Privilege Escalation	Process Injection		System Network Connections Discovery	Exploitation of Remote Services	Video Capture	Standard Non-Application Layer Protocol		
	Rundll32	Accessibility Features	DLL Search Order Hijacking	Connection Proxy		System Owner/User Discovery	Pass the Hash	Screen Capture	Uncommonly Used Port		
	Service Execution	Bootkit	Application Shimming	Redundant Access		Network Share Discovery		Data from Network Shared Drive	Fallback Channels		
	Graphical User Interface	Component Firmware		Rundll32		Permission Groups Discovery			Multi-hop Proxy		
	Mshta	BITS Jobs		Software Packing		Security Software Discovery			Data Obfuscation		
	Regsvr32	Modify Existing Service		Web Service		System Service Discovery			Domain Fronting		
	Execution through API	DLL Search Order Hijacking		Bypass User Account Control		Virtualization/Sandbox Evasion			Data Encoding		
	Component Object Model and Distributed COM	Shortcut Modification		DLL Side-Loading		Query Registry			Domain Generation Algorithms		
	Windows Remote Management	Windows Management Instrumentation Event Subscription		DLL Search Order Hijacking		Network Sniffing			Standard Cryptographic Protocol		
	CMSTP	Winlogon Helper DLL		Hidden Files and Directories		Peripheral Device Discovery					
	Compiled HTML File	Account Manipulation		Hidden Window							
		Application Shimming		Indicator Removal from Tools							
		Hidden Files and Directories		Indicator Removal on Host							
				Modify Registry							
				Mshta							
				Network Share Connection Removal							
				Process Hollowing							
				Regsvr32							
				Rootkit							
				Template Injection							
				Virtualization/Sandbox Evasion							
				Binary Padding							
				BITS Jobs							
				Disabling Security Tools							
				Execution Guardrails							
				Compiled HTML File							
				Component Firmware							
				CMSTP							
				Clear Command History							
				Compile After Delivery							

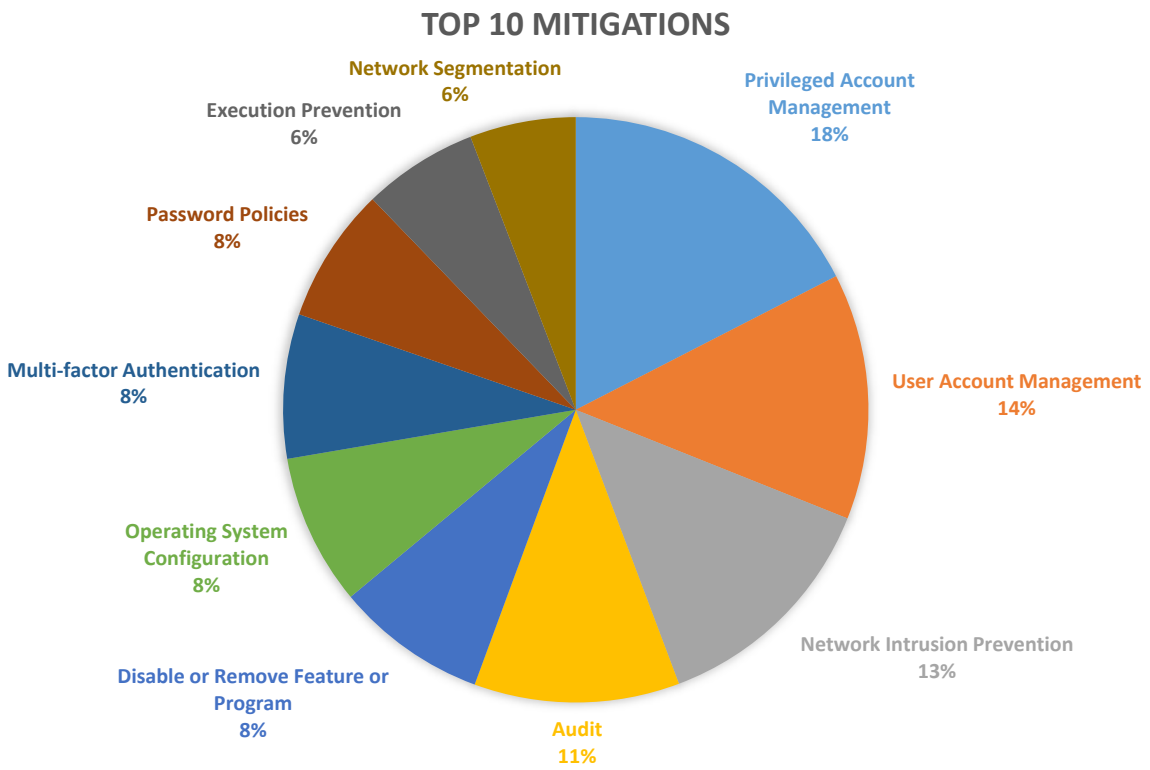
List of APTs targeting aviation

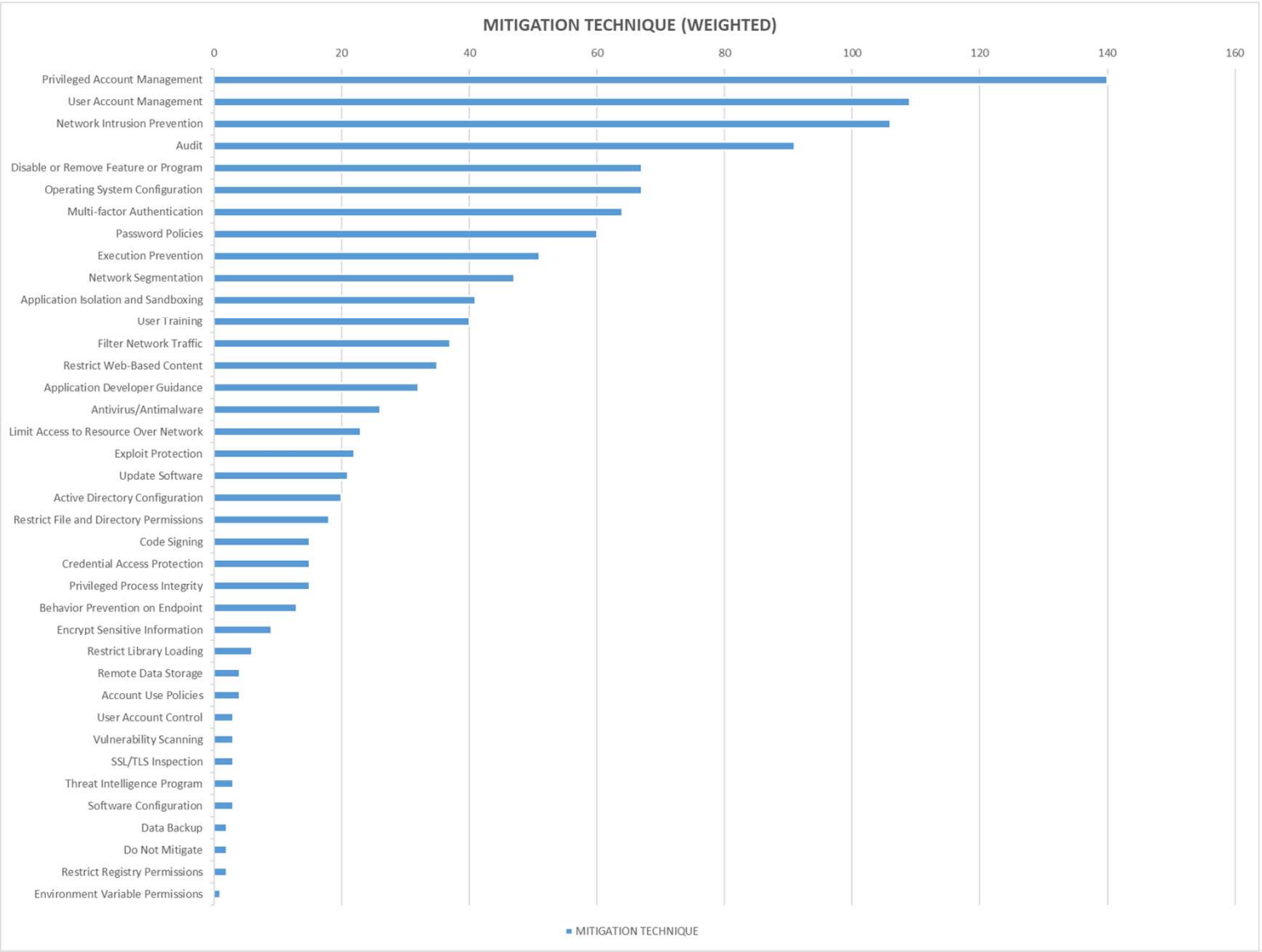
APT Group	Country		Sponsor	Motivation	Countries
APT 1	China		State-sponsored	Information theft and espionage	Europe, Asia & Pacific, South Africa, Midde East, North America
APT 2	China		State-sponsored	Information theft and espionage	North America
APT 3	China		State-sponsored	Information theft and espionage	Europe, Asia & Pacific, North America
APT 10	China		[unknown]	Information theft and espionage	Asia & Pacific, Europe, South/Latin America, South Africa, Middle East, North America
APT 14	China		State-sponsored	Information theft and espionage	Asia & Pacific, Europe, North America
APT 18	China		State-sponsored	Information theft and espionage	North America
APT 20	China		[unknown]	Information theft and espionage	Asia & Pacific, North America
APT 27	China		[unknown]	Information theft and espionage	Asia & Pacific, North America, Middle East, Europe
APT 29	Russia		State-sponsored	Information theft and espionage	Asia & Pacific, Europe, South/Latin America
APT 33	Iran		State-sponsored	Information theft, espionage and sabotage	Middle East, Asia & Pacific, North America
APT 37	North Korea		State-sponsored	Information theft and espionage	Europe, Asia & Pacific, Middle East
APT 39	Iran		State-sponsored	Information theft and espionage	Europe, Middle East, Asia & Pacific, North America
APT 41	China		[unknown]	[unknown]	Asia & Pacific, North America, Europe, Middle Easr

List of APTs targeting aviation

Axiom	China		State-sponsored	Information theft and espionage	Asia & Pacific, North America
DNSpionag	Iran		State-sponsored	Information theft and espionage	Europe, Asia & Pacific, Middle East, North Africa, North America
Equation	USA		State-sponsored	Sabotage and destruction	Middle East, Asia & Pacific, South/Latin America, Europe, South Africa, North America
FIN7	Russia		[unknown]	Financial gain	Europe, North America
Ke3chang	China		State-sponsored	Information theft and espionage	European Union, Asia & Pacific
Leafminer	Iran		[unknown]	Information theft and espionage	Europe, Asia & Pacific, Middle East, North America
Leviathan	China		[unknown]	Information theft and espionage	Europe, Asia & Pacific, Middle East, North America
Longhorn	USA		State-sponsored	Information theft and espionage	Middle East, Europe, Asia & Pacific, Africa
Lucky Cat	China		[unknown]	Information theft and espionage	Asia & Pacific
Molerats	Gaza		Hamas - political organization and militant group	Information theft and espionage	Asia & Pacific, Middle East, Europe, North America
MuddyWa	Iran		[unknown]	Information theft and espionage	Middle East, Asia & Pacific, Europe, North America
Patchwork	India		[unknown]	Information theft and espionage	Asia & Pacific, Middle East, North America
TeleBots	Russia		[unknown]	Sabotage and destruction	Worldwide
Tropic Tro	[unknown]		[unknown]	Information theft and espionage	Asia & Pacific

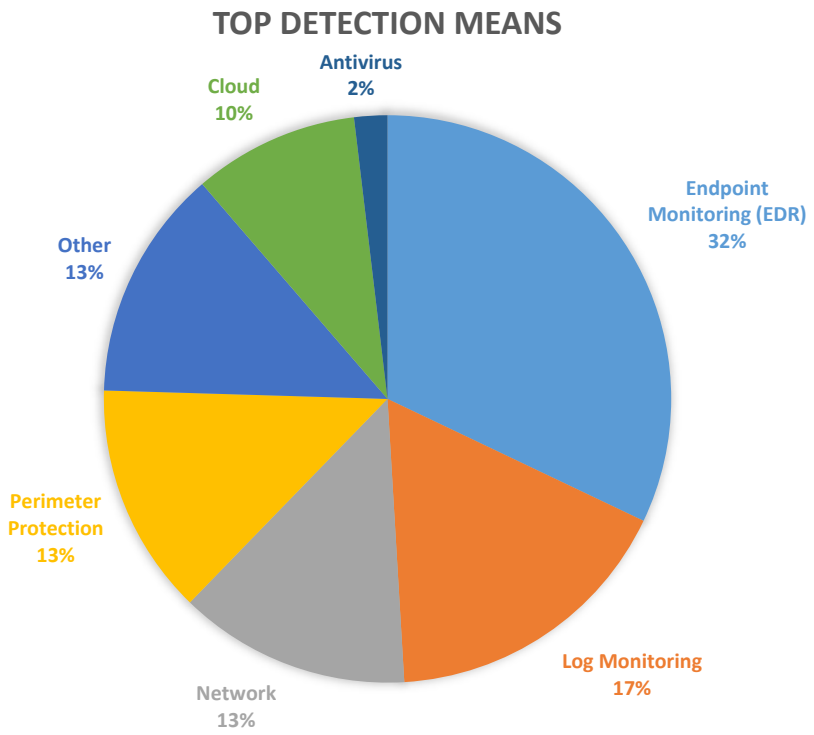
Top 10 Mitigation Means

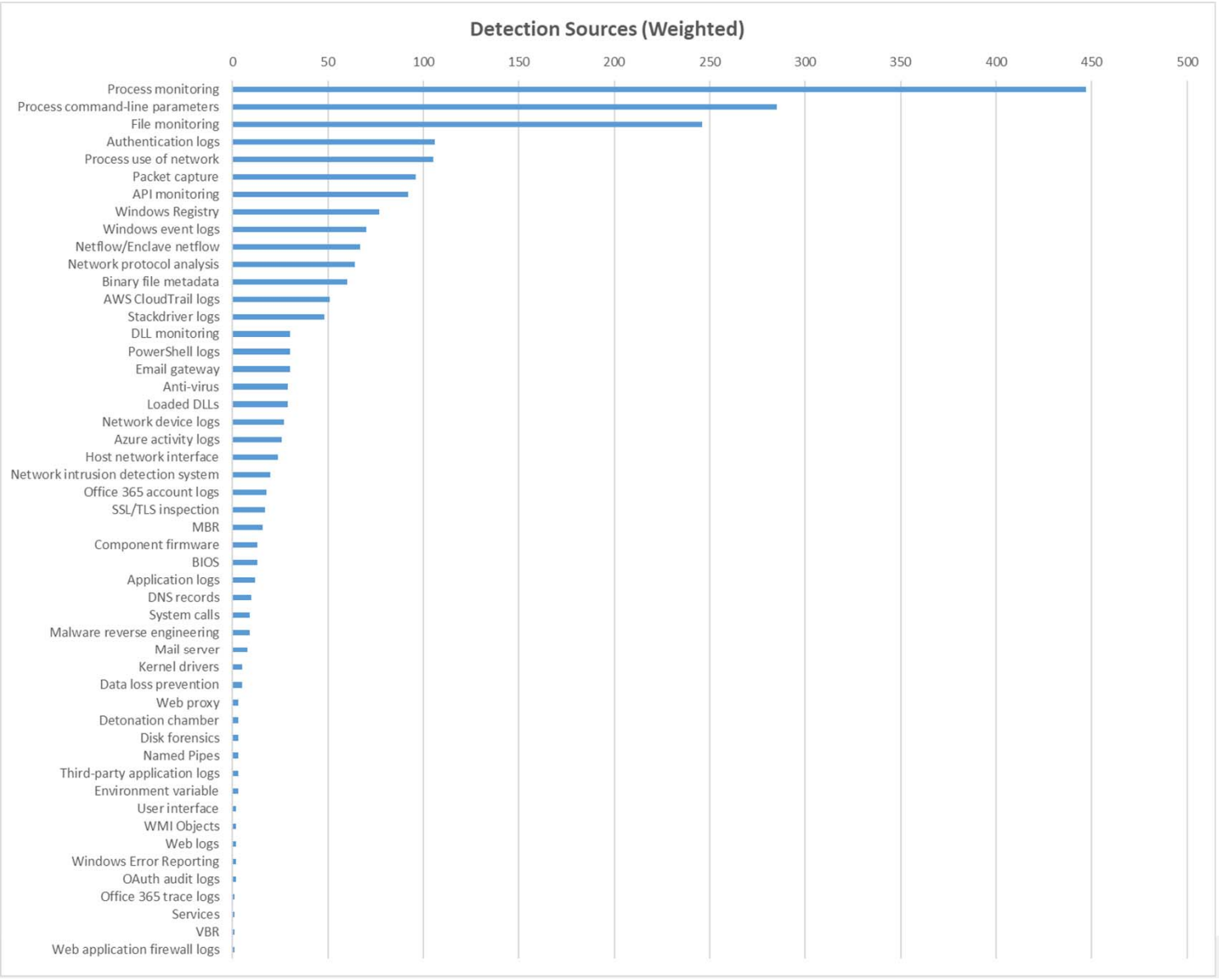




Most stimulated Mitigation Means

Top Detection Means



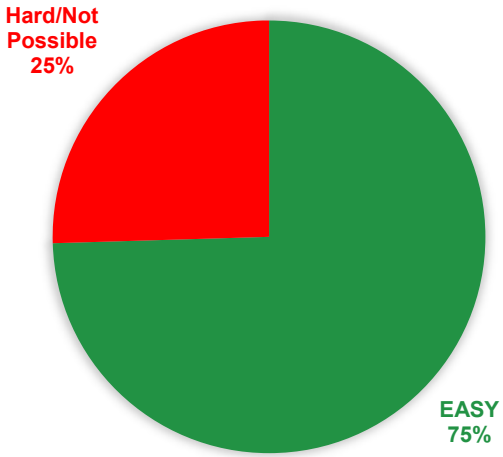


EUROCONTROL

Most needed Detection Means

Surprise

MITIGATION POSSIBILITY



TACTIC	TECHNIQUE
Persistence	Registry Run Keys / Startup Folder
Discovery	System Network Configuration Discovery
Discovery	Process Discovery
Collection	Data from Local System
Defense Evasion	File Deletion
Discovery	System Information Discovery
Discovery	System Owner/User Discovery
Defense Evasion	Code Signing
Defense Evasion	Deobfuscate/Decode Files or Information
Discovery	File and Directory Discovery
Credential Access & Collection	Input Capture
Discovery	Remote System Discovery
Discovery	System Network Connections Discovery
Collection	Data Staged
Exfiltration	Data Encrypted
Discovery	Network Share Discovery
Discovery	Peripheral Device Discovery
Discovery	Permission Groups Discovery
Collection	Screen Capture
Discovery	Security Software Discovery
Discovery	System Service Discovery
Collection	Audio Capture
Defense Evasion	Binary Padding
Defense Evasion	Compile After Delivery
Persistence & Defense Evasion	Component Firmware
Collection	Data from Network Shared Drive
Execution	Graphical User Interface
Persistence & Defense Evasion	Hidden Files and Directories
Defense Evasion	Indicator Removal from Tools
Defense Evasion	Network Share Connection Removal
Defense Evasion	Process Hollowing
Discovery	Query Registry
Impact	Resource Hijacking
Defense Evasion	Rootkit
Impact	System Shutdown/Reboot
Collection	Video Capture
Defense Evasion & Discovery	Virtualization/Sandbox Evasion

- For APT targeting aviation, only 75% of techniques have Mitigations Means
- 25% of the techniques are very hard/impossible to mitigate
- Detection is vital

Supporting
European
Aviation

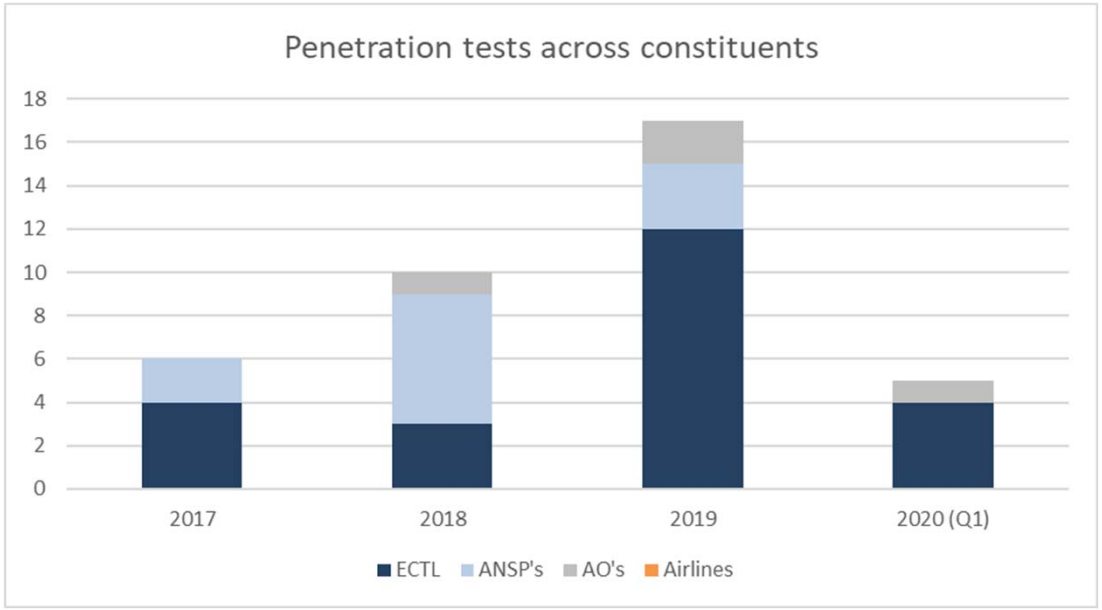
EUROCONTROL

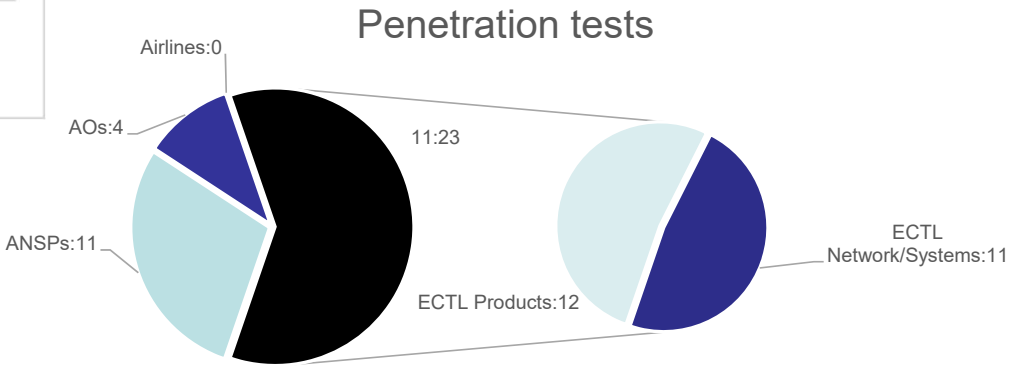
Vulnerabilities

FOUNDING MEMBER SESAR JOINT UNDERTAKING

NETWORK MANAGER

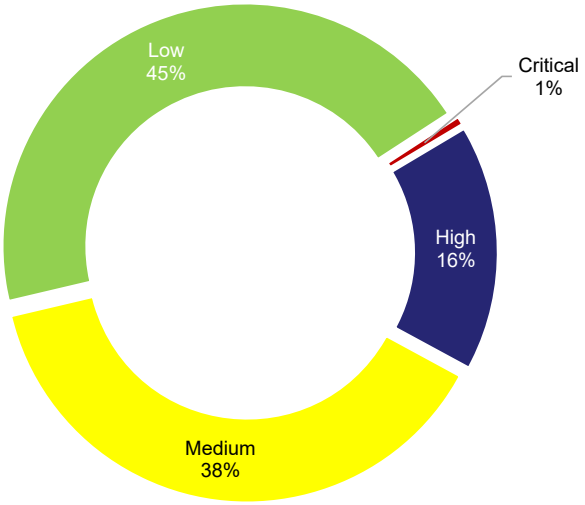
Pentests


Penetration tests across constituents
18
16
14
12
10
8
6
4
2
0
2017
2018
2019
2020 (Q1)
ECTL
ANSP's
AO's
Airlines

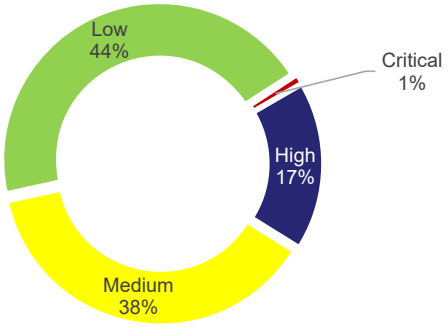

Penetration tests
Airlines:0
AOs:4
11:23
ANSPs:11
ECTL Products:12
ECTL Network/Systems:11

Discovered vulnerabilities (pentests)

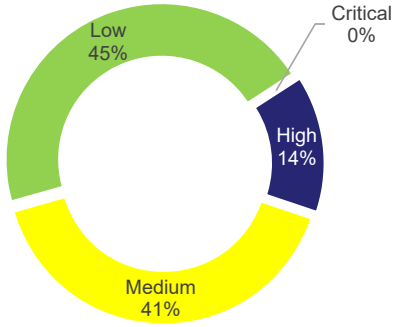
Discovered Vulnerabilities

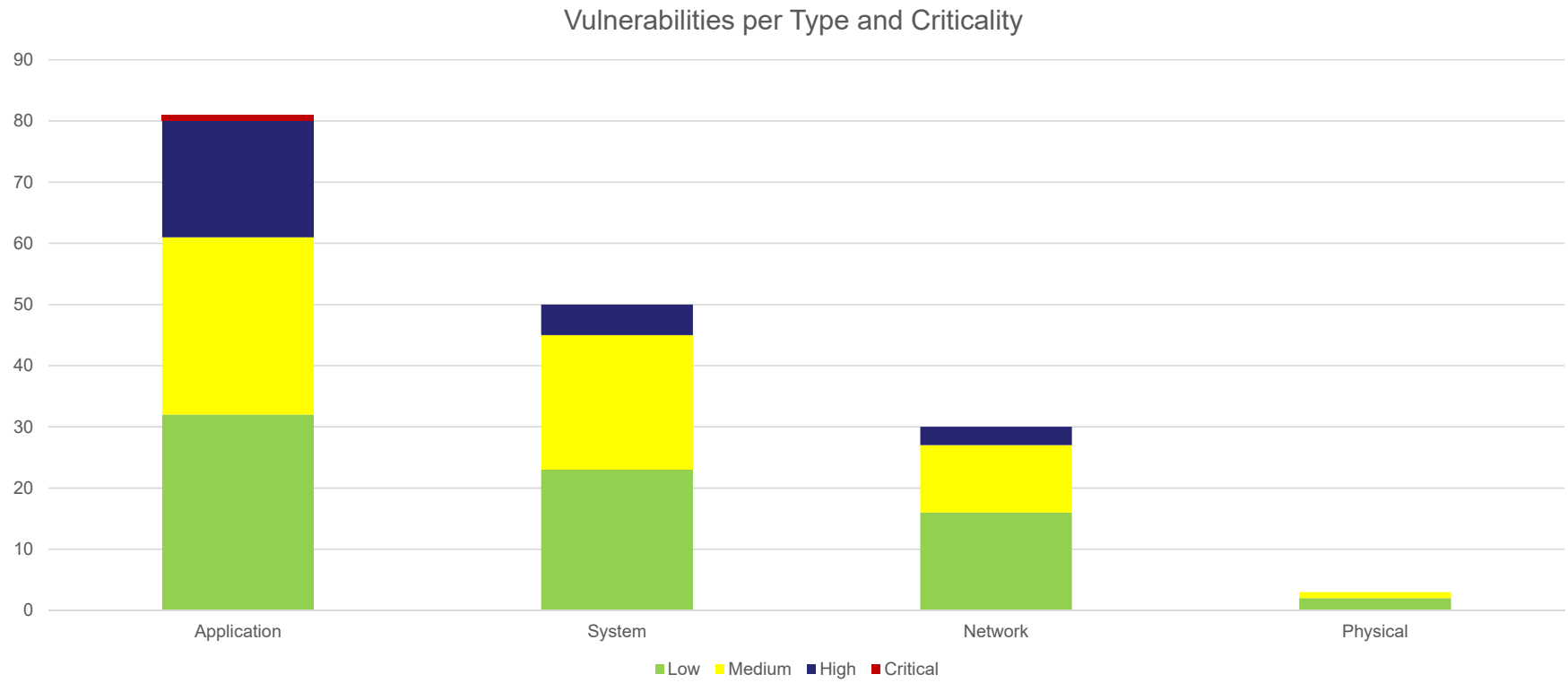


Discovered Vulnerabilities at EUROCONTROL

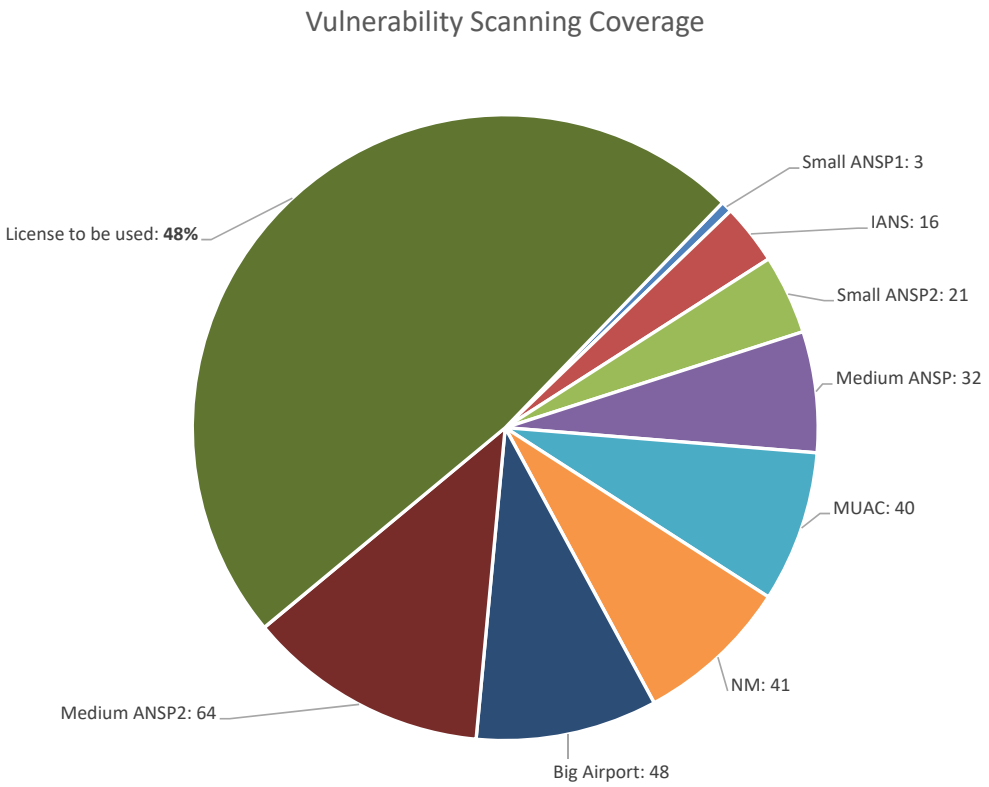


Discovered Vulnerabilities Constituents




Vulnerabilities per Type and Criticality
90
80
70
60
50
40
30
20
10
0
Application
System
Network
Physical
Low
Medium
High
Critical

Vulnerability scanning service



Supporting
European
Aviation

EUROCONTROL

Financial impact

FOUNDING MEMBER SESAR JOINT UNDERTAKING

NETWORK MANAGER

Financial impact on aviation

- Cyber-crime/attacks financial damages on aviation : ~ tens of billion €/year
- Fraudulent website: ~1 Bn $/year (IATA)
- Frequent flyer miles: unknown … but probably significant

- Scams impersonating EUROCONTROL:
  - Cost of the attack: few hundred €/year + some human resource – inexpensive)
  - A top 5 European airline paid **7 M€** to fraudsters in 2016.
  - A top 5 world express delivery company paid **900 K€** to fraudsters in 2016.
  - A regional airline paid **1 M€** to fraudsters in 2018.

Supporting
European
Aviation

EUROCONTROL

Human resources

FOUNDING MEMBER SESAR JOINT UNDERTAKING

NETWORK MANAGER

Cyber resources

- Cyber expertise:
  - Shortage of resources
  - Not enough universities offering cyber cursus
  - Aviation at financial risk => not attractive

- How to attract and retain cyber resources?
  - Training – maintain competence
  - Adding-value tasks (use of AI/ML to reduce “boring” tasks)
  - Good salaries
  - Visibility
  - Propose challenges / innovation

Supporting
European
Aviation

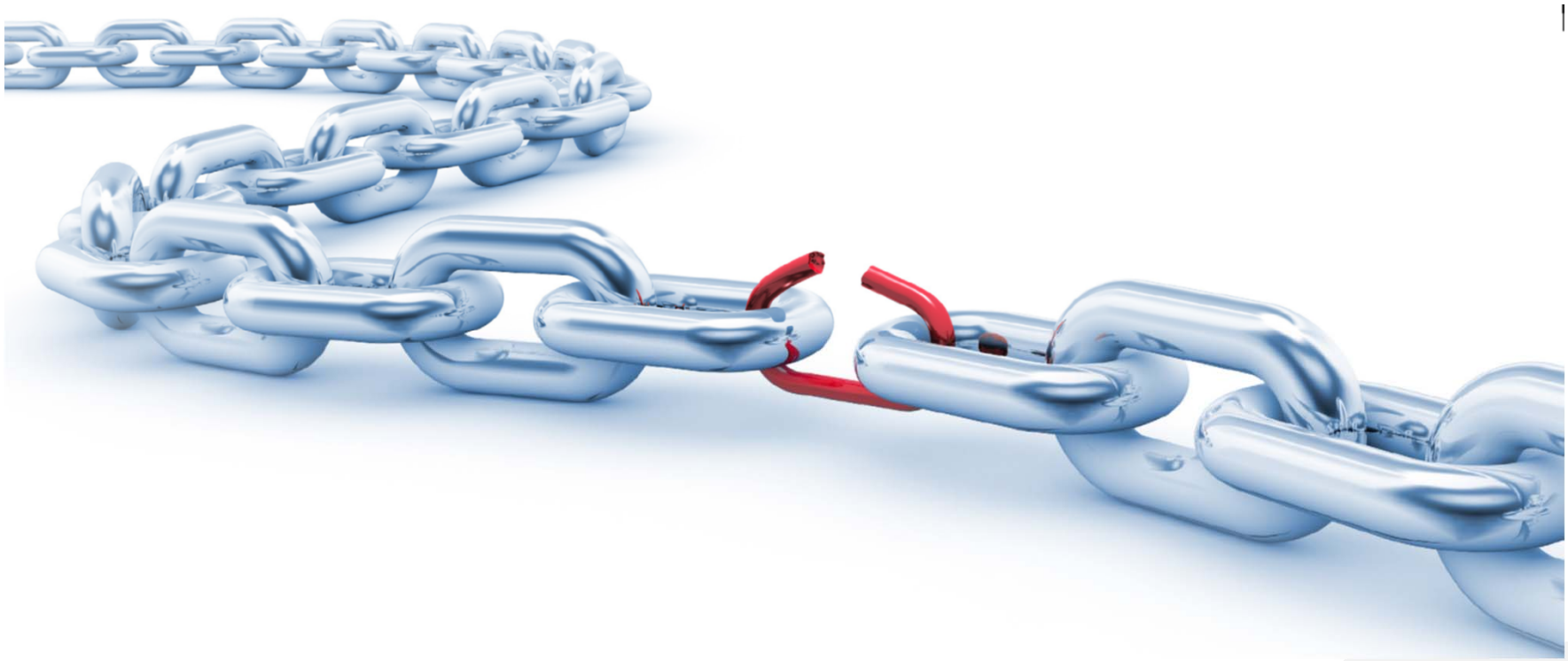
EUROCONTROL

Moving towards cyber-resilience

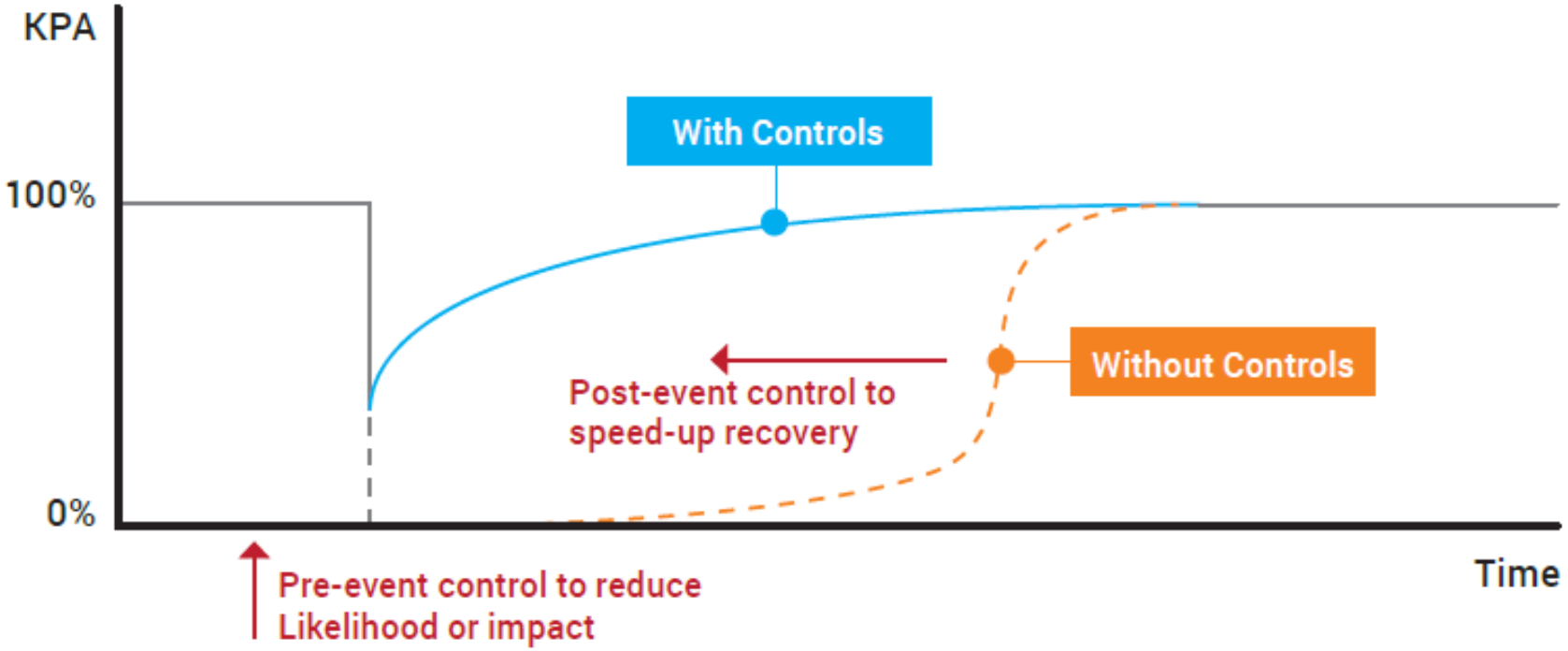
FOUNDING MEMBER SESAR JOINT UNDERTAKING

NETWORK MANAGER

All together … as we are as strong as the weakest link



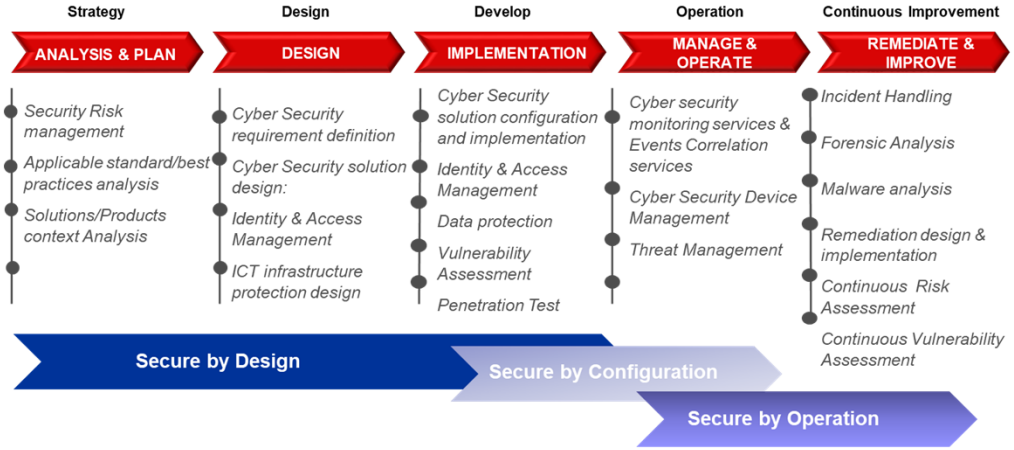
BECOME CYBER-RESILIENT … ALL TOGETHER



Cybersecurity management framework

Invest in Humans

Apply a secure development lifecycle



Adapt processes

Build a Trust Framework

AVIATION ISAC

ISAC EUROPEAN AVIATION

EASA European Aviation Safety Agency

European Centre for Cybersecurity in Aviation

AIR TRAFFIC MANAGEMENT CYBER SECURITY SERVICES

EUROCONTROL

KEEP CALM & CALL EATM-CERT

eatm-cert@eurocontrol.int or +32 2 729 46 55

THANK YOU

patrick.mana@eurocontrol.int