Supporting
European
Aviation

EUROCONTROL

CERT for ATM – Communication between CERT constituents

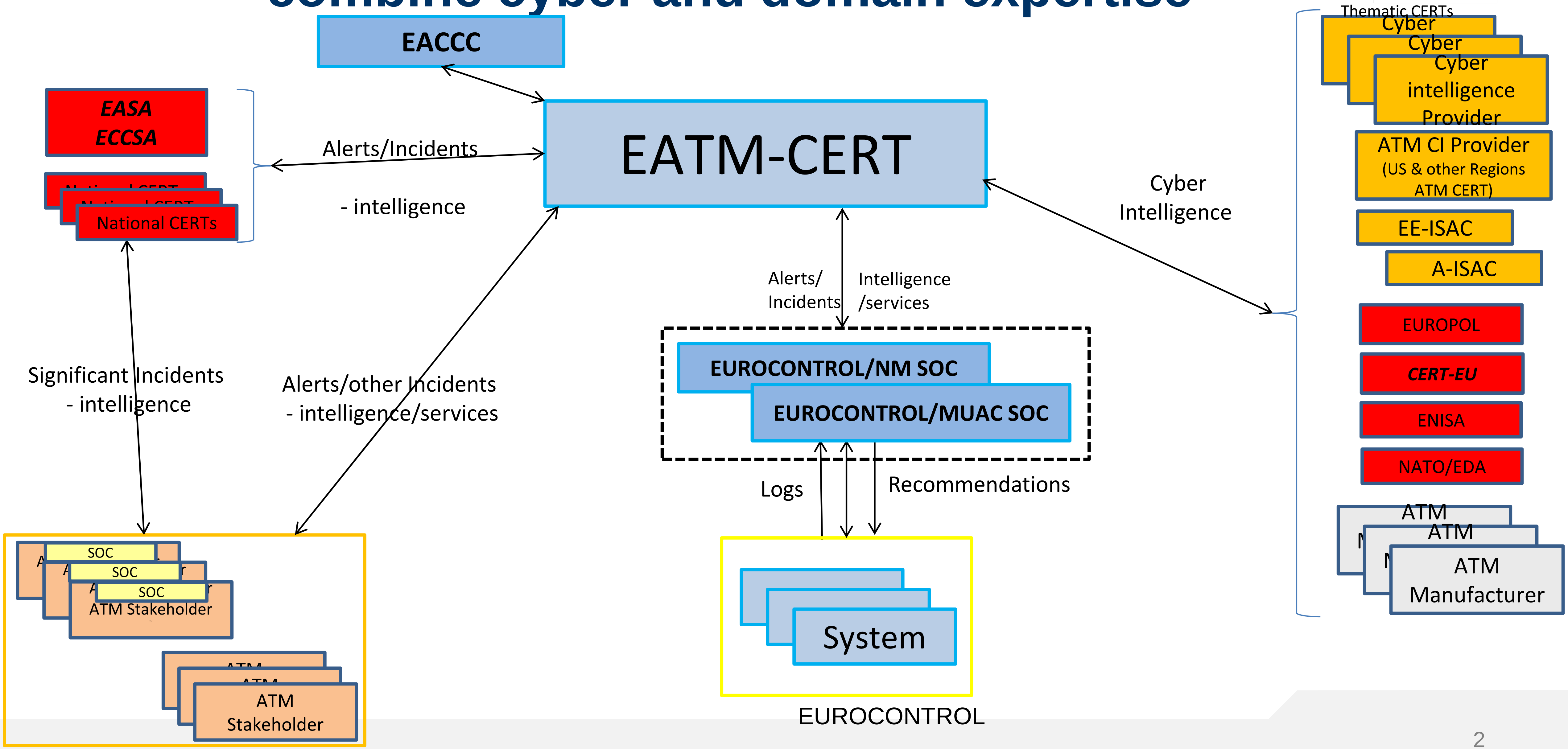
IFE

Patrick MANA
EATM-CERT Manager

FOUNDING MEMBER SESAR JOINT UNDERTAKING

NETWORK MANAGER

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



EACCC

EATM-CERT

EASA ECCSA

National CERTs

Alerts/Incidents

- intelligence

Significant Incidents
- intelligence

Alerts/other Incidents
- intelligence/services

Alerts/ Incidents

Intelligence /services

EUROCONTROL/NM SOC

EUROCONTROL/MUAC SOC

Logs

Recommendations

System

EUROCONTROL

SOC

ATM Stakeholder

ATM Stakeholder

Cyber Intelligence

Thematic CERTs

Cyber intelligence Provider

ATM CI Provider (US & other Regions ATM CERT)

EE-ISAC

A-ISAC

EUROPOL

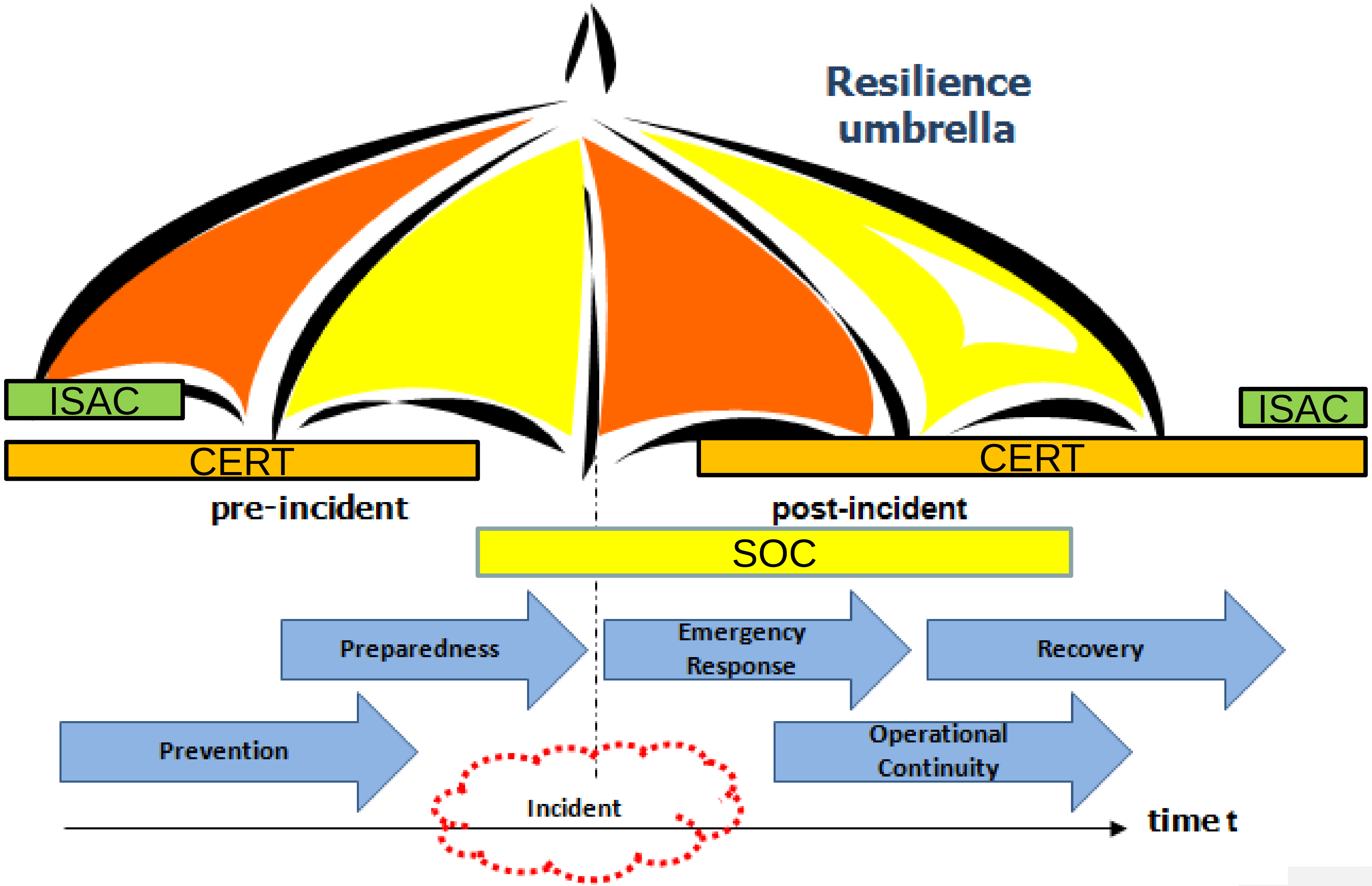
CERT-EU

ENISA

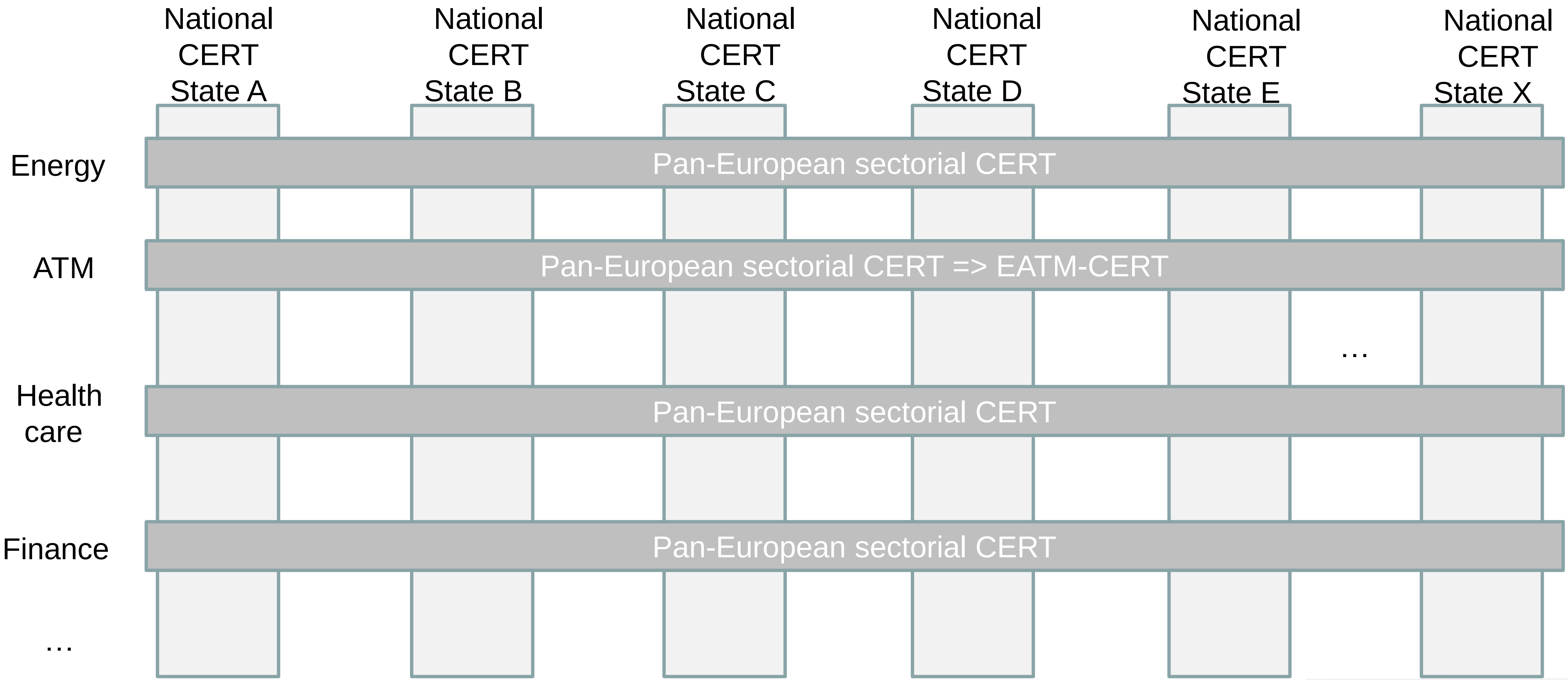
NATO/EDA

ATM Manufacturer

ISAC & CERT & SOC



EATM-CERT and European National CERTs



National CERT State A

National CERT State B

National CERT State C

National CERT State D

National CERT State E

…

National CERT State X

Energy: Pan-European sectorial CERT

ATM: Pan-European sectorial CERT => EATM-CERT

Health care: Pan-European sectorial CERT

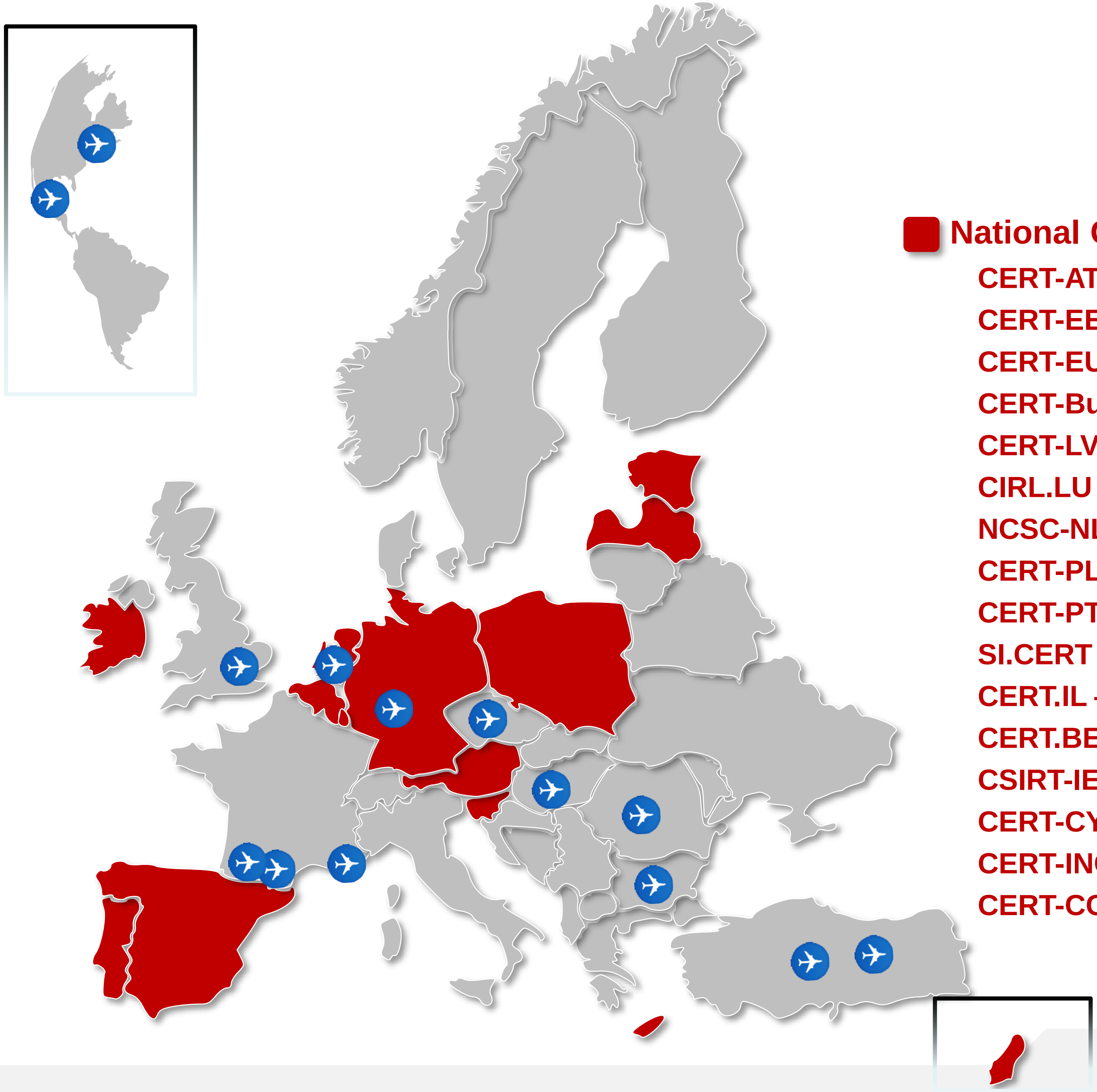
Finance: Pan-European sectorial CERT

…

MISP

🟦 Aviation PARTNERS

- CERT-AIRBUS A/C
- CERT-IST – Thales
- DLH-DE –Lufthansa Group
- CERT-THY – Turkish Airlines
- AeroMexico
- IATA (by 3rd party CTI platform)
- Amadeus
- ECCSA (test)
- CAA-RO - Romanian CAA
- Airport 1
- Heathrow airport
- Schiphol Airport
- Prague Airport
- Hungarocontrol
- BULATSA
- DHMI



🟥 National CERT

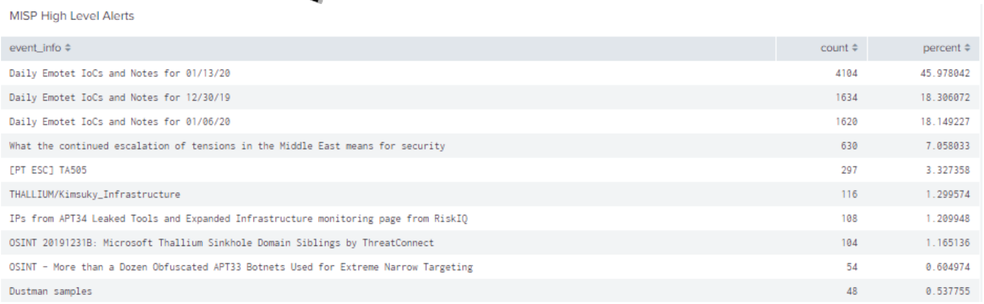
- CERT-AT – Austria
- CERT-EE – Estonia
- CERT-EU – EU institutions
- CERT-Bund – Germany
- CERT-LV – Latvia
- CIRL.LU – Luxembourg
- NCSC-NL – Netherlands
- CERT-PL – Poland
- CERT-PT – Portugal
- SI.CERT – Slovenia
- CERT.IL – Israel
- CERT.BE – Belgium
- CSIRT-IE – Ireland
- CERT-CY-Cyprus
- CERT-INCIBE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

MISP - Integration

SIEM

splunk>

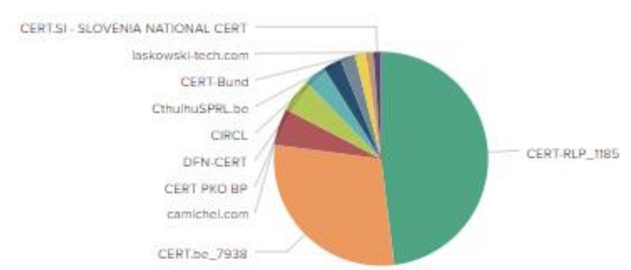
MISP
Threat Sharing

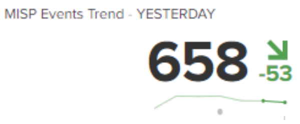


MISP High Level Alerts

event_info ⇕	count ⇕	percent ⇕
Daily Emotet IoCs and Notes for 01/13/20	4104	45.978042
Daily Emotet IoCs and Notes for 12/30/19	1634	18.306072
Daily Emotet IoCs and Notes for 01/06/20	1620	18.149227
What the continued escalation of tensions in the Middle East means for security	630	7.058033
[PT ESC] TA505	297	3.327358
THALLIUM/Kimsuky_Infrastructure	116	1.299574
IPs from APT34 Leaked Tools and Expanded Infrastructure monitoring page from RiskIQ	108	1.209948
OSINT 20191231B: Microsoft Thallium Sinkhole Domain Siblings by ThreatConnect	104	1.165136
OSINT - More than a Dozen Obfuscated APT33 Botnets Used for Extreme Narrow Targeting	54	0.604974
Dustman samples	48	0.537755

Last 30 days MISP CERT Activity

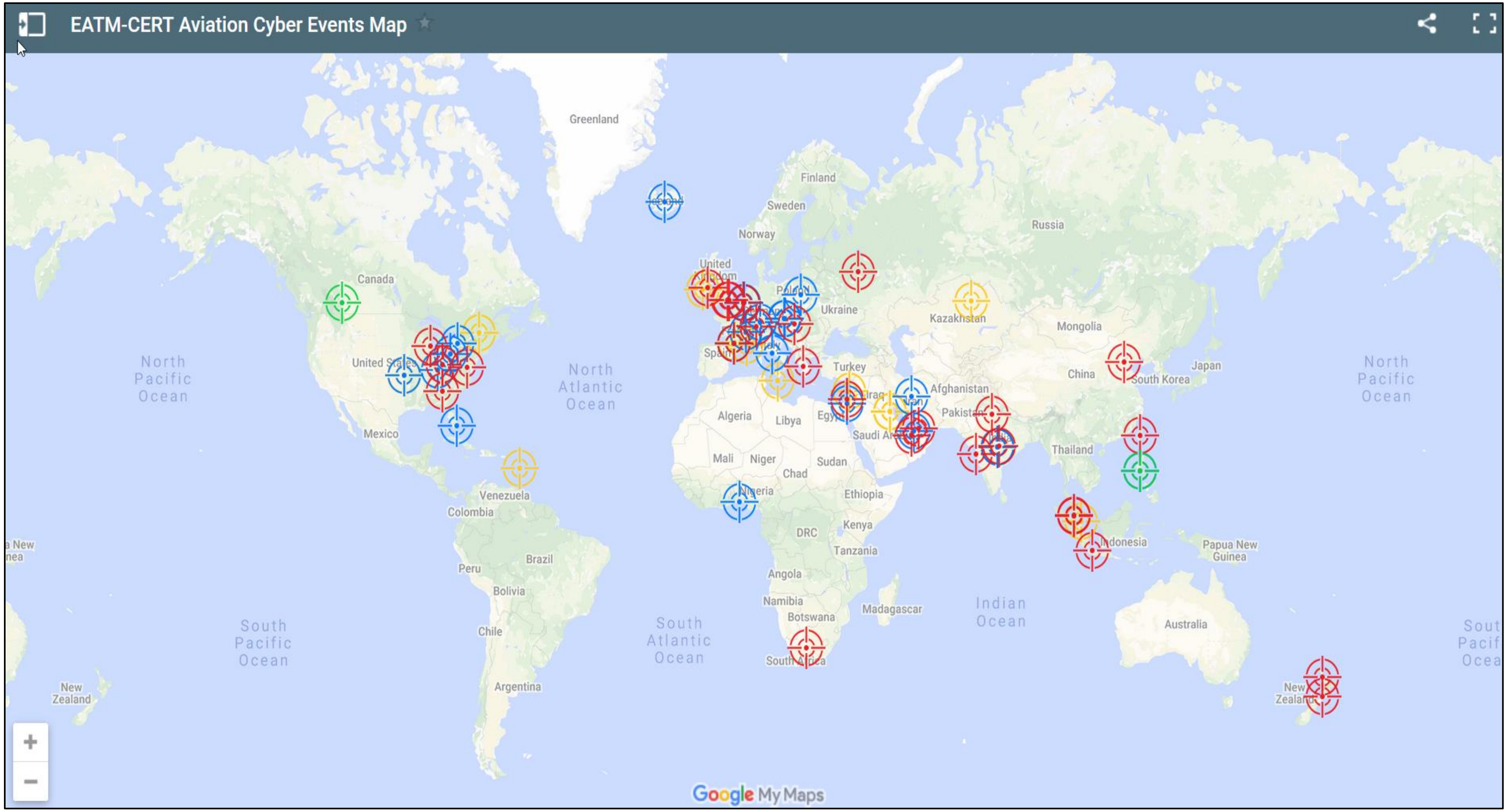



MISP Events Trend - YESTERDAY

658 ↘ -53

FIREWALL

Quarterly cyber threat landscape report
TLP:WHITE CTI tools – raising awareness



Sharing cyber-information

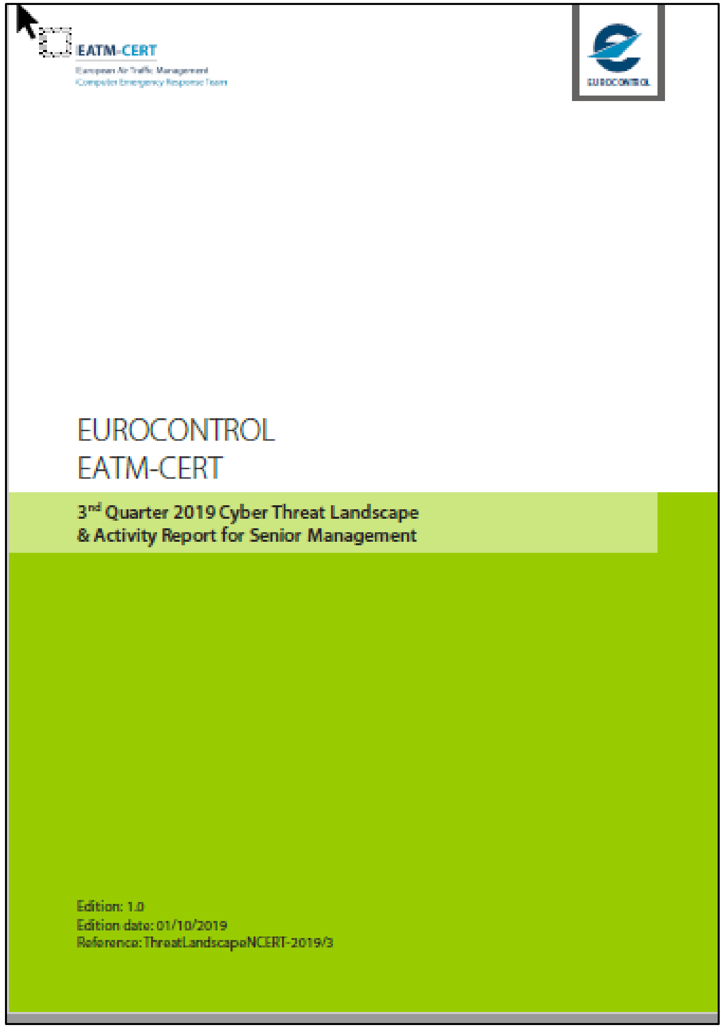
EATM-CERT

European Air Traffic Management
Computer Emergency Response Team

Security Alert

EMOTET Banking Trojan Phishing Attacks

Reference: ECTAR-Alert-008-2018
Date: 07/11/2018
Version: 1.0



EATM-CERT

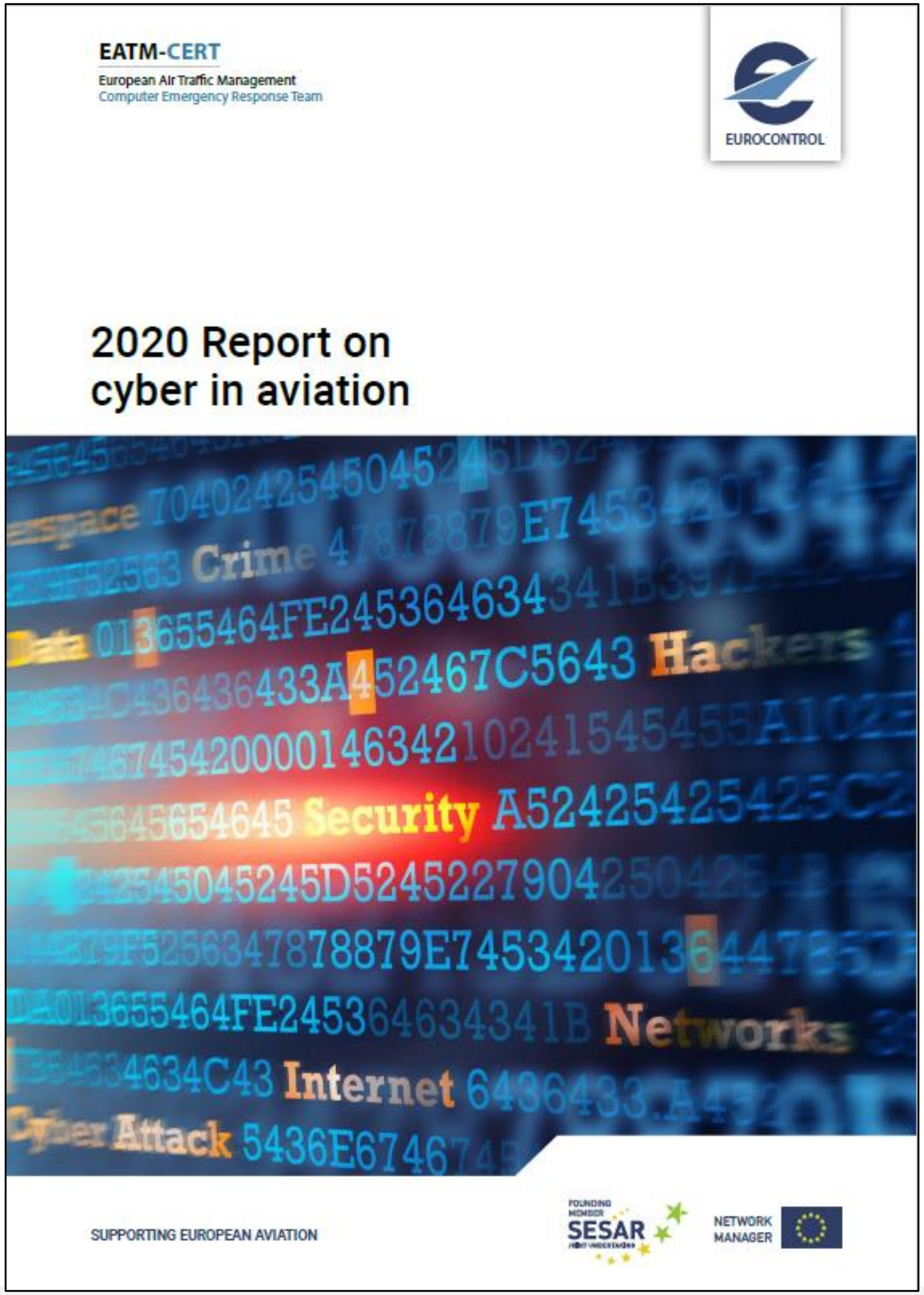
European Air Traffic Management
Computer Emergency Response Team

EUROCONTROL
EATM-CERT

3rd Quarter 2019 Cyber Threat Landscape
& Activity Report for Senior Management

Edition: 1.0
Edition date: 01/10/2019
Reference: ThreatLandscapeNCERT-2019/3

Report is TLP:GREEN



EATM-CERT
European Air Traffic Management
Computer Emergency Response Team

EUROCONTROL

2020 Report on cyber in aviation

SUPPORTING EUROPEAN AVIATION

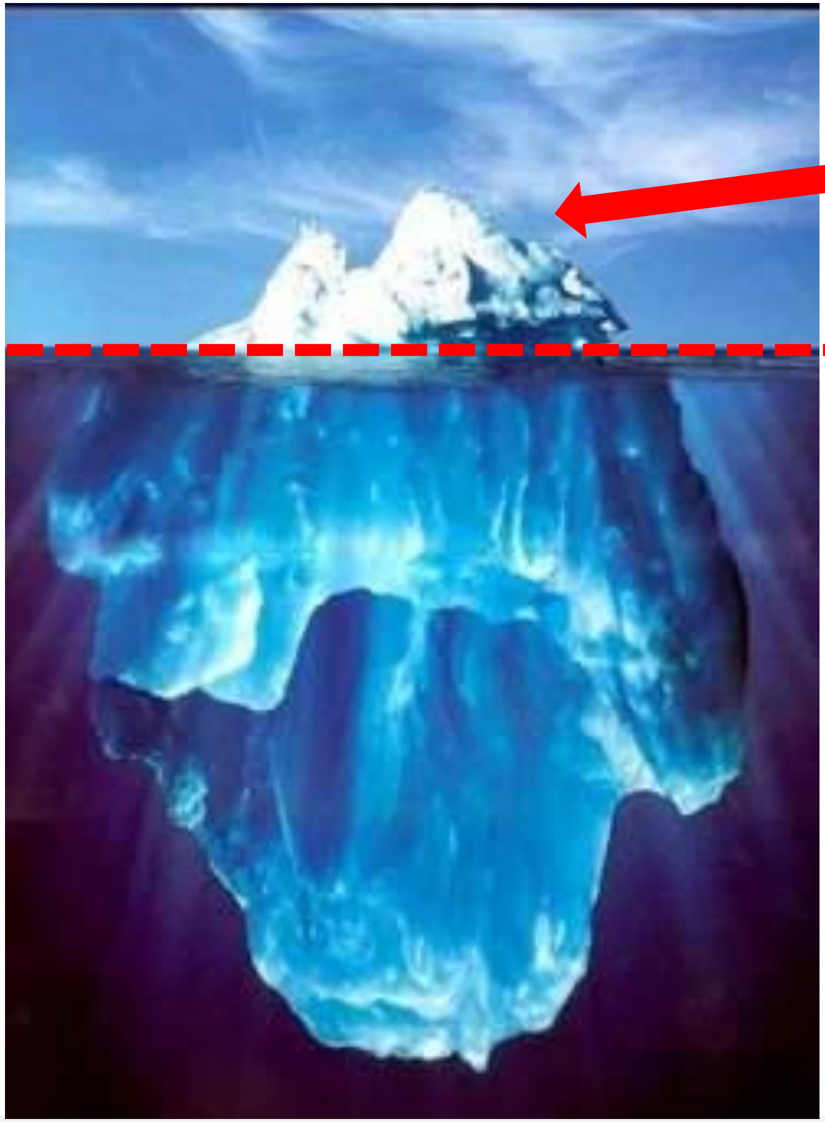
FOUNDING MEMBER SESAR

NETWORK MANAGER

EUROCONTROL

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

Context and limitations



Our dataset

No detection means (e.g. SOC)

Legal framework to share

Misuse of TLP

Lack of maturity

Company sharing culture

National regulation

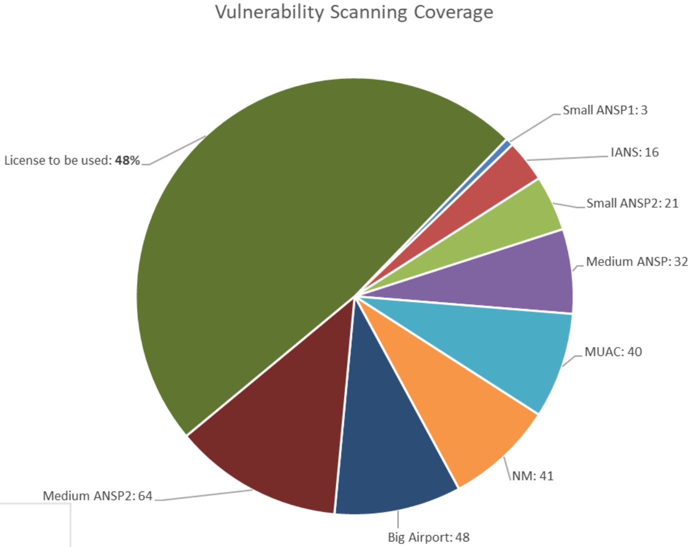
De-identification

Trust

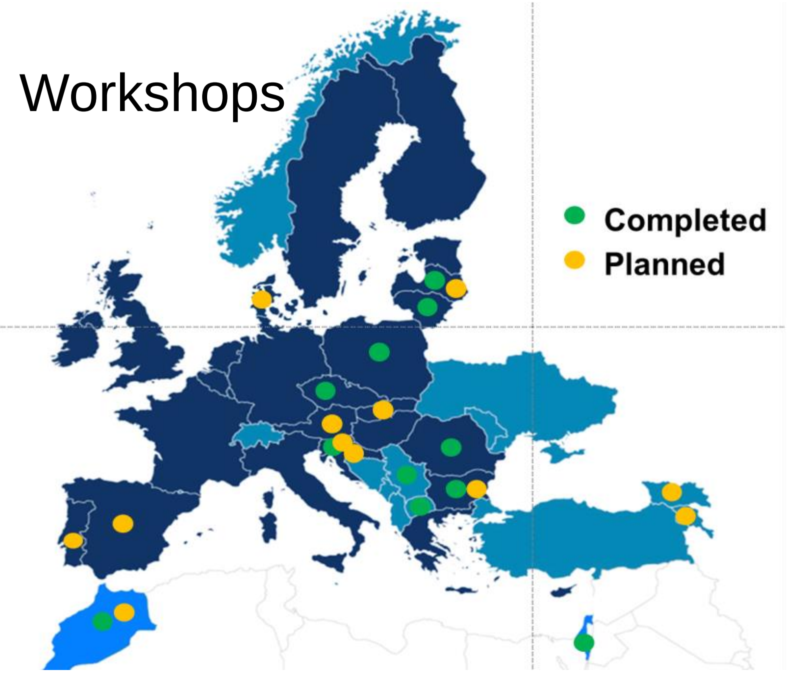
How to build trust ?

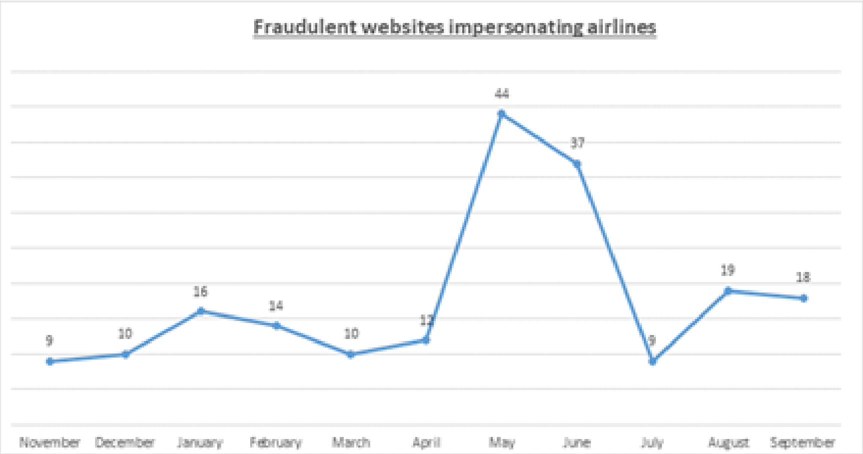
Sharing experience with constituents

EACCC - CYBER18



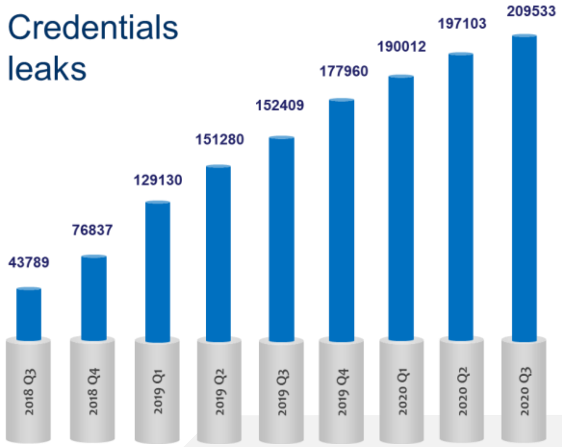
Workshops





Delivering cost-effective services

Credentials leaks



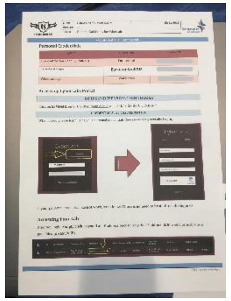
61 Constituents

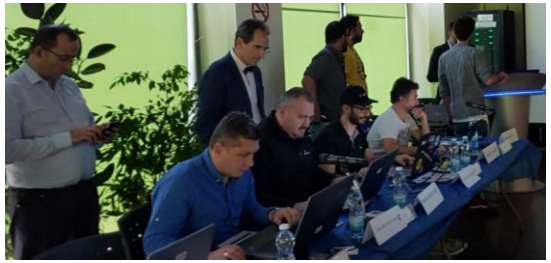
EUROCONTROL

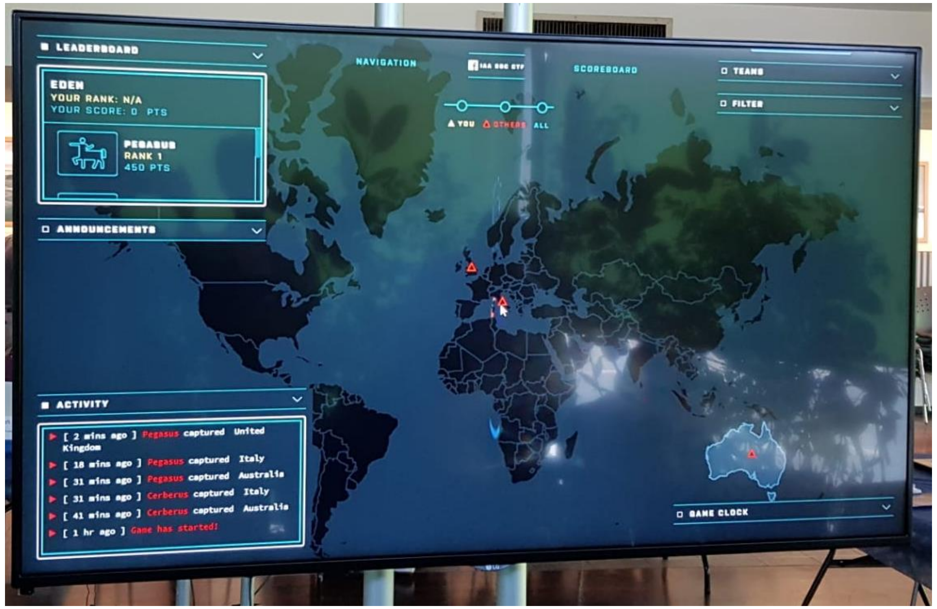
Capture The Flag

רשות שדות התעופה בישראל
ISRAEL AIRPORTS AUTHORITY

EUROCONTROL







EDEN
YOUR RANK: N/A
YOUR SCORE: 0 PTS

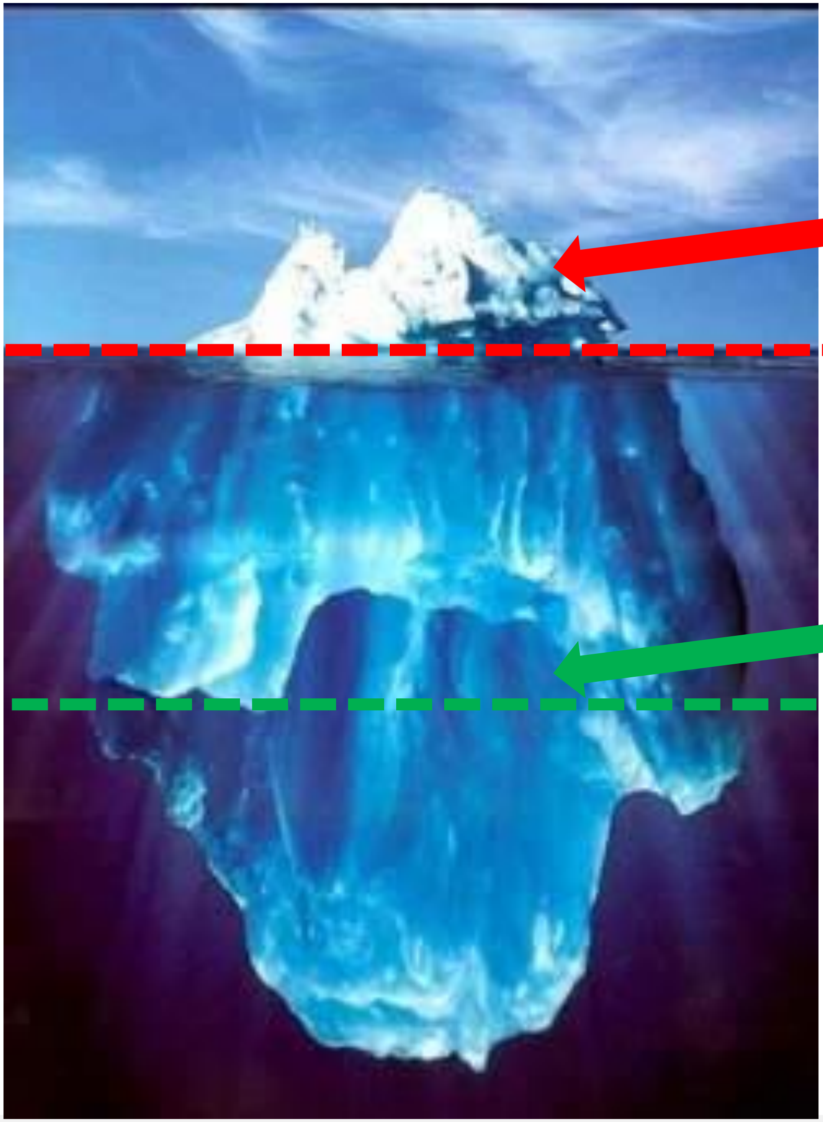
PEGASUS
RANK 1
450 PTS

```
▶ [ 2 mins ago ] Pegasus captured United Kingdom
▶ [ 18 mins ago ] Pegasus captured Italy
▶ [ 31 mins ago ] Pegasus captured Australia
▶ [ 31 mins ago ] Cerberus captured Italy
▶ [ 41 mins ago ] Cerberus captured Australia
▶ [ 1 hr ago ] Game has started!
```

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							

Call for cooperation



2020 report dataset

Thanks to you !

2021 report dataset

Aviation stakeholders
=
THE source of cyber info
… not CTI vendors

EUROCONTROL

AIR TRAFFIC MANAGEMENT CYBER SECURITY SERVICES

1

Are you hacked?

- incident response support & coordination
- artifact analysis (forensics)

2

Are you vulnerable?

- penetration testing
- red team/blue team scenarios
- security best practices review

3

Are you prepared?

- cyber threat intelligence
- log collection & intrusion detection
- alerts & warnings
- advisories & announcements
- security awareness building
- cyber security training

KEEP CALM & CALL EATM-CERT

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

THANK YOU

✉ patrick.mana@eurocontrol.int