Supporting
European
Aviation

EUROCONTROL

Cyber in aviation

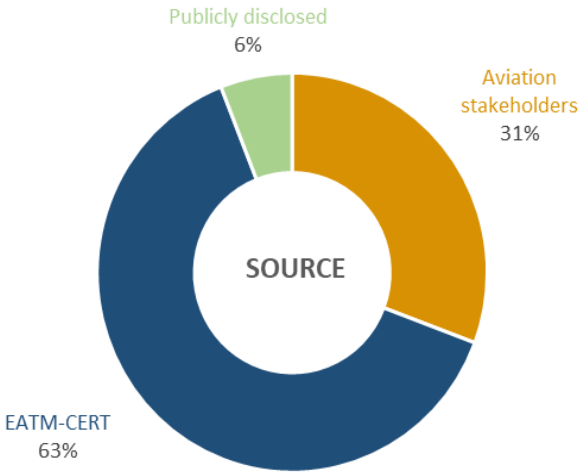
EUROCONTROL/EATM-CERT

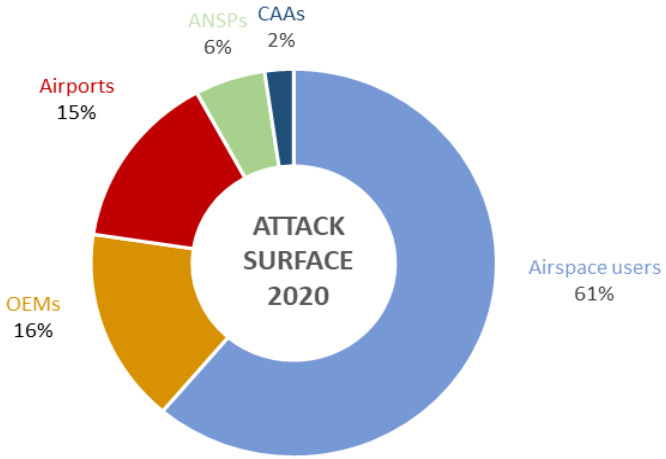
Patrick MANA
EATM-CERT Manager

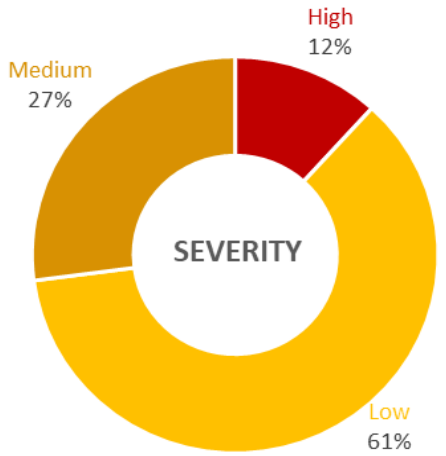
FOUNDING MEMBER SESAR JOINT UNDERTAKING

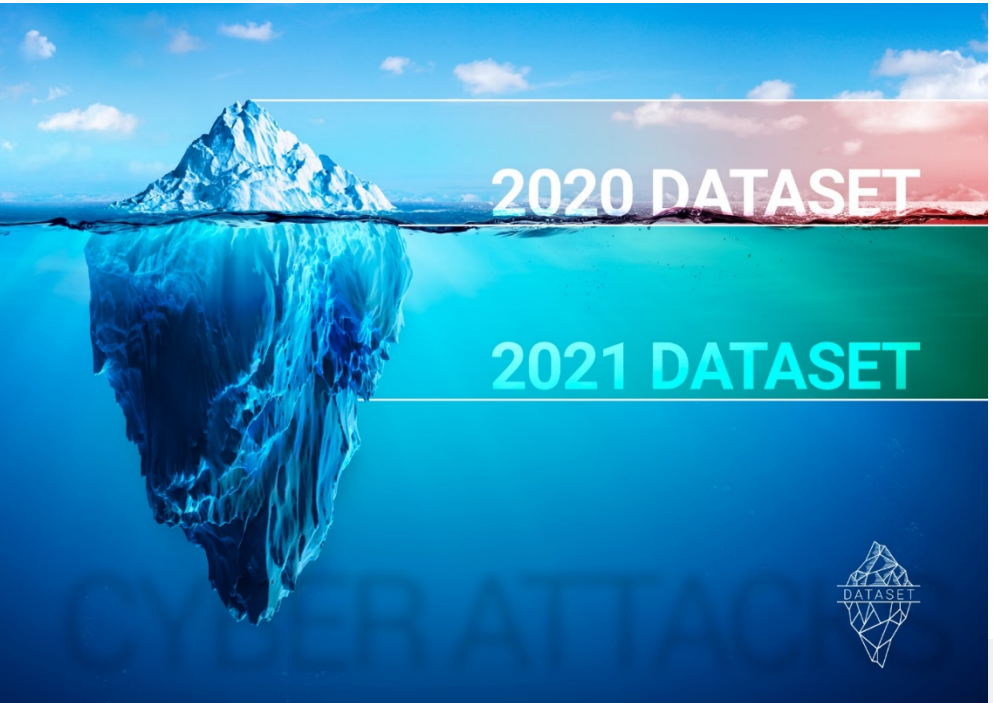
NETWORK MANAGER

EATM-CERT 2021 report on cyber in aviation









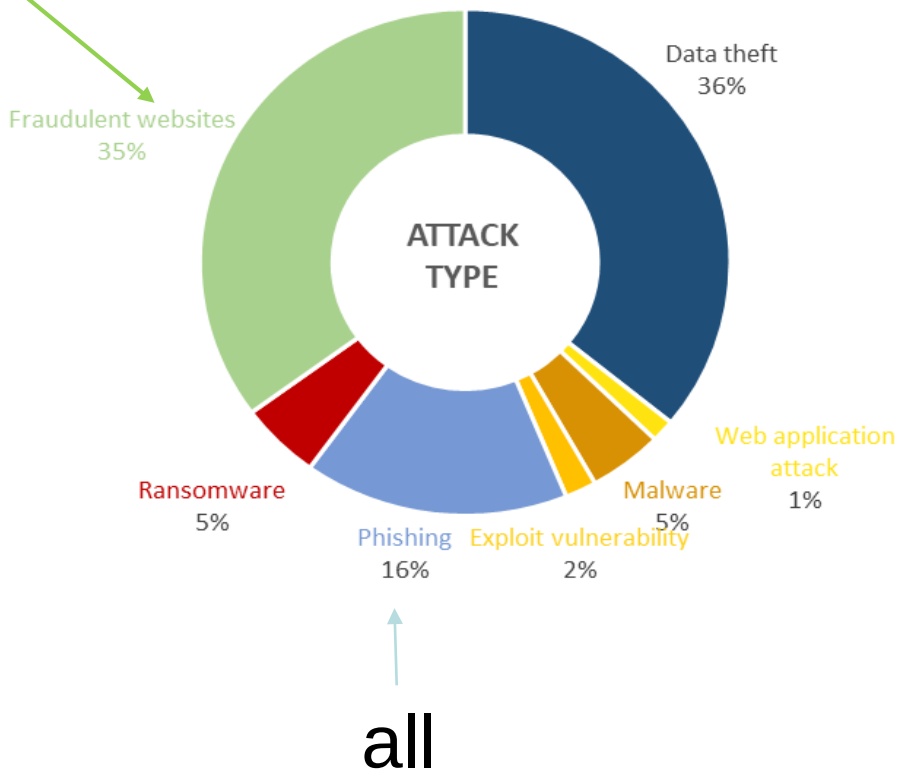
~200 events

~1.260 events

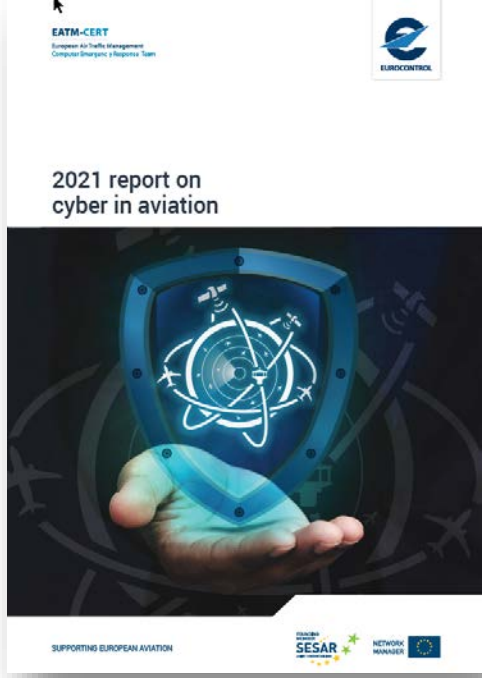
Report is TLP:GREEN

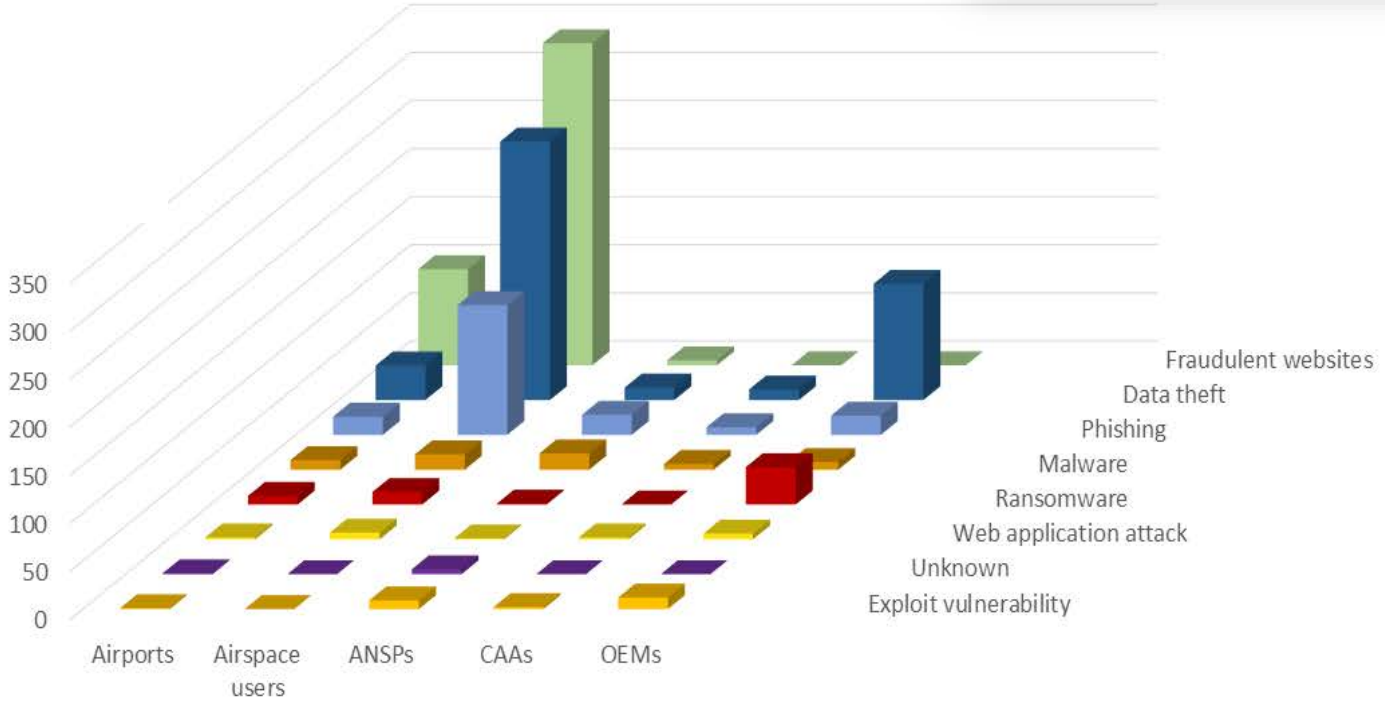
EATM-CERT 2021 report on cyber in aviation

1 Bn$/y



all



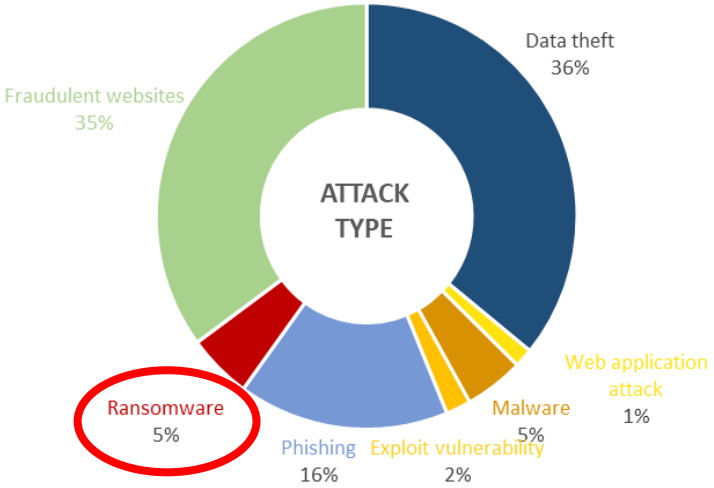


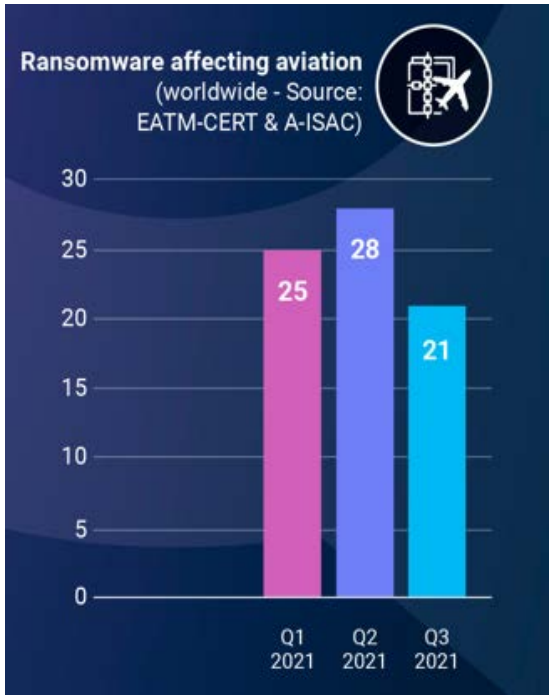
Aviation cyber threat landscape

Ransomware on aviation (global)

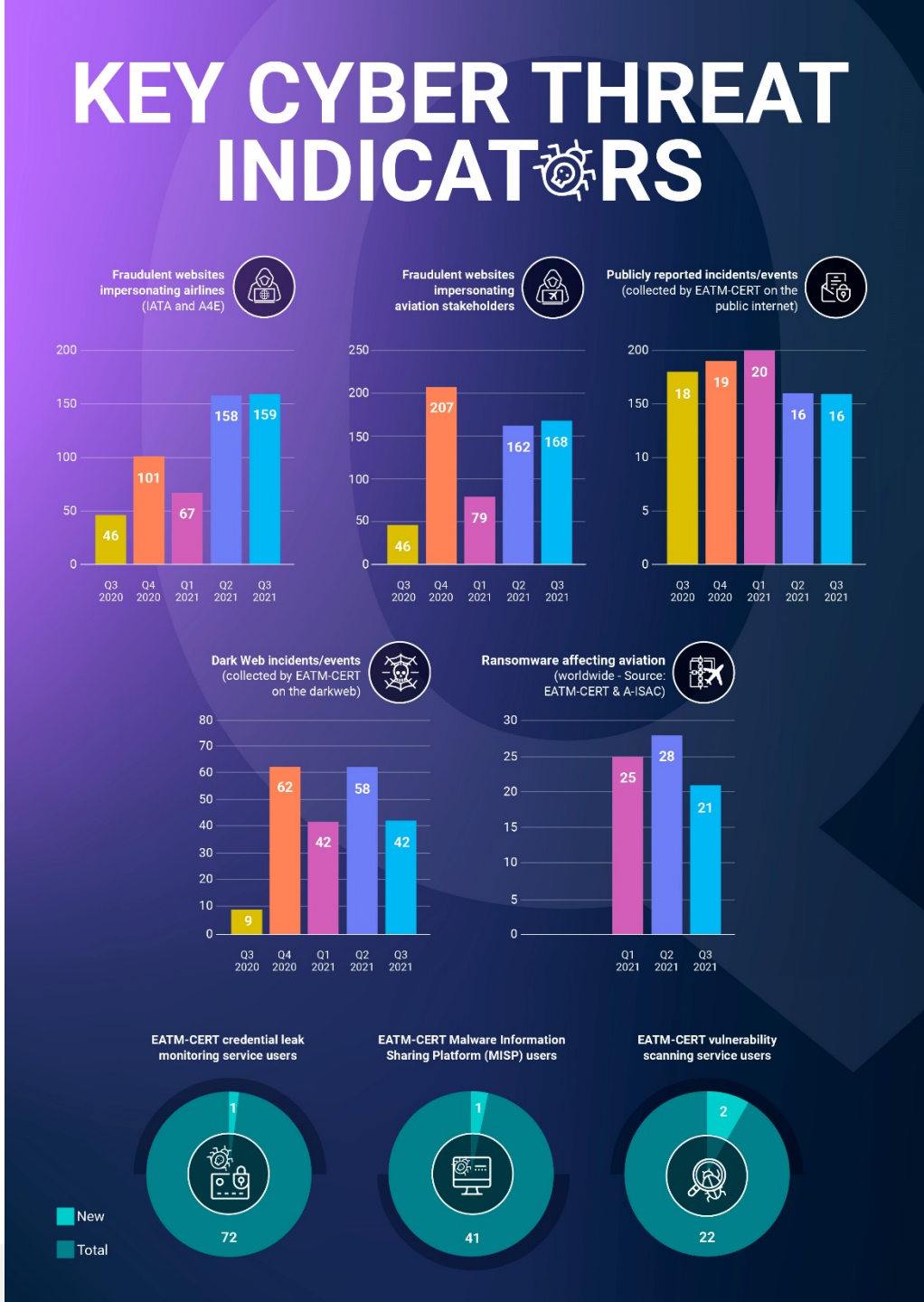
2020
One/week

2021
Two/week





Out of 1.260 events



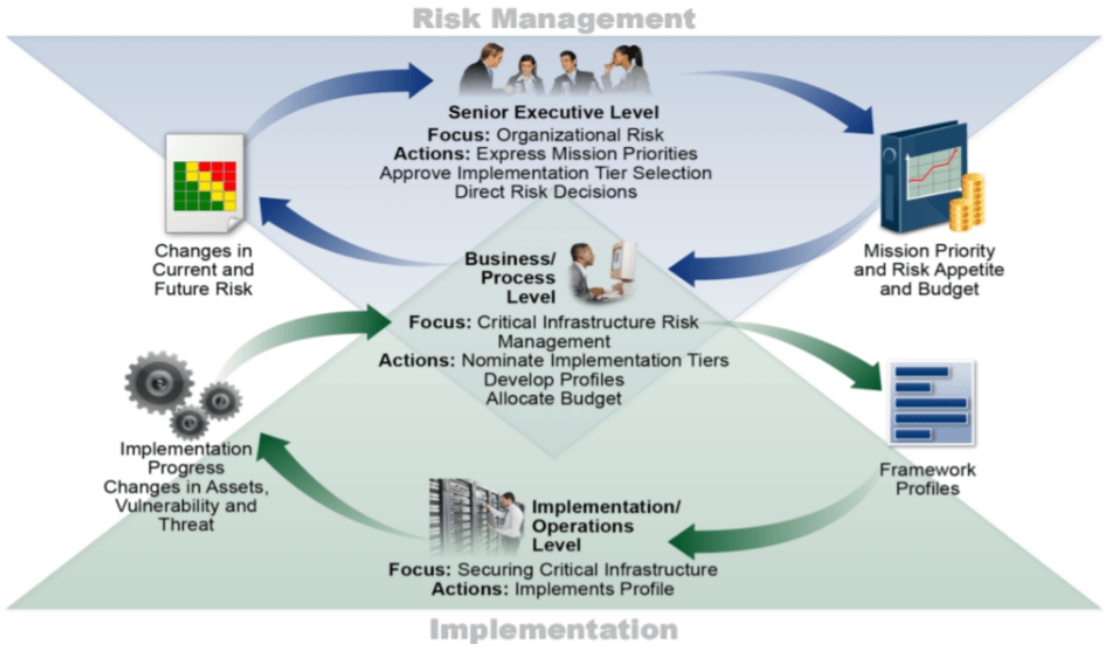
Supporting
European
Aviation

EUROCONTROL

INTEGRATED RISK MANAGEMENT

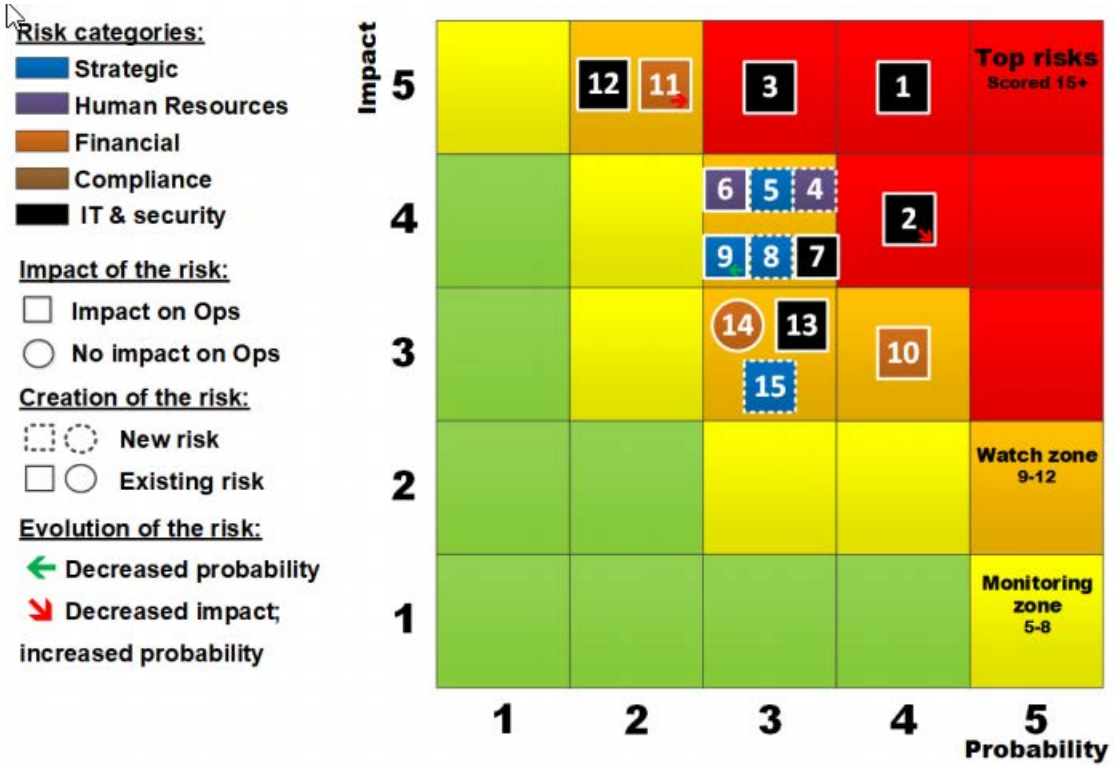
FOUNDING MEMBER SESAR JOINT UNDERTAKING

NETWORK MANAGER


Risk Management
Senior Executive Level
Focus: Organizational Risk
Actions: Express Mission Priorities
Approve Implementation Tier Selection
Direct Risk Decisions
Changes in Current and Future Risk
Mission Priority and Risk Appetite and Budget
Business/ Process Level
Focus: Critical Infrastructure Risk Management
Actions: Nominate Implementation Tiers
Develop Profiles
Allocate Budget
Framework Profiles
Implementation Progress Changes in Assets, Vulnerability and Threat
Implementation/ Operations Level
Focus: Securing Critical Infrastructure
Actions: Implements Profile
Implementation

Risk Management

EUROCONTROL

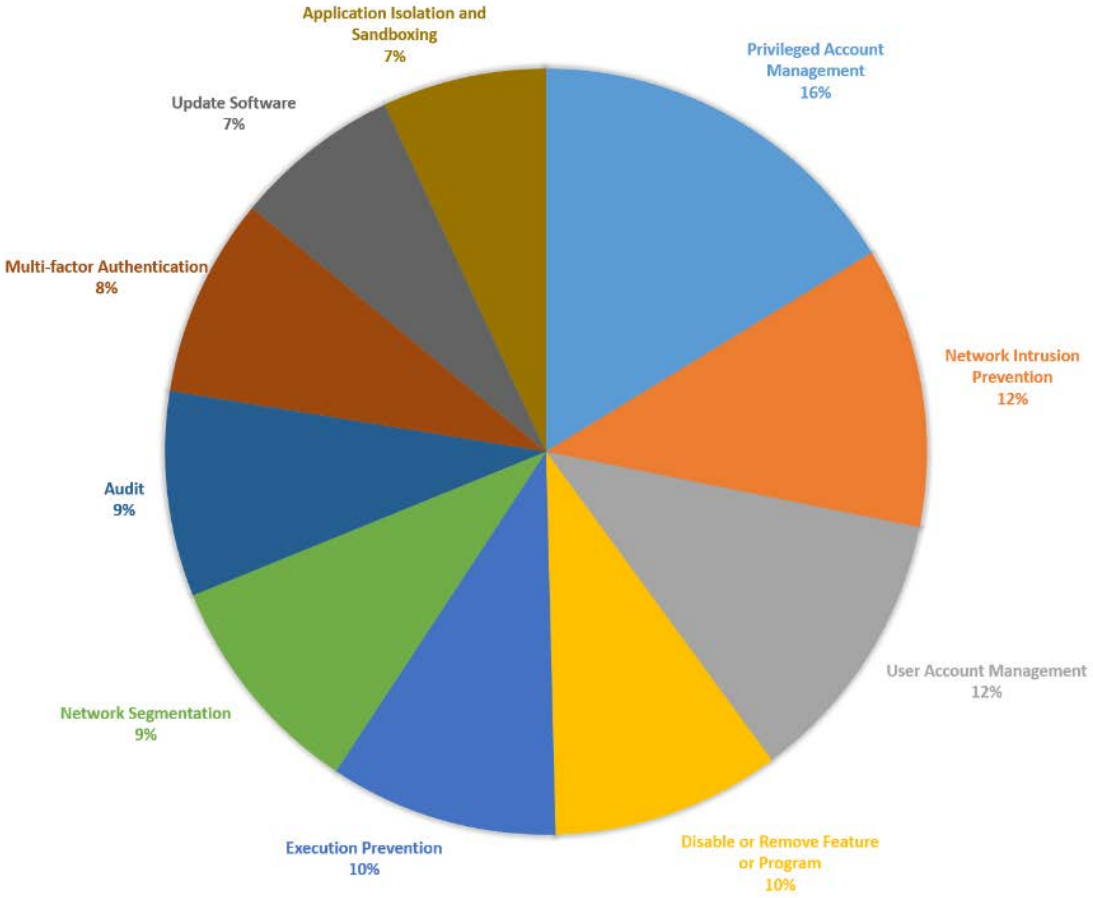


MITRE ATT&CK : Techniques most commonly used to attack aviation

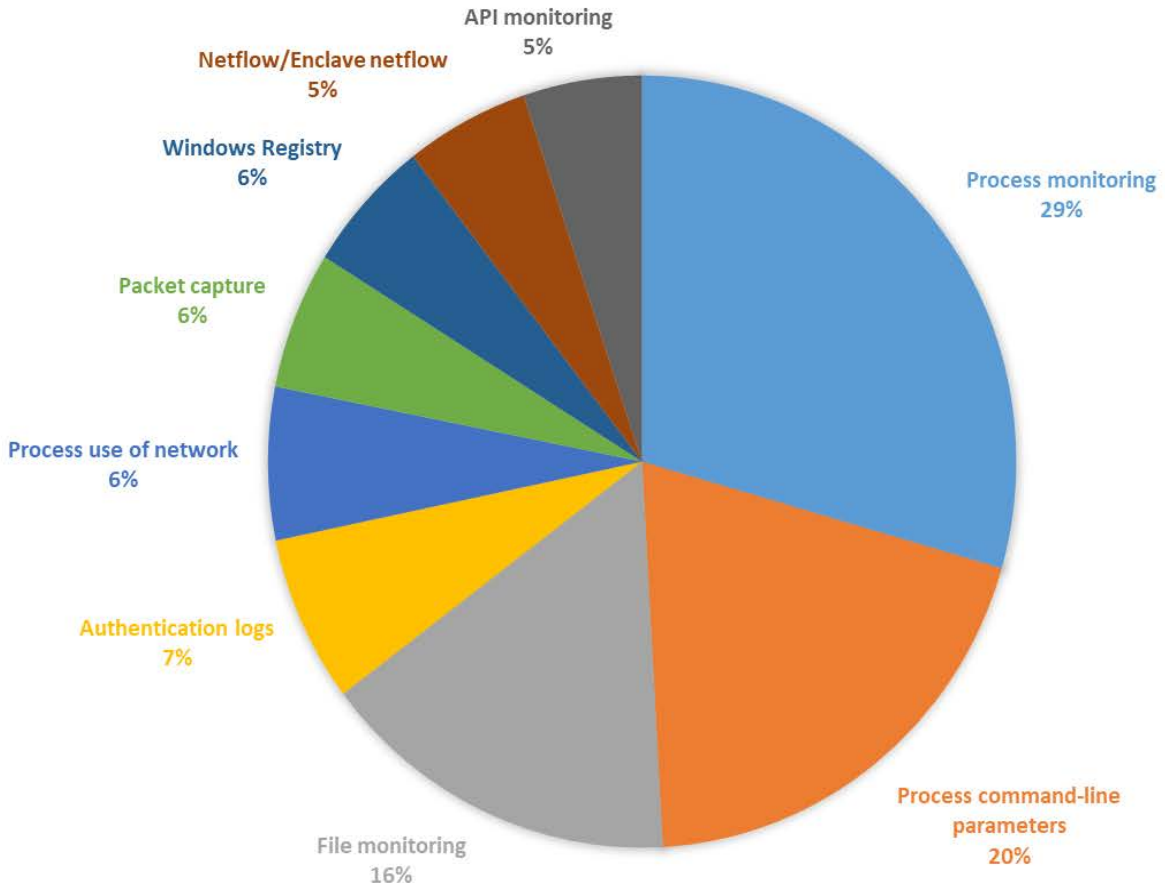
EUROCONTROL

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

Top 10 Mitigation Means



Top Detection Means



Supporting European Aviation

EUROCONTROL

TRAINING

FOUNDING MEMBER SESAR JOINT UNDERTAKING

NETWORK MANAGER

IANS Trainings

- EUROCONTROL has training facilities Luxembourg IANS
- We are planning to expand cyber security trainings with more technical ones
- We are slowly resuming training courses with physical attendance:
  - key for a topic such as cybersecurity

Available Training at IANS for ATM Security

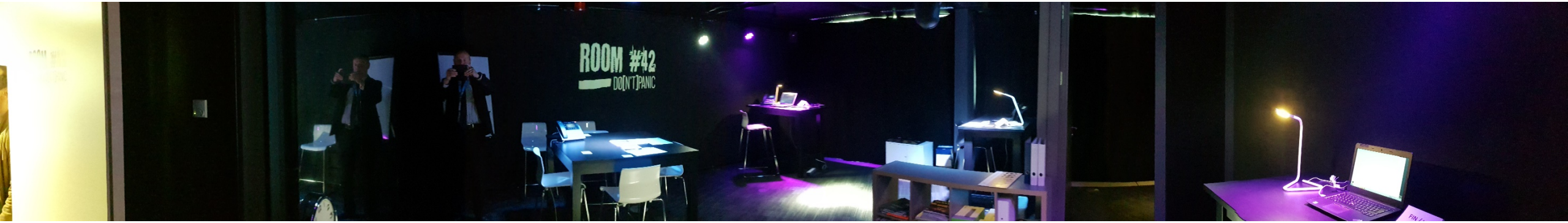
Virtual Courses		Classroom Courses	
	**Conducting an ATM Security Risk assessment [SEC-RA]**		**Oversight of Security Management Systems in ATM [LEX-CYBER]**
	**An introduction to cyber security in ATM [SEC-CYBER-INTRO]**		**Cyber security in ATM - Main threats and solutions [SEC-CYBER]**
			**Introduction to Managing Cyber Security in ATM [SEC-CYBER-MS]**
			**Cybersecurity for operational staff [SEC-CYBER-OPS]**

IANS Security Catalogue

Webinars

- 2 hours or 1h15
- Some *on invitation*: aviation, cyber, other sectors
- 2020:
  - *2020 report on cyber in aviation*
  - *SOC*
  - *Pentest*
  - *MITRE ATT&CK in aviation*
- Future:
  - *Ransomware*
  - *Social engineering*
- 2021:
  - How can we build a more cyber-resilient aviation?
  - *2021 report on cyber in aviation*
  - FlyAI – AI for cyber, cyber for AI
  - *Cyber Threat Intelligence*
  - *Vulnerability management*
  - Is aviation cyber-resilient enough?

Crisis management exercise: Room42



Crisis management exercise: Room42

EACCC CYBER 2018 EXERCICE SCENARIO

- Through getting access to a common network infrastructure and exploiting specific vulnerabilities in the surveillance infrastructure, the perpetrator manipulates the performance of the ANSP systems in a way that is not recognizable as cyber-attack.
- Air Traffic Control (ATC) centers in the directly affected States running on approximately XX% capacity reductions due to performance issues;
- Breaking News from media reports that an organization is claiming that they have cyber-attacked these centers and they will continue with attacks on all other ATC centers in Europe;
- EACCC to coordinate and share information

Directly affected states:

BULGARIA
ITALY
MONTENEGRO
SERBIA
THE NETHERLANDS

ENISA Cyber Europe exercises are **simulations of large-scale cybersecurity incidents that escalate to become cyber crises**. The exercises offer opportunities to analyze advanced technical cybersecurity incidents but also to deal with complex business continuity and crisis management situations.

THANK YOU

patrick.mana@eurocontrol.int