



ICAO

UNITING AVIATION

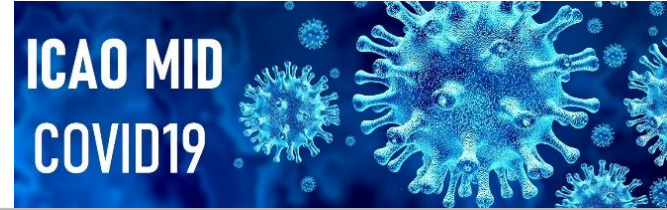
Supporting
European
Aviation



NewPENS

WELCOME TO THE **ICAO-MID - NewPENS Webinar**

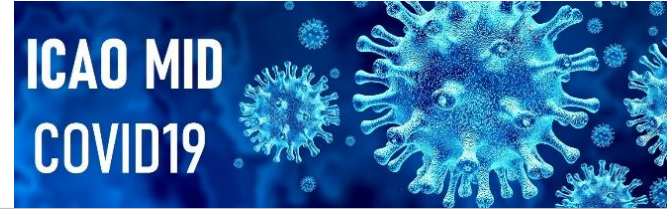
10 November 2021



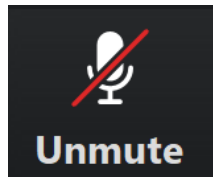
Item 1: Welcome & Introduction



Speaker: Muna Alnadaf (ICAO-MID)



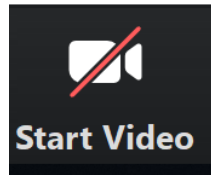
Meeting Notes



Unmute

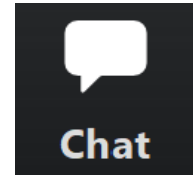
Keep Mic muted

Unmute your mic only when invited to speak



Start Video

Switch off camera if the quality of Internet is not good

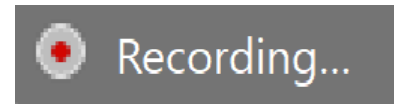


Chat

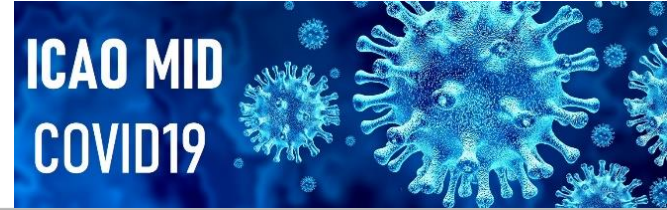


Raise Hand

use “Raise hand” or chat box if you wish address question or comment



Meeting is recorded



Group Photo




A screenshot of a Zoom meeting grid showing 63 participants. The grid is organized into rows and columns. Each tile contains a video feed of a participant, their name, and a small red 'X' icon indicating that their video is muted. The participants' names include: Sharron Caunt, Stefano Baronci, Robert Roxbrou, speed ahmed b., Amer, emasa, Youns, Mohammed Ar..., Rashad Karaky, Walid Elhoss, Mubarak Al-Ghelani, Souhail DALLEL, Gary Leung ACI, Ali Ahmed, Mohermad Hu..., Hussain Alyami, galhamadi, Ahmed Al-Jalaf..., SL Wong ACI, Mohamed Thami, Fateh Bekhti, Shayne Campbe..., Jack Netskar, A.M.R. Arjoub T..., Ahmad Amireh, nasser al-sowadi, Mohamed Chakib, Walid Rahmani, Ahmad Amireh, CANSO Nico Vo..., Haitham Misto, manal fares, Hamed Al-Abri, Ahmad Kaveh, Khaled Antar, Bander Almgbel, Mohammed Na..., faqirj, Mr MANAR, Abdul Wahab T..., Manal DIAB, Abdullah Alomair, Dr. Bader Al Sagri, radhouan aissa..., Amany Habashy, Sue Kodsi, Mashhor Alblowi, Mohammed Na..., A.M.R. Arjoub T..., Hamed Al-Abri, Ahmad Amireh, Kamal Riyadh A..., room:MD@icao.int, Sonia ElSakka, Sharron Caunt, Stefano Baronci, Robert Roxbrou, Ahmed Al-Jalaf..., Dr. Bader Al Sagri, Abdullah Alomair, Youns, Bander Almgbel, Rashad Karaky, Walid Elhoss, Mubarak Al-Ghelani, Souhail DALLEL, Gary Leung ACI, Haitham Misto, Ali Ahmed, Hussain Alyami, Mohammed Alr..., SL Wong ACI, Mohamed Thami, Fateh Bekhti, Shayne Campbe..., Jack Netskar, nasser al-sowadi, radhouan aissa..., Scott F, CANSO Nico Vo..., Haitham Misto, Hamed Al-Abri, Mashhor Alblowi, Ahmad Kaveh, Walid Rahmani, Muna ALNADAF, Khaled Antar, faqirj, Mr. MANAR, Abdul Wahab T..., Manal DIAB, Abdullah Alomair.

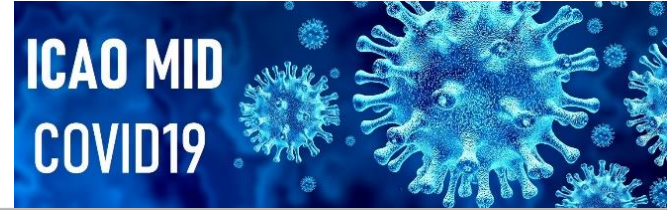
At the bottom of the grid, there is a control bar with the following icons and labels: Unmute, Stop Video, Participants (63), Chat, Share Screen, Record, Reactions, and Leave Meeting.

Wednesday, 10 November 2021

Time (UTC)	Topic	Speaker
11:00 – 11:15	Welcome & Introduction	Muna (ICAO MID)
11:15 - 12:00	NewPENS – A general introduction <ul style="list-style-type: none">✓ A common procurement agreement for managed IP transport services✓ A governance✓ A contractual framework✓ Key concepts & figures (users, geographical coverage)✓ Q&A	Nathalie Moedersheim (EUROCONTROL)
12:00 – 12:30	The NewPENS Operating Model <ul style="list-style-type: none">✓ Policies (accession handling), People (roles and responsibilities), Processes and tools✓ Q&A	Geert Pierlet (British Telecom)

Wednesday, 10 November 2021

Time (UTC)	Topic	Duration
12:30 – 12:40	Break 	
12:40 – 13:10	The NewPENS architecture ✓ an introduction to key technical concepts and work practices ✓ Q&A	Jonathan Newman (British Telecom)
13:10 – 13:40	Cyber Security & EATM CERT	Patrick Mana (EUROCONTROL)
13:40 – 14:00	Wrap-up & Closing	Nathalie Muna



Background on MID IP Network

MIDANPIRG/18 (Online, 15-22 February 2021)

The meeting noted that in spite of several coordination meetings with the CRV service provider (PCCW), the running cost of the CRV Project is very high and does not meet the objective of the project in having cost-effective solution. The meeting agreed that alternative means to establish Regional IP Network should be explored, in particular through discussion with EUROCONTROL to join the European PENS project. Accordingly, the meeting agreed to the following MIDANPIRG Conclusion:

MIDANPIRG Conclusion 18/37: Alternative Solution to Establish MID IP Network

That, the ICAO MID Office, with the support of concerned States, initiate discussions with EUROCONTROL, in order to explore the possibility of joining the PENS project as an alternative solution for establishing a MID IP Network.

Background on MID IP Network

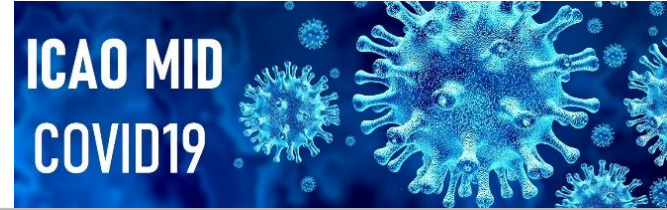
Follow-up to MIDANPIRG Conclusion 18/37

- ✓ ICAO MID Regional Office and the chairmen of CNS SG & MIDAMC STG, initiated discussions with EUROCONTROL through correspondences and virtual meeting, and it was agreed that as a first step, a list of interested States to join the New PENS would be sent to the Service Provider (British Telecom) to check the technical possibility of providing connectivity service and discuss our request with the New PENS governance body.
- ✓ Followup State letter Ref. ME 3/2.2.1 – 21/084 was sent on 2 June 2021, requesting States to confirm their interest to join the New PENS (letter of intent/agreement in principle subject to further consultation with concerned parties) and provide the ICAO MID Regional Office with the coordinates of the IP Network equipment room.

Background on MID IP Network

Follow-up to MIDANPIRG Conclusion 18/37

- ✓ 8 States confirmed their intent to join the New PENS (Bahrain, Egypt, Jordan, Lebanon, Kuwait, Oman, Saudi Arabia, and UAE).
- ✓ A NEW PENS Webinar to be conducted to inform the MID States about the technical and institutional frameworks of the IP Network Project (NEW PENS). And provide an overview of the New PENS Project operating model, architecture, governance and key concepts.



Next Speaker

Ms. Nathalie Moedersheim

Head of the PENS Management Unit - EUROCONTROL

She is an engineer in electronics and signal processing, later, she specialized in telecommunications with a focus on the development and delivery of managed network services. Nathalie joined EUROCONTROL in 2006 bringing expertise in the procurement and management of outsourcing solutions. She started collaborating on PENS as service level manager early 2010 with a primary objective to establish robust service management practices. She was appointed as Head of the PENS Management Unit in 2017 and led the transition programme from PENS to NewPENS.

ITEM 2 - NewPENS - A General Introduction

- A common procurement agreement for managed IP transport services (WAN)
- A governance
- A contractual framework
- Key concepts and figures (users, geographical scope)
- Q&As

Speaker: Nathalie Moedersheim (EUROCONTROL – PMU)

(New)PENS – The Pan-European Network Service



- (New) PENS is an international ground/ground communication infrastructure jointly implemented in 2018 by EUROCONTROL and European ANSPs
- The successor to PENS (*first generation*) – deployed in Europe in 2009

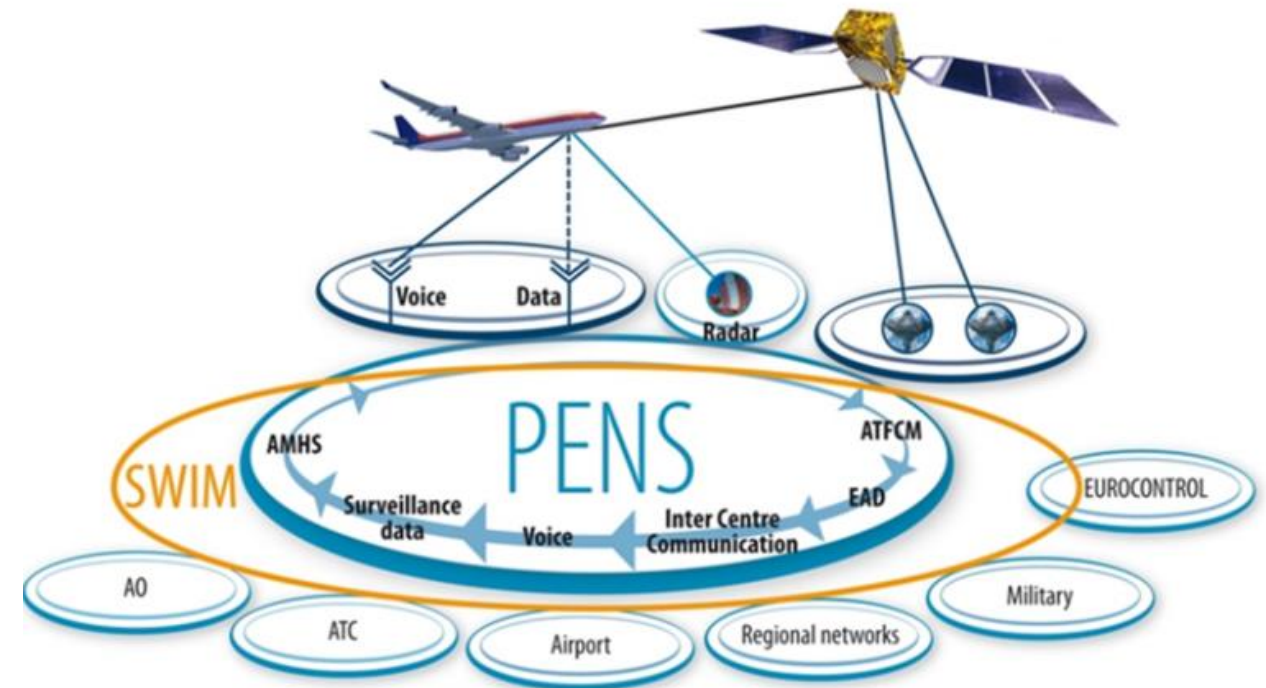


- A Pan-European collaboration framework

(New)PENS – The Pan-European Network Service

A Robust IP-transport infrastructure for exchanging critical and common ATM information, reliably, securely and safely in a cost-efficient manner

- Evolves with technology & business requirements
- Addresses a wide range of ATM Stakeholders
- Differentiated services
- Pay per Use
- Up to 99,999% availability
- Cybersecurity precautions



(New)PENS Building Blocks

Common Procurement for end-to-end managed (IP transport) network services (WAN)

Common Procurement Agreement (CPA)
= Code of Conduct, Governance & Charging Scheme



Contractual Element

NewPENS Contract with BT
Via EUROCONTROL/Direct
(Managed Services)



Contractual Element



NewPENS Governance & Collaborative Framework



Operating Model

PENS – Some History



- 2006-2007: the context
 - ✓ EUROCONTROL and a number of ANSPs understood the need and assessed the feasibility and benefits for an international IP Network Service
 - ✓ The Single European Sky (SES) was developing interoperability rules
 - ✓ New EATM services were emerging, requiring a communications network
 - ✓ The contract to provide EAD network services was expiring in June 2008
 - ✓ The contract to provide network services for NM (former CFMU) was expiring in 2009
- An **opportunity** to create a single comprehensive network to meet the needs of both EUROCONTROL and the ANSPs of the EUROCONTROL Member States
- EUROCONTROL was requested to conduct a Common Procurement on behalf of interested ANSP
- **Directive of the EUROCONTROL Permanent Commission 07/70 - 24 October 2007**

PENS – Some History



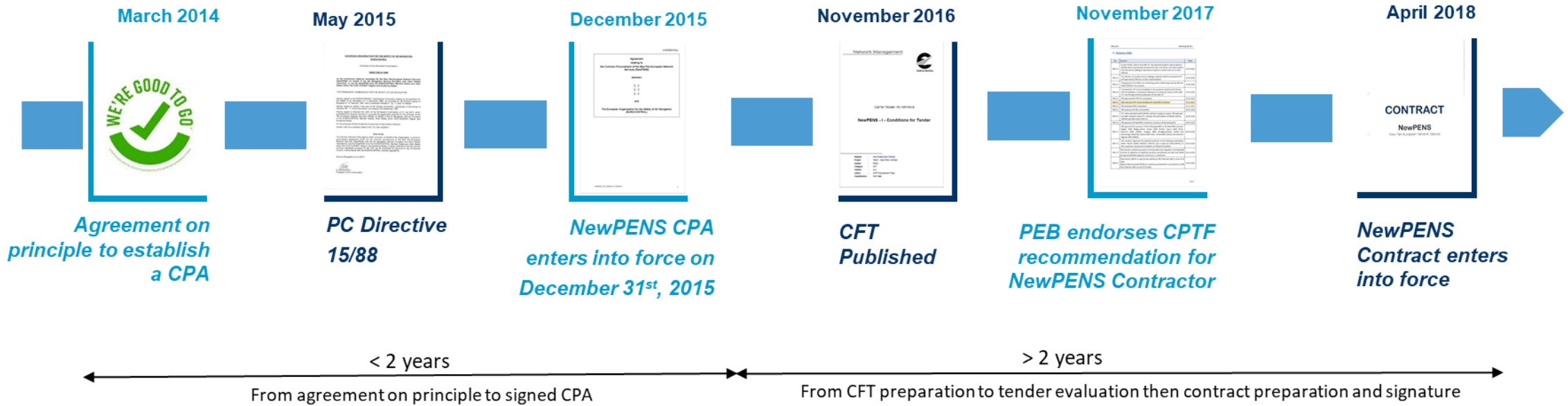
- Call for Tenders published in November 2007
- Contract awarded to SITA for 8,5 years, ending on 7 June 2018 – later extended for 2 years to accommodate the transition to the second generation contract (NewPENS)
- In May 2013
 - ✓ 17 ANSPs and EUROCONTROL have joined PENS
 - ✓ More ANSPs wanted to join and the transport of NM related data such as AFTN and EAD but also ATS messaging carrying flight information was seen beneficial
- The **geographical area for PENS needed to be extended** to other States within the ICAO EUR/NAT Region and bordering States
- **Directive of the EUROCONTROL Permanent Commission 13/81 – 12 July 2013**

Preparing for the second generation of PENS Contract (NewPENS)

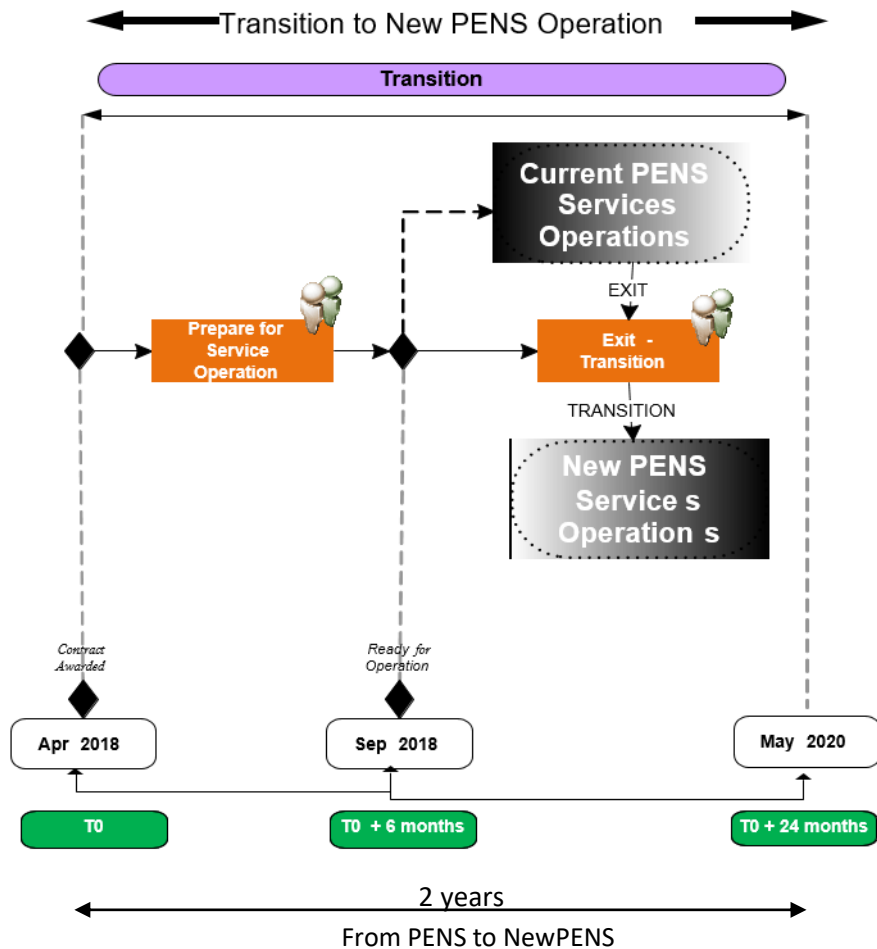


- Lessons learnt – A success story
- Multi-stakeholder governance – user driven service
- Technology Drivers for Change – NewPENS should be designed to
 - ✓ Provide true scalable multi-stakeholder support
 - ✓ Provide differentiated service levels
 - ✓ Call upon standard telco(s) feature sets
 - ✓ Provide an architecture which allows for end-to-end control & ownership
 - ✓ Build an architecture able to accommodate new and more ATM services
- Opportunity to open to the wider ATM community (civil/military ANSPs, CSPs, meteo providers, industry partners.....)

NewPENS Procurement Timeline



Transition from PENS to NewPENS



- First 6 months
 - ✓ Service management framework setup (people, process, tools) and acceptance
 - ✓ Core site deployment and acceptance
 - ✓ Infrastructure acceptance tests formalised and agreed (basic (*service providers responsibility*) and extended (*PENS User responsibility*))
 - ✓ Flow migration scenarios formalised and agreed
- NewPENS infrastructure deployment was initiated in April 2018 and completed Q1 2020
- All communications were **transparently** transferred from PENS to NewPENS in the course of June 2019-May 2020 (~200 service flows for NM/EAD, ~625 ANSP data and voice flows)

Key Figures



Geographical Scope

- ✓ 42 Countries of the ICAO EUR/NAT region and bordering countries
- ✓ 116+ Service Delivery Points (SDPs)

Service Scope

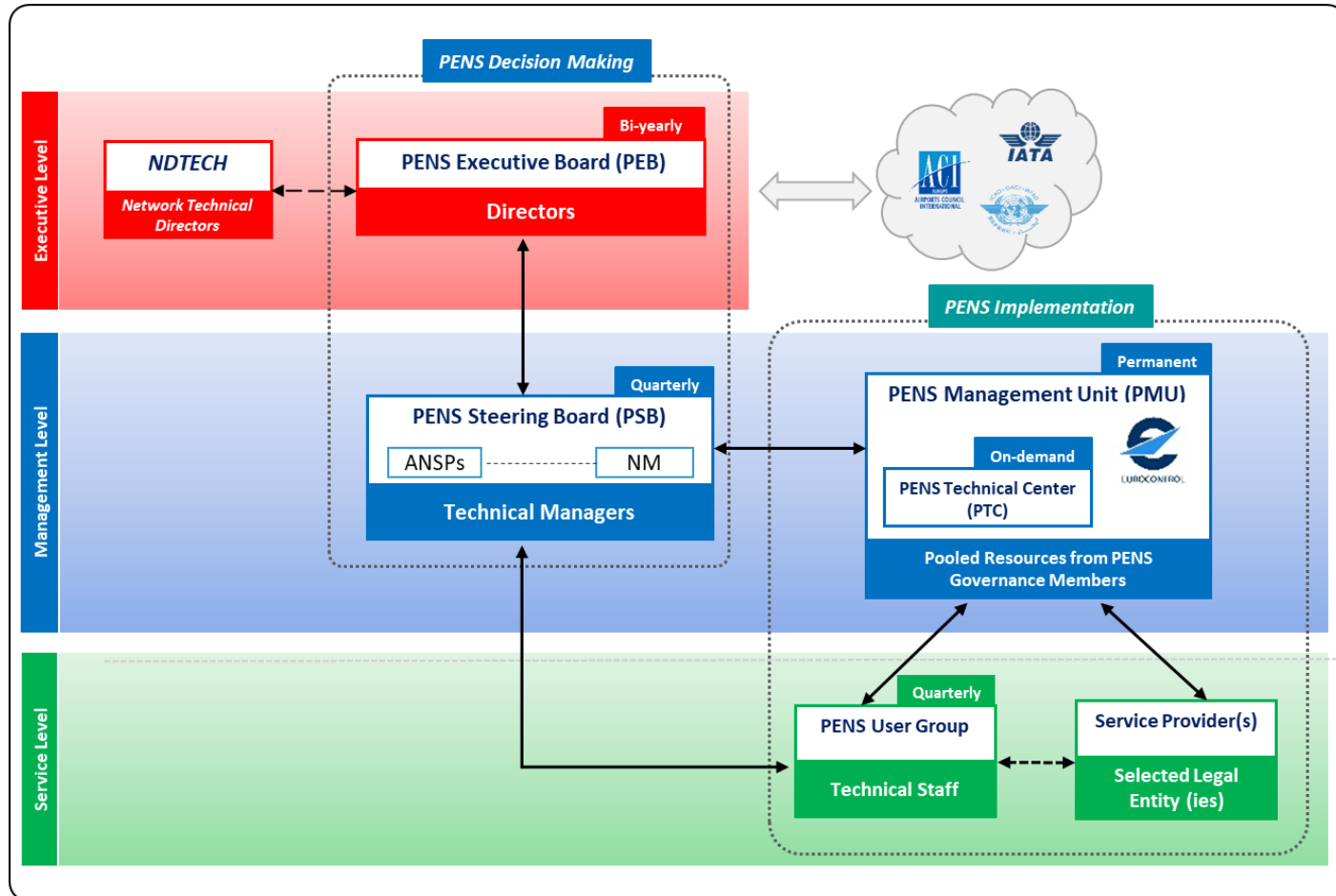
- ✓ IP data-communication (largest deployment base)
- ✓ Voice communication (development ongoing)
- ✓ Some legacy (e.g. XOT)
- ✓ Public Internet (EUROCONTROL only)

	New PENS User	Country		New PENS User	Country		New PENS User	Country
1	EUROCONTROL (NM-MUAC)		16	HCAA	Greece	31	NAV Canada	Canada
2	ALBCONTROL	Albania	17	HUNGAROCNTR	Hungary	32	NAV Portugal	Portugal
3	ANA	Luxembourg	18	ENAV	Italy	33	NAVIAIR	Denmark
4	ANS CR	Czech Republic	19	ENNA	Algeria	34	OACA	Tunisia
5	AUSTROCONTROL	Austria	20	FinTraffic ANS	Finland	35	ORO NAVIGACIJA	Lithuania
6	AVINOR	Norway	21	IAA Ireland	Ireland	36	PANSA	Poland
7	AZANS	Azerbaijan	22	IsraelIAA Israel	Israel	37	Ports of Jersey	Jersey
8	BULATSA	Bulgaria	23	ISAVIA	Iceland	38	RNLAF	The Netherlands
9	CROCONTROL	Croatia	24	LFV	Sweden	39	SKEYES	Belgium
10	DCAC	Cyprus	25	LPS SR	Slovakia	40	SKYGUIDE	Switzerland
11	DFS	Germany	26	LGS	Latvia	41	SLOVENIACNTR	Slovenia
12	DHMI	Turkey	27	LVNL	The Netherlands	42	SMATSA	Serbia and Montenegro
13	DSNA	France	28	M-NAV	Republic of North Macedonia	43	ROMATSA	Romania
14	EANS	Estonia	29	MATS	Malta			
15	ENAIRE	Spain	30	NATS	United Kingdom			

Not yet connected to Pens

(New)PENS Governance & Collaborative Framework

A User Driven Multi-Stakeholder Governance



PENS Governance & Operating Model

NewPENS Governance

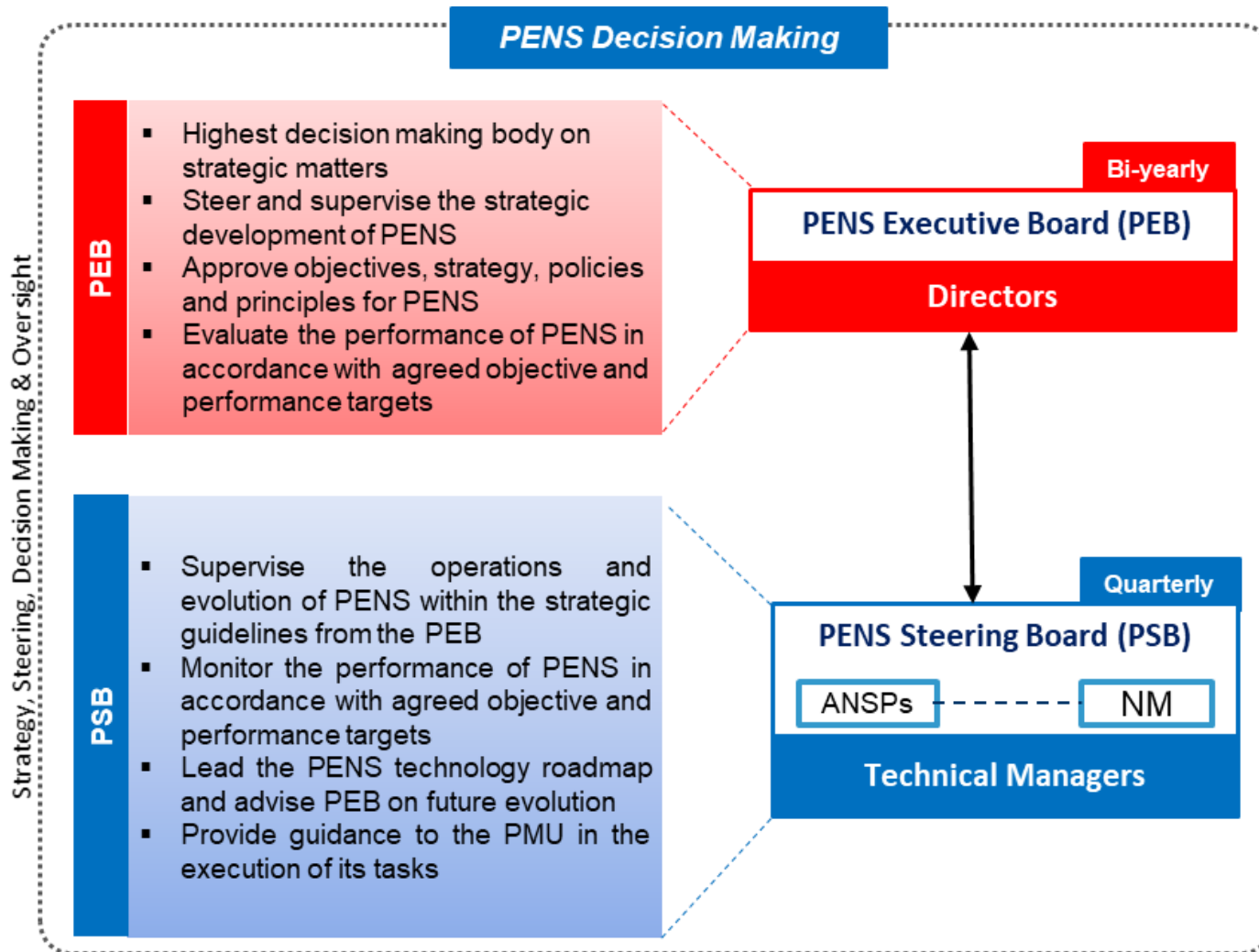
- ✓ 2 boards (PEB, PSB)
- ✓ 1 advisory body (PUG)

NewPENS Operations

- ✓ A PENS Management Unit
- ✓ A PENS Technical Centre
- ✓ A Service Provider (BT)

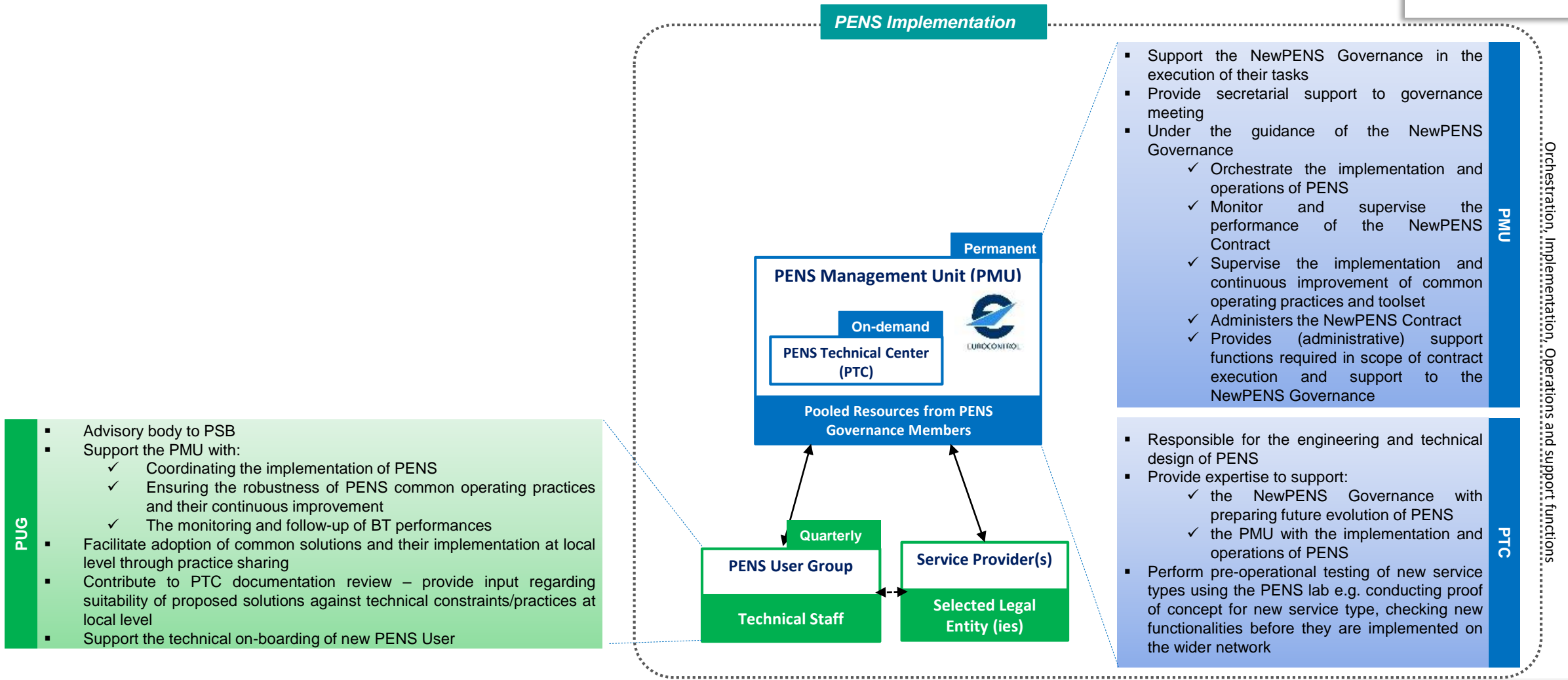
Working together with the EUROCONTROL Network Manager as part of the Collaborative Decision Making Process

PENS Decision Making



- Each board has a Chair and Vice Chair
- Decision is normally by consensus
- A voting procedure is foreseen as - exception mechanism - at the highest level
- PEB usually meets twice a year or upon request
- PSB meets on a quarterly basis

PENS Implementation (RUN)



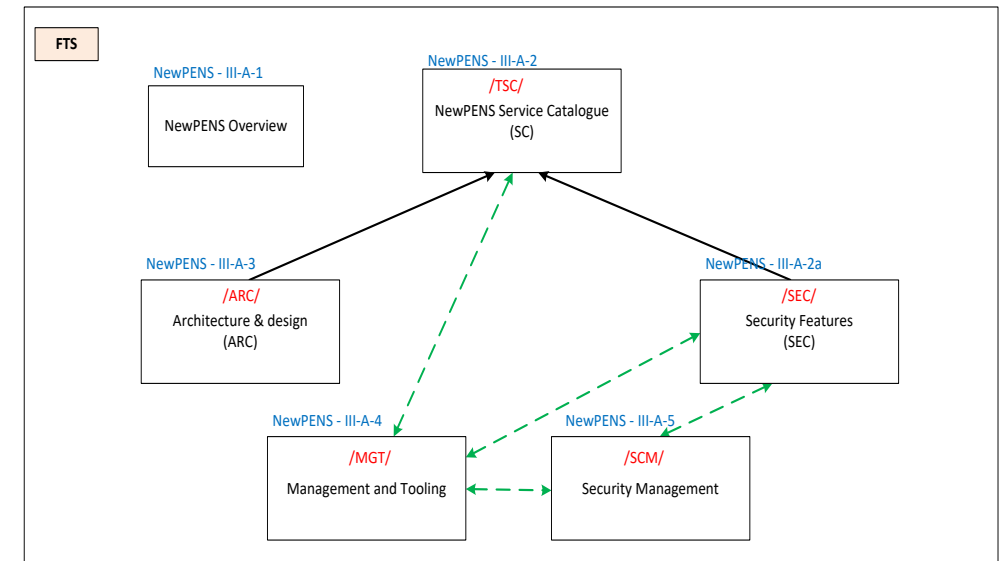
The NewPENS Contract with BT



- Awarded to BT in April 2018 as outcome to a common procurement procedure
 - ✓ Managed IP transport services (WAN)
- Maximum duration: 10 years – full lifecycle from deployment, to operations and support then exit phase including decommissioning
- The NewPENS Contract foresees:
 - ✓ Audit right on the services sourced to BT
 - ✓ Access to service level engagements between BT and their subcontractors
 - ✓ Benchmarking clause
 - ✓ Confidentiality clause
 - ✓ Central ATM aware NewPENS Service Desk
 - ✓ Extensive service management obligations
 - Support to safety provisions
 - Wide range of service levels
 - Extensive performance and monitoring tooling – document management system – workflows....
 - Comprehensive reporting (to serve as input to National Safety Authorities)

The (New)PENS Technical Service Catalogue

- The Technical Service Catalogue is at the heart of the Contract and built from:
 - ✓ Architecture and design specifications
 - ✓ Security features specifications
 - ✓ Security management specifications
 - ✓ Management and tooling specifications
- The Technical Service Catalogue offers an important number of options avoiding locked-down solutions for the future
- The Technical Service Catalogue is associated to a corresponding price lists



(New)PENS – Charging Scheme

Pay Per Use Principle



NewPENS Operating Costs (i.e. PMU & PTC)
Common to all PENS Users

Shared among all PENS users on basis of agreed Global Sharing Key (GSK)

Invoiced by EUROCONTROL

Infrastructure Costs (BT)

Service Management, tooling and NewPENS Service Desk
Common to all PENS Users (setup & recurring)

Shared among all PENS users on basis of agreed Global Sharing Key (GSK)

NewPENS Site & Features
User Specific (setup & recurring)

- User specific costs
- Site Sharing Key allows to distribute costs between users sharing common infrastructure elements

Invoiced by the Service Provider

- Circuit costs are geographically dependent
- Most cost units are common to all PENS Users (e.g. routers, VPN activation.....)

Pre-requisites to becoming a (New)PENS User

- The requesting Party must be in scope of Directive N°15/88 dated 21.5.2015 of the EUROCONTROL Permanent Commission
- Proposed Use Case(s) must be formally approved by the NewPENS Governance
 - ✓ Core principle – What is not explicitly allowed by the NewPENS Governance is prohibited
- The accession request to PENS must be formally approved by the NewPENS Governance
 - Also, from requesting Party perspective, CBA to be considered

How does one practically become a (New)PENS User



1. Pre-requisites to becoming a PENS User are fulfilled
2. Contractual/Legal
 - ✓ Become a party to (sign) the Common Procurement Agreement and,
 - ✓ Become a signatory to the NewPENS Contract with the Service Provider (by accession amendment)
3. Order your connectivity to PENS / Order your PENS site
4. The Service Provider deploys the site then hands it over to the requesting Party after successful completion of basic acceptance tests *(community defined and agreed)*
5. Optional (strongly recommended): The requesting Party has then two weeks to perform extended acceptance tests *(community defined and agreed)* before the site is formally accepted.
6. Upon formal acceptance of the site the requesting Party becomes a PENS User and is ready to establish connectivity over PENS in accordance with approved used cases.

Q&As



ITEM 2 - (New)PENS Operating Model

- (New)PENS Service Management Framework
- The Service Provider Organisation for NewPENS

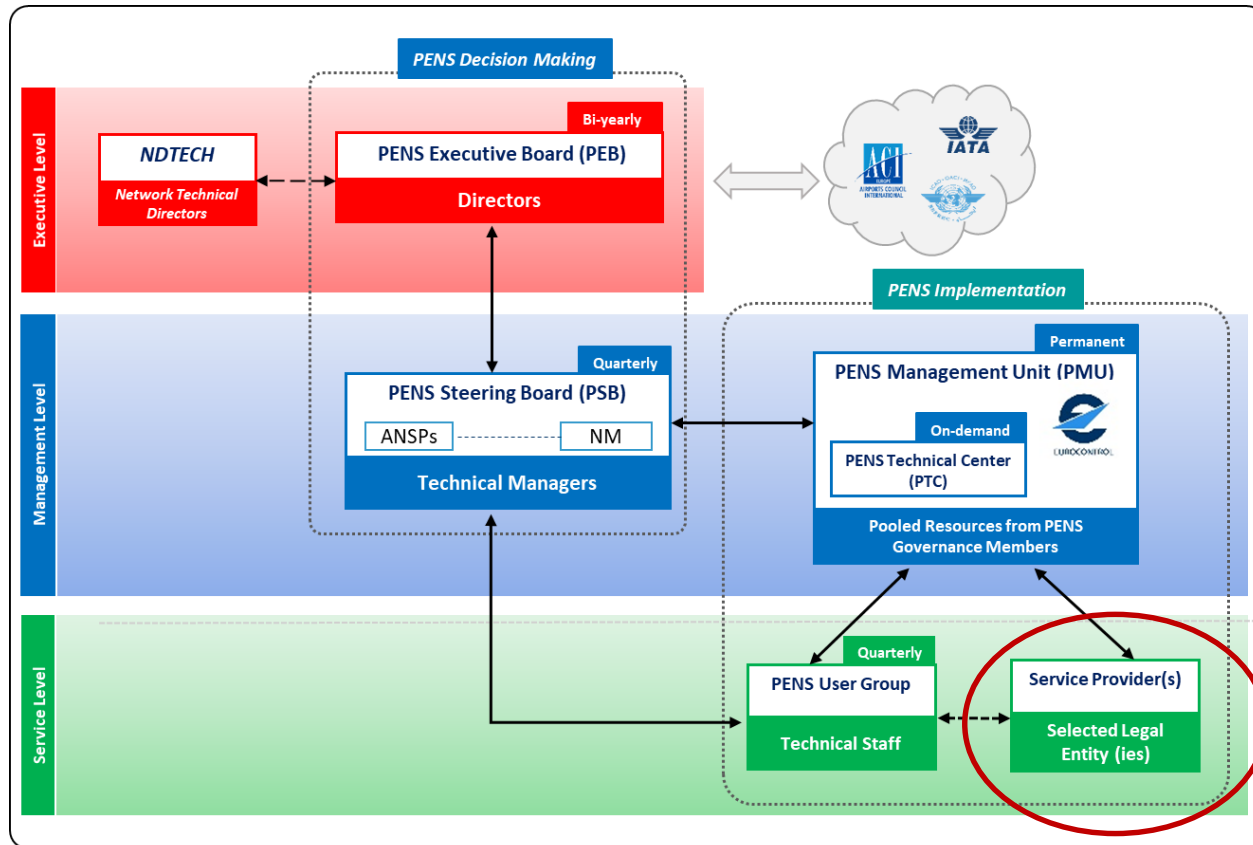
*Speakers: **Nathalie Moedersheim (EUROCONTROL – PMU)**
Geert Pierlet (BT)*

(New)PENS Service Management Framework



- To efficiently direct, manage, monitor and evolve the Pan European Network Service a comprehensive **Service Management Framework (SMF)** was put in place (*ITIL v3 based*)
- This SMF aims to provide the necessary organisational capabilities (i.e. resources, processes, functions and tools) to allow NewPENS to fulfil its business objectives and achieve the required levels of services.
- The direct benefits expected from the framework include:
 - ✓ Consistency of approach across all NewPENS users
 - ✓ Common policies and standards
 - ✓ Common service management processes, working practices and procedures
 - ✓ Operational efficiency
 - ✓ Streamlined communications between all parties involved
 - ✓ Ability to progressively achieve end-to-end service management.

Embedding Service Provider Organisation in the (New)PENS Service Management Framework



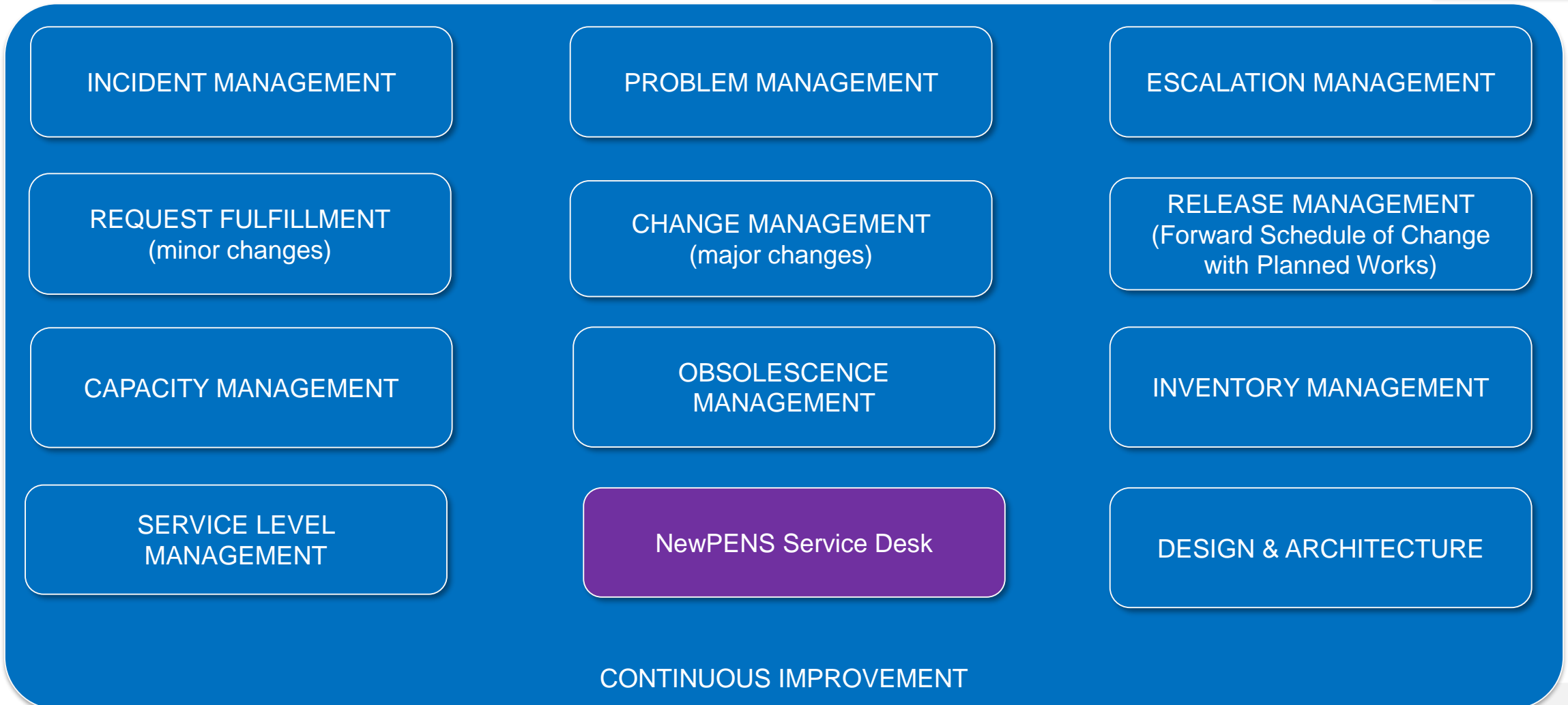
PENS Governance & Operating Model

	PEB	NewPENS Boards	PMU	Service Provider	PTC	NewPENS User
Service Strategy						
Strategy Generation	A,R	S	C			C
Service Portfolio Management	A	R	S	S		C
Demand Management	A	R	S	S		
Financial Management	A	R	S	S		I
Service Design						
Service Level Management		A	R	R,S	C	I
• Service Measurement			A	R,S	C	C
• Service Reporting			A	R,S	C	C
• Service Analysis			A	R,S	C	C
Service Catalogue Management		A	R	S	C	I
Capacity Management			A	S	R	I
Availability Management			A	S	R	I
IT Service/Business Continuity		A	A	A	R	I
Information Security Management		A	R	S	S	I
Supplier Management		A	R	S		I
Service Transition						
Change Management		C	A,R	S	C	
Service Asset and Configuration Management			A	R,S		
Release and Deployment Management			A	R,S	C	
Validation and Testing Management			A	S	R	
Transition Planning and Support		A	R	S	S	C,I
Service Operations						
Incident Management			A	R,S		C,I
Event Management			A	R,S		I
Request Fulfilment			A	R,S		C,I
Problem Management			A	S	R	C,I
Access Management			A	S	R	I
Technical Management			A	S	R	
Operations Management			A	R,S		
Service Desk Function			A	R,S		
Continuous Service Improvement						
Continuous Service Improvement		A	R	S	C	I

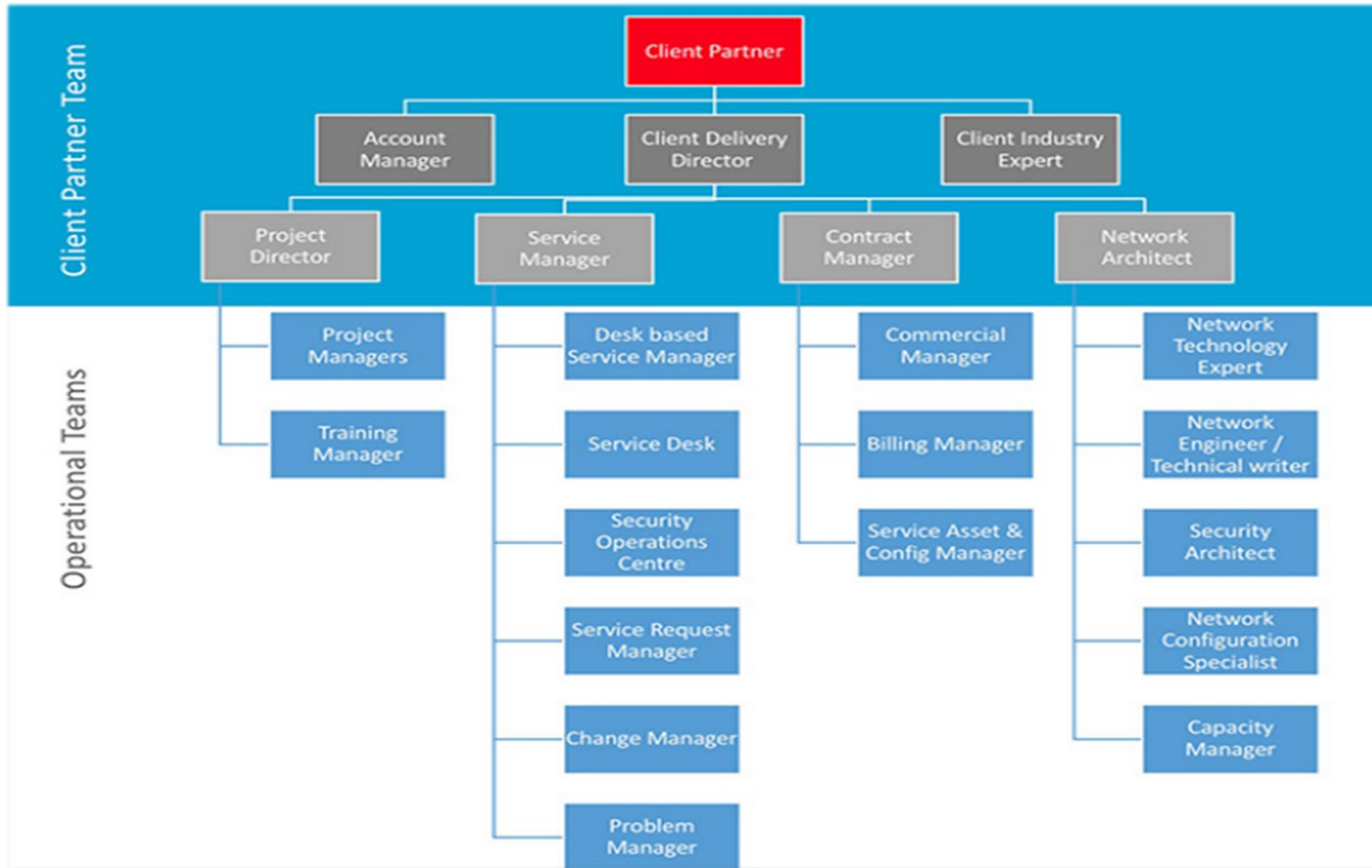
R: Responsible – A: Accountable – S: Resource Allocated – C: Consulted – I: Informed

Table 3: NewPENS Process Framework RASCI

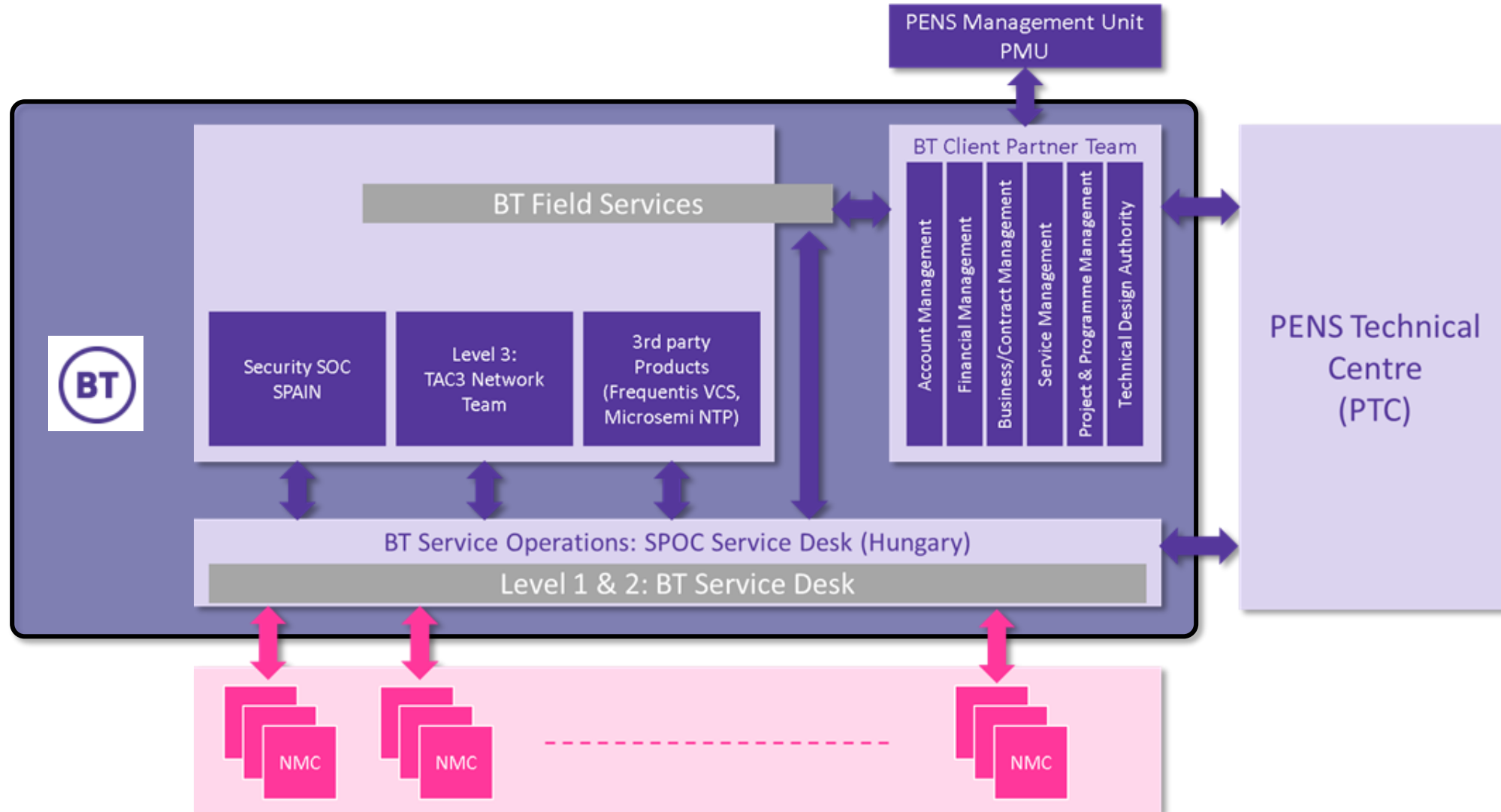
Some Key Processes and Functions



The BT Client Partner Team



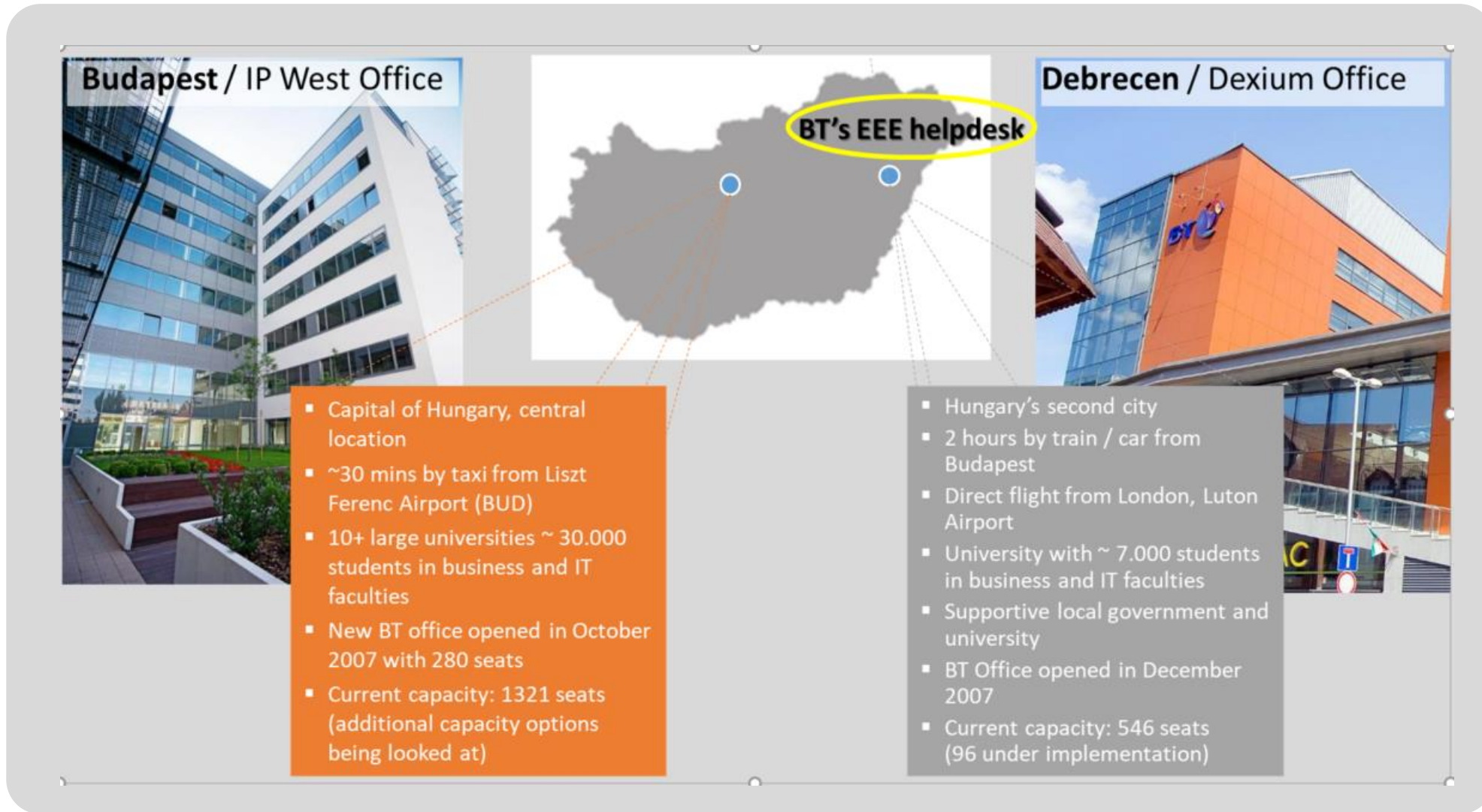
BT's Service Management Organisation for NewPENS



BT's Worldwide Support Organisation



BT's Service Desk for NewPENS



Budapest / IP West Office

- Capital of Hungary, central location
- ~30 mins by taxi from Liszt Ferenc Airport (BUD)
- 10+ large universities ~ 30.000 students in business and IT faculties
- New BT office opened in October 2007 with 280 seats
- Current capacity: 1321 seats (additional capacity options being looked at)

BT's EEE helpdesk

Debrecen / Dexium Office

- Hungary's second city
- 2 hours by train / car from Budapest
- Direct flight from London, Luton Airport
- University with ~ 7.000 students in business and IT faculties
- Supportive local government and university
- BT Office opened in December 2007
- Current capacity: 546 seats (96 under implementation)

BT's Service Desk for NewPENS

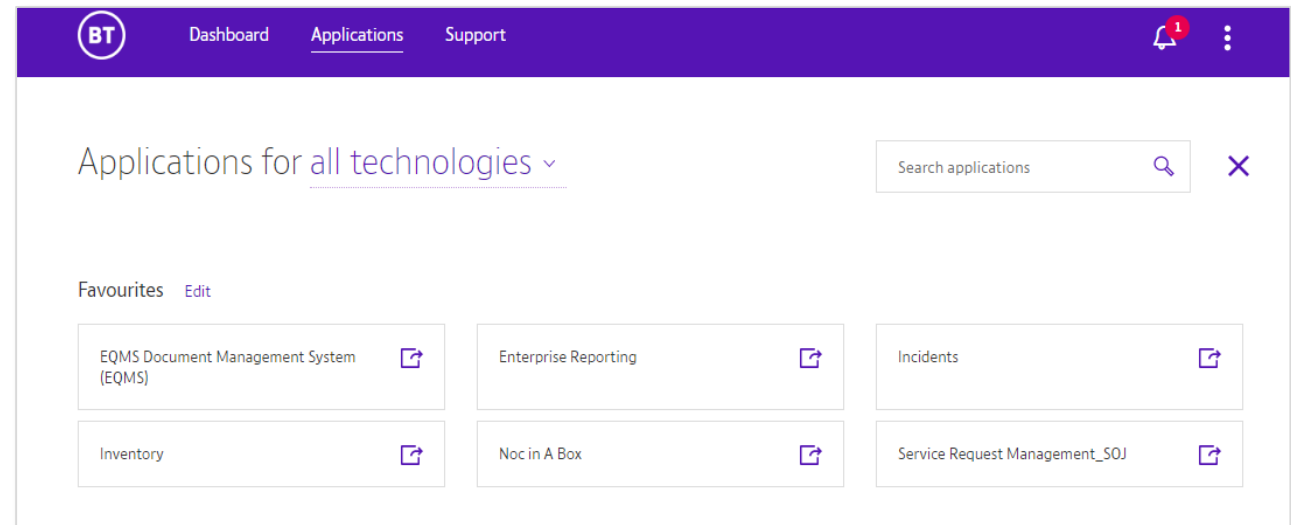


- Dedicated to a limited number of customers because of requirements on:
 - Customer's business awareness (e.g. ATM awareness)
 - Responsiveness
 - Technical & Communication skills
- Providing 7/24/365 support
 - Background: bachelor or master's degree
 - Good communication skills in English, both verbally and in writing (selection criteria)
 - Low attrition (<10%)
- Trendsetter for other BT helpdesks

Common Tooling – BT's MyAccount Portal



- PENS User interface for
 - ✓ Incident Management
 - ✓ Request Management for minor changes (Request fulfilment) and major changes (Change management)
 - ✓ Documentation Management, incl. training
 - ✓ Inventory Management
 - ✓ Network Performance Management



Common Tooling – BT's My Account Portal Incident Management Application



BT Dashboard Applications Support

Incidents > Manage incidents > Status list

+ Raise new Search

Status list

24hrs | 48hrs | 1 week | 1 month | 1 year | show all

Export Sort

Showing 1-10 of 12 < 1 2 >

Date raised	Reference	Customer/Site/Title	Status/Escalation
2021-11-10 10:00	BT-123456789	EUROCONTROL-I BT-123456789 BT-123456789	Open
2021-11-10 10:00	BT-123456789	EUROCONTROL-I BT-123456789 BT-123456789	Open
2021-11-10 10:00	BT-123456789	EUROCONTROL-I BT-123456789 BT-123456789	Open
2021-11-10 10:00	BT-123456789	EUROCONTROL-I BT-123456789 BT-123456789	Open
2021-11-10 10:00	BT-123456789	EUROCONTROL-I BT-123456789 BT-123456789	Open
2021-11-10 10:00	BT-123456789	EUROCONTROL-I BT-123456789 BT-123456789	Open
2021-11-10 10:00	BT-123456789	EUROCONTROL-I BT-123456789 BT-123456789	Open

Control Panel

- Toolkit
- Planned work
- Raise an incident
- Manage incidents

Customer: EUROCONTROL-I

Contract: All

Search by BT Reference

Search

Advanced search >

Common Tooling – BT's My Account Portal Performance Management Application



CPU Utilization (Sorted by Average, DESC)
Apr 14, 2021 14:58 to Apr 21, 2021 14:58 (UTC+00:00)

Device Name	Object Name	Indicator	Past 7 days	Past 7 days (Unsorted)	
				CPU Util (max) (max)	CPU Util (95%) (95 %tile)
...	CPU7	CPU Utilization (%)	34.85 %	35.00 %	35.00 %
...	CPU7	CPU Utilization (%)	32.90 %	33.00 %	33.00 %
...	CPU1	CPU Utilization (%)	22.00 %	24.00 %	22.00 %
...	CPU1	CPU Utilization (%)	22.00 %	23.00 %	22.00 %
...	CPU1	CPU Utilization (%)	22.00 %	23.00 %	22.00 %
...	CPU1	CPU Utilization (%)	22.00 %	23.00 %	22.00 %

Memory Utilization (Sorted By Average, DESC)
Apr 14, 2021 15:00 to Apr 21, 2021 15:00 (UTC+00:00)

Device Name	Object Name	Indicator	Past 7 days	Past 7 days (Unsorted)	
				Memory Util (max)	Memory Util (95 %tile)
...	Memory2	Memory Utilization	37.14 %	37.14 %	37.14 %
...	Memory2	Memory Utilization	37.14 %	37.14 %	37.14 %
...	Memory2	Memory Utilization	37.14 %	37.14 %	37.14 %
...	Memory2	Memory Utilization	37.14 %	37.14 %	37.14 %
...	Memory2	Memory Utilization	37.14 %	37.14 %	37.14 %
...	Memory2	Memory Utilization	37.14 %	37.14 %	37.14 %
...	Memory1	Memory Utilization	37.14 %	37.14 %	37.14 %
...	Memory1	Memory Utilization	37.14 %	37.14 %	37.14 %
...	Memory1	Memory Utilization	37.14 %	37.14 %	37.14 %
...	Memory1	Memory Utilization	37.14 %	37.14 %	37.14 %

Capacity Performance Availability

STD Most Utilized Interfaces (Inbound AVG & Bandwidth)
Apr 14, 2021 15:03 to Apr 21, 2021 15:03 (UTC+00:00)

Device Name	Object Name	Indicator	Past 7 days
...	Gi0/0/1	Inbound Utiliz...	13.47 %
...	Gi0/0/1.101	Inbound Utiliz...	13.19 %
...	Gi0/0/1	Inbound Utiliz...	13.18 %
...	Gi0/0/1.101	Inbound Utiliz...	12.91 %
...	Gi0/0/1	Inbound Utiliz...	9.06 %
...	Gi0/0/1	Inbound Utiliz...	9.00 %
...	Gi0/0/1	Inbound Utiliz...	8.89 %
...	Gi0/0/0	Inbound Utiliz...	8.71 %
...	Gi0/0/2	Inbound Utiliz...	6.73 %
...	Gi0/0/1	Inbound Utiliz...	4.16 %

STD Most Utilized Interfaces (Inbound AVG & Bandwidth) > Performance Metrics

Name	Avg	Last	T...	U...
pens-eucbfr-i-rtr01 - Gi0/0/1 - BT INTERNET t2c3.nl-ams2 XE-3/2/0 * BTM A...	9.09	8.30	9.16K	%
pens-eucbfr-i-rtr02 - Gi0/0/1 - BT INTERNET t2c3.fr-par XE-0/0/0 * BTM A-S...	9.10	3.84	9.17K	%
pens-euchbe-i-rtr01 - Gi0/0/0 - Customer LAN * BTM * - Inbound Utilization	8.99	20.44	9.06K	%
pens-euchbe-i-rtr01 - Gi0/0/1 - BT INTERNET t2c3.be-bru, XE1/0/0 * BTM A-...	9.50	16.67	9.57K	%

NewPENS Service Level Agreement

An extensive sets of Key Performance Indicators



<input type="checkbox"/> A-SDP	SDP Availability	<input type="checkbox"/> CCCL	Contract compliance with the contractual landscape
<input type="checkbox"/> A-SL	Single Line Availability	<input type="checkbox"/> BSC	Balanced Score Card
<input type="checkbox"/> A-VPNC	VPN Connection Availability	<input type="checkbox"/> RD-OT	Reports Delivered on time
<input type="checkbox"/> A-LAN	SDP LAN Availability	<input type="checkbox"/> RD-RFT	Reports Delivered Right First Time
<input type="checkbox"/> A-H2S-P	Hub to Spoke VPN Path Availability	<input type="checkbox"/> SQD-OT	Standard Quotes delivered on Time
<input type="checkbox"/> A-P2P-P	Peer to Peer VPN Path Availability	<input type="checkbox"/> SQD-RFT	Standard Quotes delivered Right First Time
<input type="checkbox"/> A-IP	SDP Internet Path Availability	<input type="checkbox"/> CQD-OT	Complex Quotes delivered on Time
<input type="checkbox"/> A-I-DNS	Internet DNS Availability	<input type="checkbox"/> CQD-RFT	Complex Quotes delivered Right First Time
<input type="checkbox"/> PL-VPNC	VPN Connection Packet Loss	<input type="checkbox"/> CR-OT	Change Requests Completed on Time
<input type="checkbox"/> J-VPNC	VPN Connection Jitter	<input type="checkbox"/> CR-RFT	Change Requests Completed Right First Time
<input type="checkbox"/> NRT-VPNC	VPN Connection Network Response Time	<input type="checkbox"/> SR-OT	Service Requests Completed on Time
<input type="checkbox"/> NL-P2P	Network Latency for Point-to-Point Connections	<input type="checkbox"/> PEW-OT	Planned Engineering Work Announced on Time
<input type="checkbox"/> NJ-P2P2	Network Jitter for Point-to-Point Connections	<input type="checkbox"/> MTAC	Maximum Time to Answer a Call
<input type="checkbox"/> NFL-P2P	Network Frame Loss for Point-to-Point Connections	<input type="checkbox"/> NCDI	Number of Configuration Database Inconsistencies
<input type="checkbox"/> NRT-IC	Internet Connection Response Time	<input type="checkbox"/> NMC-USI	NMC User satisfaction index
<input type="checkbox"/> ANRT-CHMI	Application Network Response Time for CHMI	<input type="checkbox"/> ERUD	Exit repository is kept-up to date
<input type="checkbox"/> OABF-SC	Observed Access Beta Factor - Single Core	<input type="checkbox"/> YNEI	Yearly Number of Errors in the Invoices
<input type="checkbox"/> OABF-DC	Observed Access Beta Factor - Dual Core		
<input type="checkbox"/> RCT-VPNC	VPN Connection Re-Convergence Time		
<input type="checkbox"/> MTRC-NS	Network Services Maximum Time to Recover		
<input type="checkbox"/> MTRP-NS	Network Services Maximum Time to Repair		

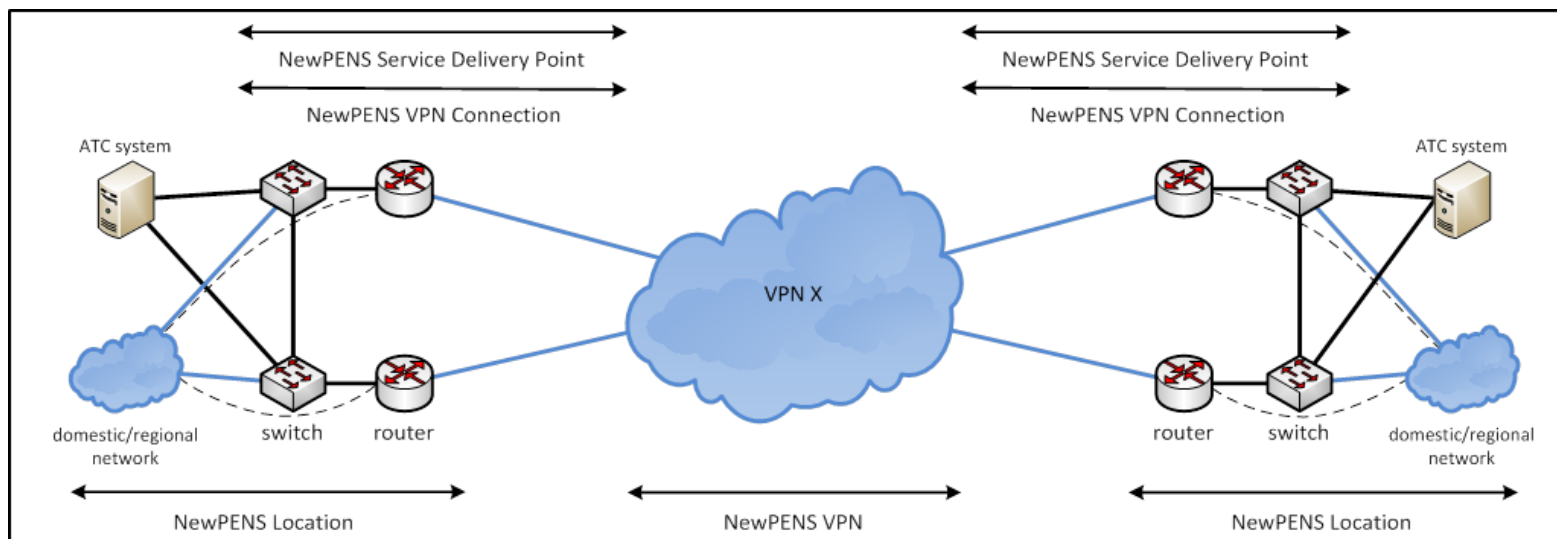
ITEM 3 - (New)PENS ARCHITECTURE

- An introduction to key technical concepts and work practices
 - Q&As
- EATM Network and Cybersecurity
 - Q&As

Speaker: Jonathan Newman (BT)

(New)PENS Architecture – Key Concepts

- **(New)PENS SDP** (*Service Delivery Point*)
 - ✓ One or more network devices that provide one or more (New)PENS User(s) with a connection to (New)PENS
- **(New)PENS Location**
 - ✓ The physical premises in which one or more (New)PENS SDPs are located
- **(New)PENS VPN**
 - ✓ Separates traffic flows and routing information from one-another on a shared network infrastructure
- **(New)PENS VPN Connection**
 - ✓ Is a connection from a (New)PENS SDP to a (New)PENS VPN

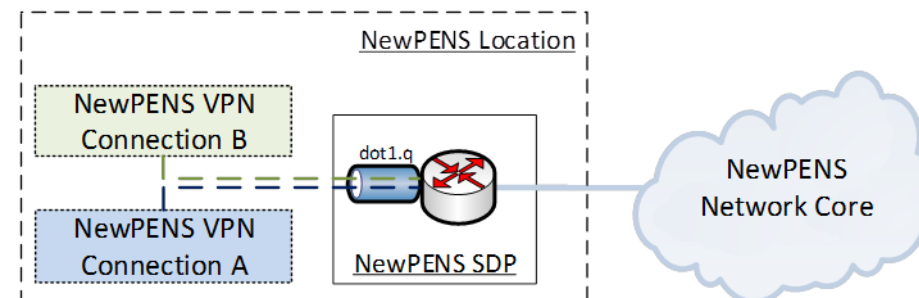
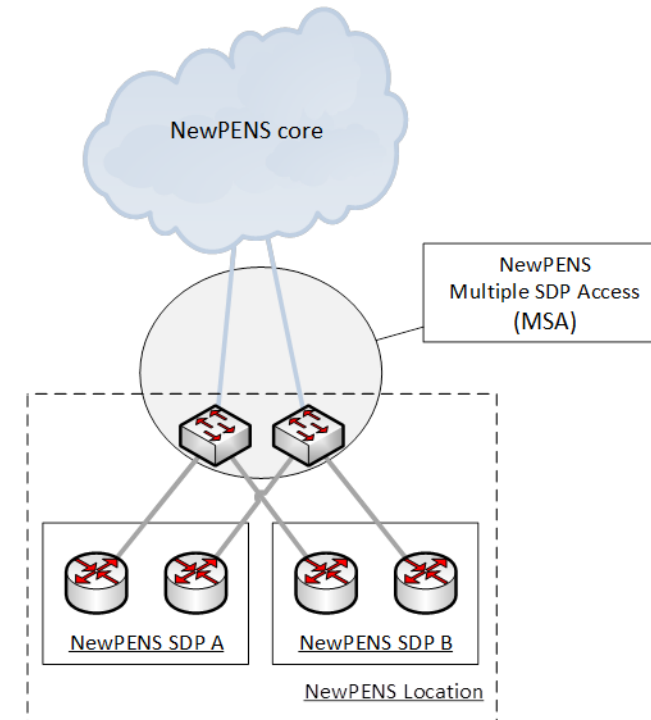
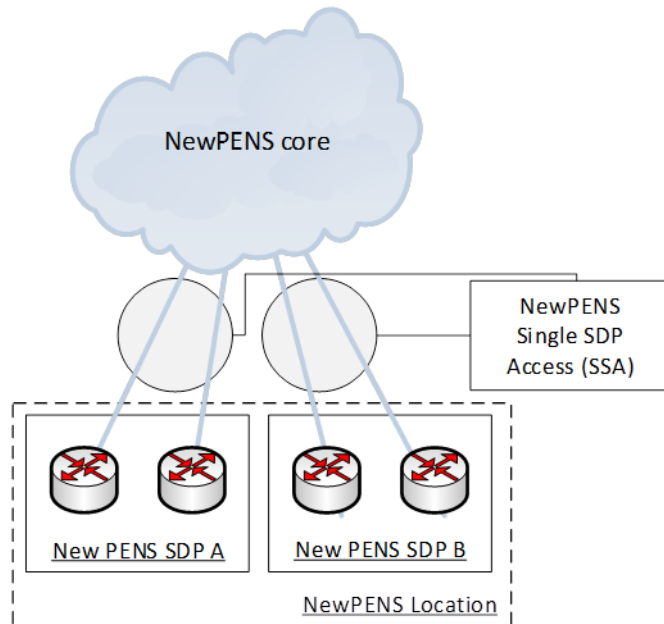


(New)PENS Architecture – Key Concepts

■ Sharing of Network Resources

(physical or logical e.g.):

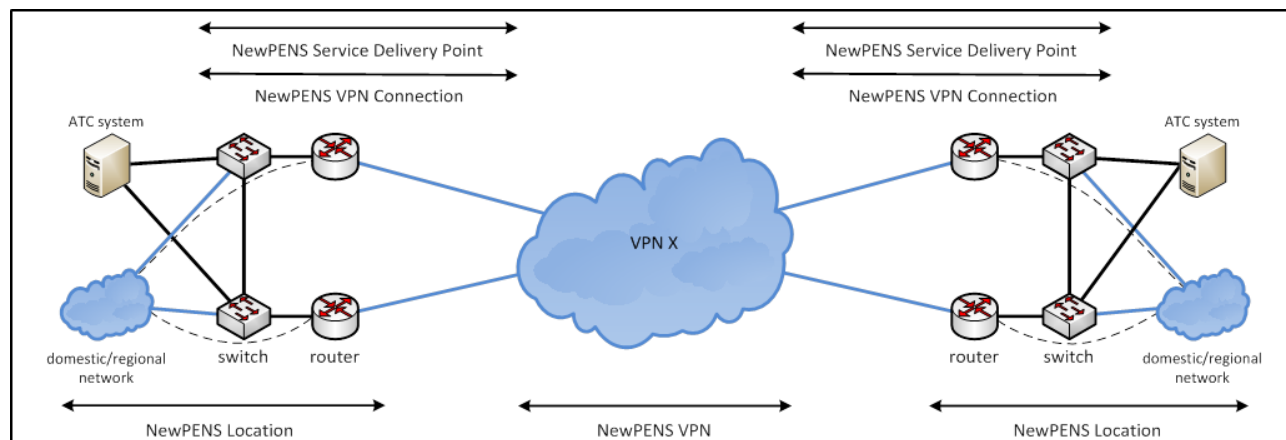
- ✓ (New)PENS VPNs
- ✓ (New)PENS SDPs
- ✓ Access circuits to a (New)PENS Location
- ✓ CPE LAN Interfaces within a SDP



(New)PENS Architecture – Key Concepts

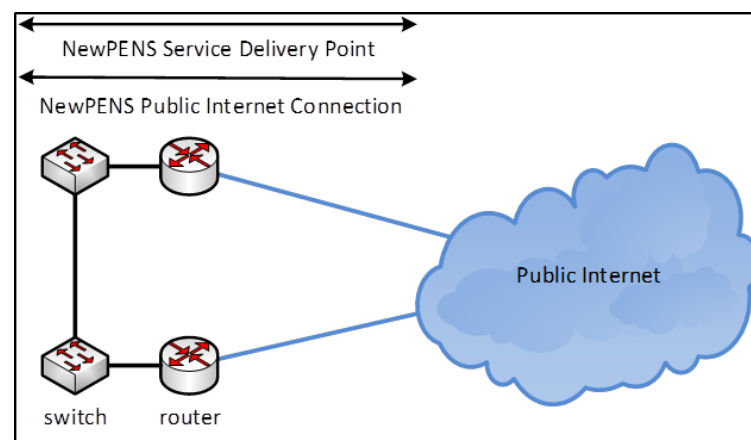
Private vs. Public Network Services

- ✓ Service offerings separately orderable via the (New)PENS Technical Service Catalogue



Private Network

- ✓ provided through MPLS IPVPN-like services or secure tunnelling over Internet

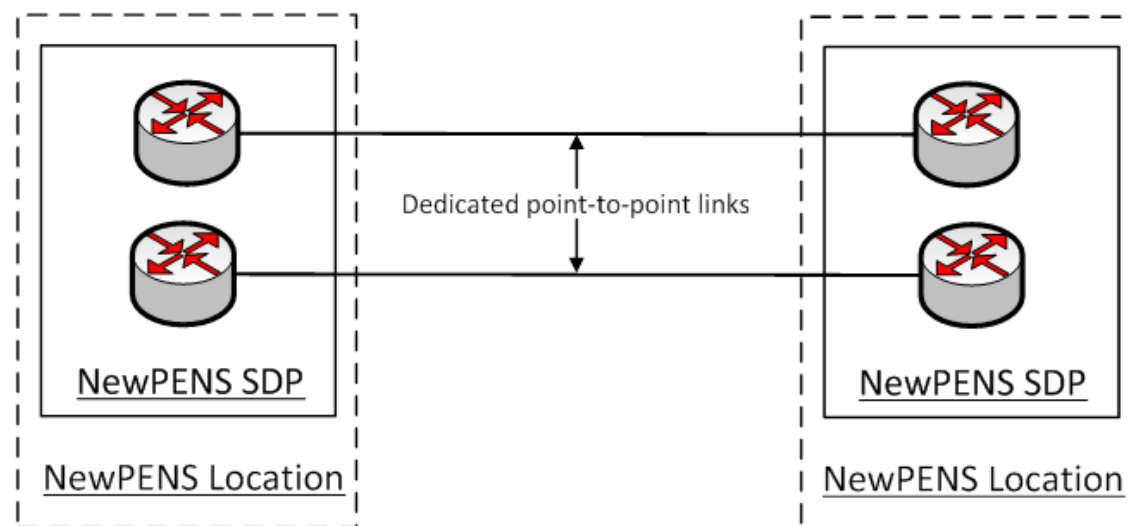


Public Network

- ✓ public Internet access service

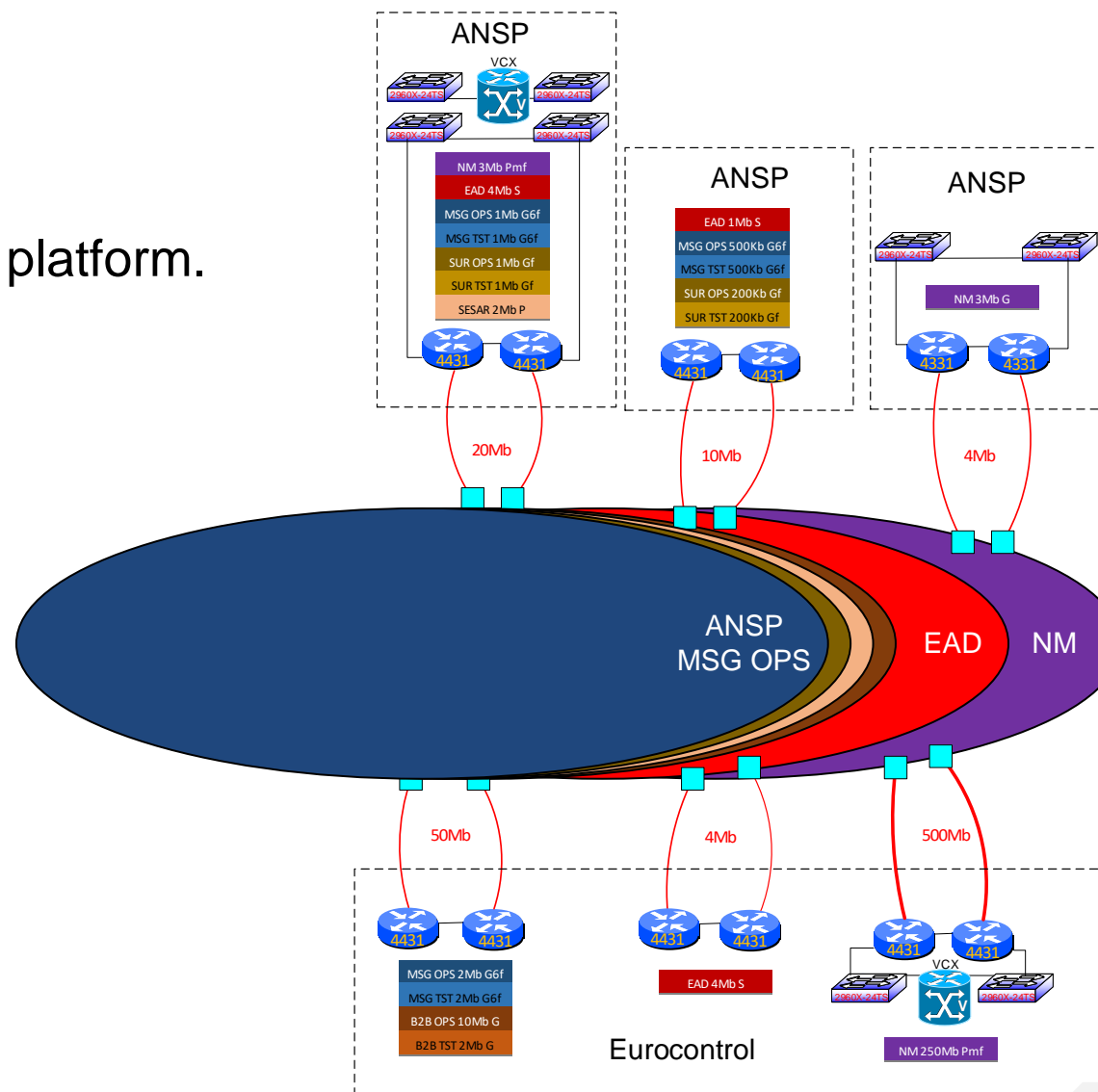
(New)PENS Architecture – Dedicated Point-to-Point Connection

- Point-to-point links between 2 NewPENS SDP's in separate locations
- Guaranteed end-to-end bandwidth
- MPLS technology is not allowed



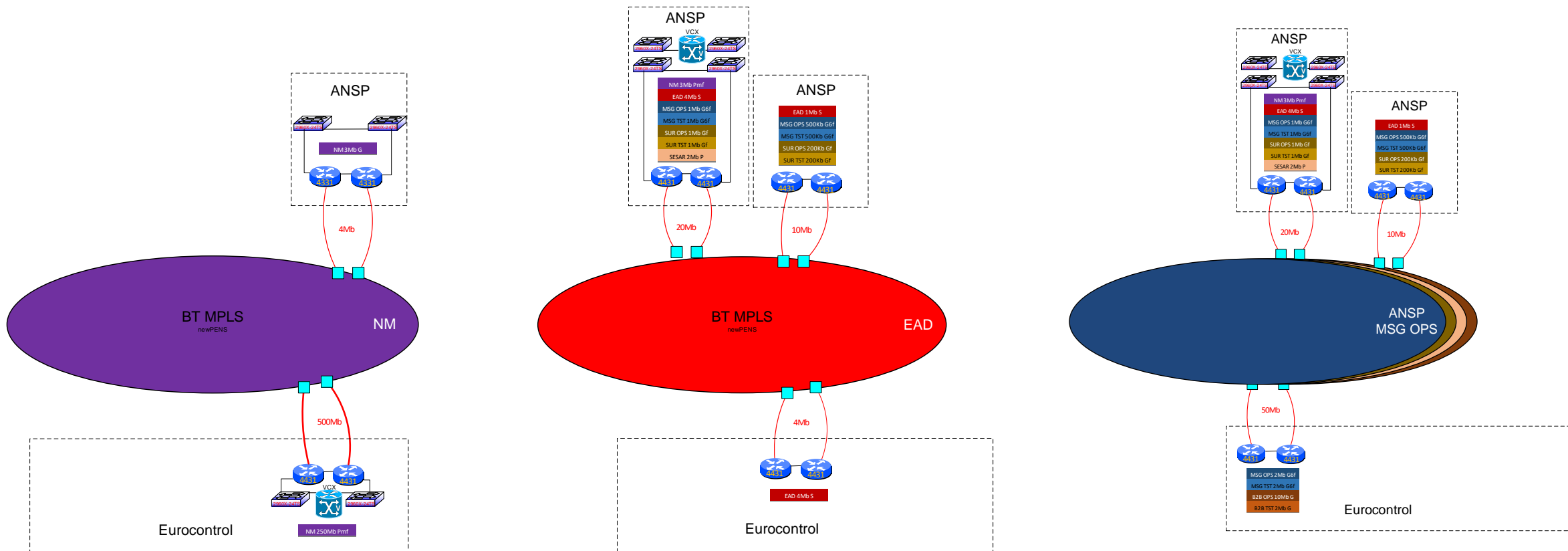
(New)PENS Architecture – Multi-VPN Concept

- Private IP connectivity
- Multi-VPN subscription model
- Built on a managed MPLS-VPN platform.



(New)PENS Architecture – Multi-VPN Concept

- Each ANSP chooses its own connectivity scope and options

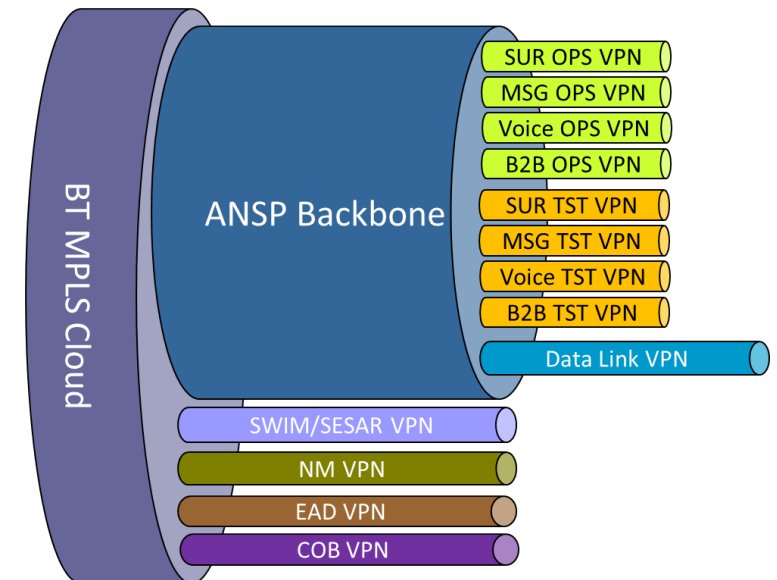


The (New)PENS VPNs



- The 'ANSP Backbone' VPNs – most also offer a Test environment.
 - ✓ MSG OPS / MSG TST (messaging – FMTP, AMHS)
 - ✓ SUR OPS / TST (radar / surveillance)
 - ✓ DataLink (access to SitaForAircraft ATN / ACARS services)
 - ✓ Voice OPS / TST (ANSP IP voice)
 - ✓ SWIM/SESAR
 - ✓ B2B OPS / TST (e.g. LARA)
- NM VPN - Network Manager
- EAD VPN (European AIS Database)
- Some EUROCONTROL-specific VPNs

- Most VPNs allow any-to-any connectivity, some are hub-and-spoke.
- Each VPN offers an agreed Class-of-Service profile.



(New)PENS Architecture – Management VPN

- NewPENS is a fully managed service.
- BT monitors its routers, switches and other devices.
- Various monitoring tools using SNMP, IP SLA...
- Most monitoring is via a separate NewPENS VPN called BT Management.
- Via this dedicated VPN, BT can:
 - ✓ Interrogate devices
 - ✓ Update configurations or software
 - ✓ Receive alarms
 - ✓ Send test traffic
 - ✓ Perform troubleshooting
- BT also offers read-only SNMP and VTY access to the customer.

(New)PENS Architecture – Key Service Characteristics

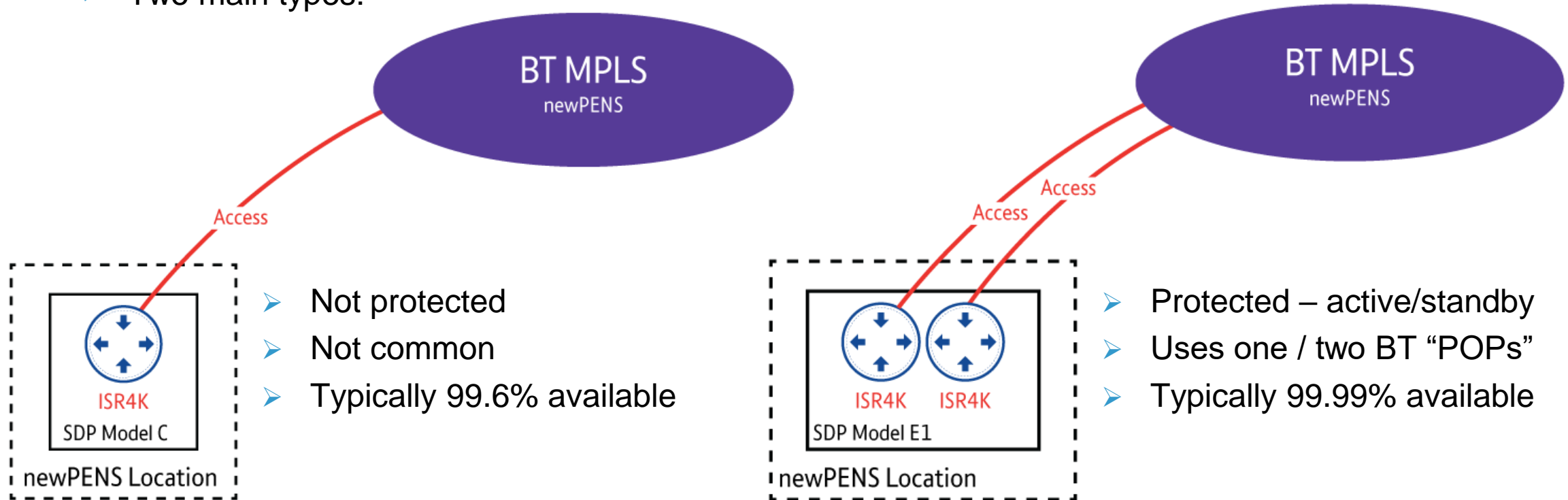


- Pre-defined per-VPN behavior
 - ✓ Topology
 - ✓ Classes of service

- Catalogue-based service options
 - ✓ Resilience options
 - ✓ Routers and switches
 - ✓ Access capacity
 - ✓ VPN mix and capacities
 - ✓ Features
 - ✓ LAN presentation type

(New)PENS Architecture – Main SDP Types

- NewPENS is accessed via a Service Delivery Point (SDP)
 - ✓ Access line(s), router(s), LAN switch(es)
 - ✓ Multiple catalogue options
 - ✓ Two main types:



(New)PENS Architecture – Routers

- Cisco ISR4K family (other options exist).
- ISR4331
 - ✓ Up to 300Mbps total in+out
 - ✓ Single PSU
- ISR4431
 - ✓ Up to 1000Mbps (total in+out)
 - ✓ Dual PSU capability
- Both expandable
 - ✓ NIM-ES2-8, NIM-2GE...
- Both accept SFP modules to support fibre.



(New)PENS Architecture – Switches

- Cisco Catalyst 2960X-24TS-L.
 - ✓ 24 x 10/100/1000 Ethernet ports + 4x SFP uplinks
 - ✓ No expansion slots
 - ✓ Forwarding rate (64-byte L3 packets): 71.4Mpps
 - ✓ Single PSU

- Currently only provided for NM VPN

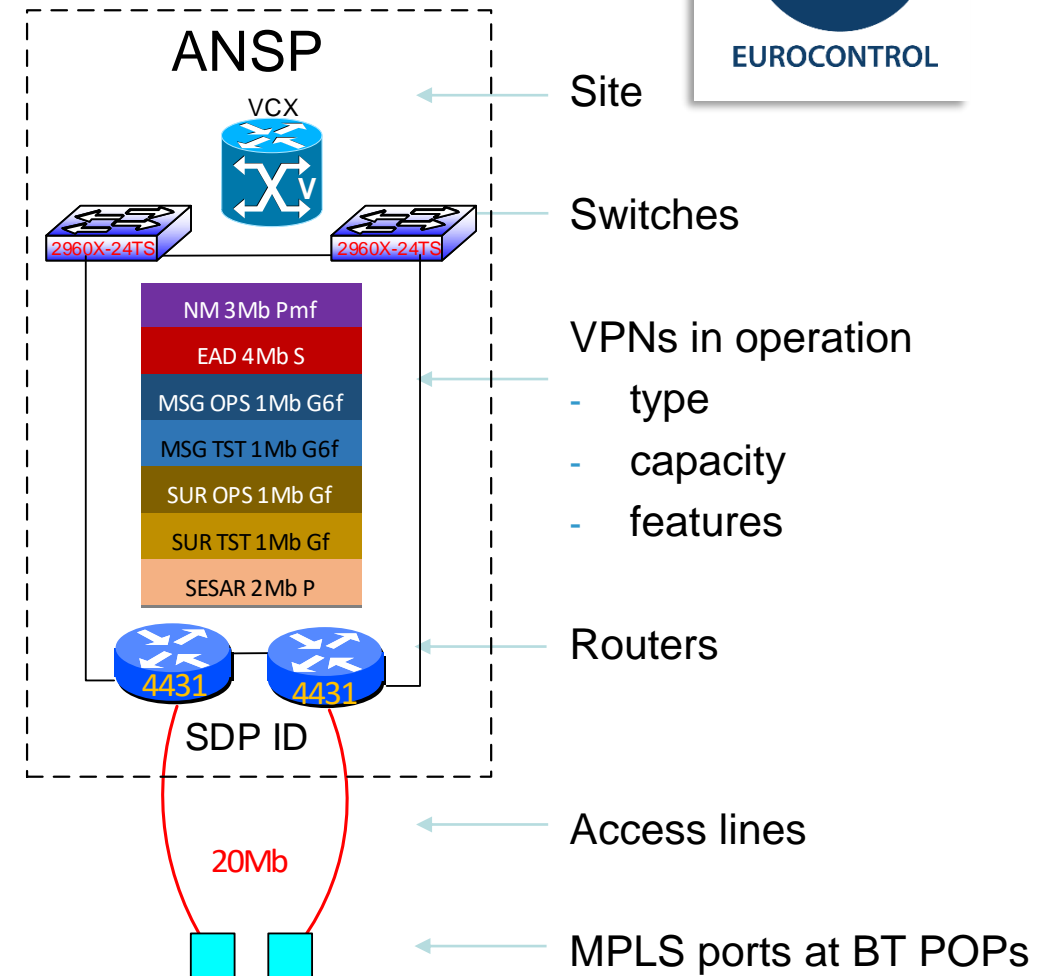


(New)PENS Architecture – Capacities

- Typical access line capacities
 - ✓ Standalone ANSP 2Mbps - 100Mbps
 - ✓ Standalone NM 2Mbps – 10Mbps
 - ✓ Shared SDP 10Mbps – 100Mbps
- Typical VPN capacities 64kbps – 2Mbps
- Capacities are chosen by the ANSP according to need.

(New)PENS Architecture - Features

- Each VPN has a fixed, dedicated capacity.
- Depending on type, each VPN can have:
 - ✓ IPv6 capability
 - ✓ Fast Convergence
 - ✓ IPv4 multicast
 - ✓ Different DSCP Class-of-Service bundles
 - ✓ 'Backdoor Resilience' between multiple SDPs
- Each VPN can be presented
 - ✓ on dedicated Ethernet or trunked LAN ports
 - ✓ on copper or fibre
 - ✓ via BGP peering or Hot-Standby Routing Protocol



(New)PENS Architecture – Security - VPNs



- The use of MPLS-VPN technology across BT's private platform makes each VPN fundamentally an isolated network.
- Access lines are private Ethernet services (whether BT or third party)
- Each VPN is a shared environment with defined connectivity rules.
- Routes are filtered to match the permitted connectivity.

- ANSPs need to take measures to secure their own infrastructure from the activities of other connected sites.

- DL VPN breaks out to SitaForAircraft via a firewalled NNI.

(New)PENS Architecture – Security – Internet and Firewalls



- The VPNs do not have Internet breakout.
- Three Standalone-NM VPNs use IPSec-over-Internet for secondary access.
- No ANSP connectivity is exposed to the Internet.

- EUROCONTROL uses separate Internet service
- BT uses managed firewalls to separate any Internet-exposed hardware from its management VPN.

- All firewalls are managed and monitored for events from BT's Madrid cybersecurity control centre.

Q&As



ITEM 4 - Cybersecurity and the EATM CERT

- EATM Network and Cybersecurity
- Q&As

Speaker: Patrick Mana (EUROCONTROL – EATM CERT)



Leonardo

Company / Kopter

20 6H 58 S

Secret data link: Hidden

Password: Hidden

Group

Kopter Group (Leonardo) have been hacked and data locked and stolen. They do not write to us so we will publish all data in 72 hours. Some example files have been uploaded for proof. 2019-12-17_Statement_of_Accounts_-_Sales_Contracts.xlsx Avionic_Elec_Detailed_Plan.xism Projekt LINDEN - Linden_Finance Q&A_05122019_V1.xlsx Projekt LINDEN - Linden_Finance Q&A_05122019.xlsx Projekt LINDEN - Linden_Finance Q&A_06122019_CTI.xlsx Projekt LINDEN - Linden Tax 191205_QA List Tax.xlsx All data release in final upload.



Manufacturing giant Aebi Schmidt hit by ransomware

Zack Whittaker @zackwhittaker / 11:04 PM GMT+2 • April 23, 2019



Boeing Hit by Cyberattack, Says Jetliner Production Not Affected

Aircraft production and deliveries aren't affected, the airplane manufacturer said.

Bloomberg

MAR 29, 2018

Airbus hit by series of cyber attacks on suppliers



Issued on: 26/09/2019 - 09:26



Saturday, 12 December 2020 08:38

Dassault subsidiary in US hit by Windows Ragnar Locker ransomware Featured

4 DEC 2020 NEWS

Aerospace Giant Embraer Downed by Suspected Ransomware

Tech Giant GE Discloses Data Breach After Service Provider Hack

By [Sergiu Gatlan](#)

March 23, 2020 05:47 PM 0





Home / About / SFO News / NOTICE OF DATA BREACH: March 2020

NOTICE OF DATA BREACH: March 2020

Click [Here](#) for Notice

April 7, 2020

TO: All Airport Commission Employees

FROM: Airport ITT

SUBJECT: Notice of Data Breach

Source: Hacker holding Cleveland Hopkins International Airport systems hostage demands ransom via Bitcoin



By [Paul Orlosky](#) | April 25, 2019 at 4:20 PM EDT - Updated April 26 at 10:46 AM

AIRLINE NEWS

Israeli Flight Attendant Sold Access to Private Passenger Information and Airline Systems in Major Security Breach

7TH JUNE 2020

EasyJet admits data of nine million hacked

By Jane Wakefield
Technology reporter
© 19 May



British Airways fined £20m over data breach

© 16 October 2020 | Technology



European Airport Systems Infected With Monero-Mining Malware

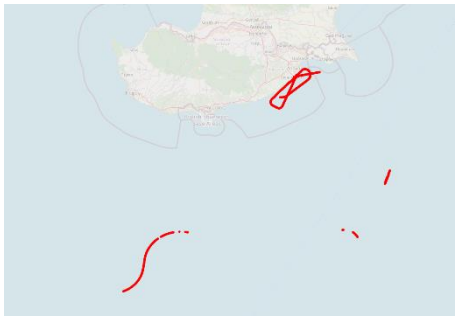
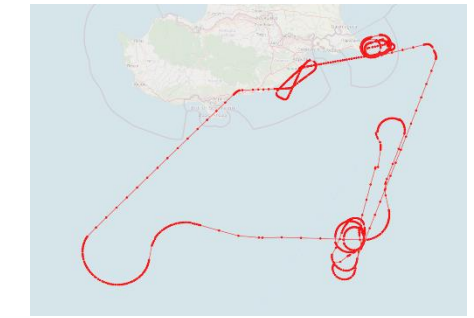
By [Sergiu Gatlan](#)

October 17, 2019 11:47 AM 0

SITA cyber attack accesses passenger data for multiple airlines

A Cyberattack on Garmin Disrupted More Than Workouts

A ransomware hit and subsequent outage caused problems in the company's aviation services, including flight planning and mapping.



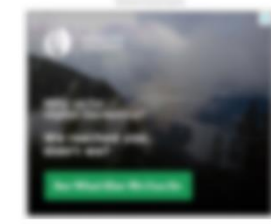
GPS DEGRADATION DASHBOARD

WORLD MAPPING OF GPS INTERFERENCE AREAS

- Can affect around 38% of European Network Traffic
- Affects major Europe to Middle-East and Asia Routes
- Measurably increases ATC and pilot workload
- Decreases aviation safety
- Requires retention of terrestrial systems

Man hijacks Portland airport monitor to play video games, until PDX officials declare 'game over'

Posted Jan 16, 2020



We are sorry for the inconvenience. Our Engineers are currently working to resolve the issue as soon as possible.

We are sorry for the inconvenience. Our Engineers are currently working to resolve the issue as soon as possible.

PARIS01	08:05	DURHAM	27	BOARDING
BAN1801	08:20	AMSTERDAM	24	BOARDING
KL1050	09:20	PALMA	2,5	BOARDING
EZ1691	10:20	BARCELONA	15	BOARDING
TOH482	10:35	BARCELONA	34	BOARDING
BW3205	10:35	PARIS	11	BOARDING
PA3243	11:30	TOULOUSE	12	BOARDING
RY6431	11:30	ALGERIE	13	BOARDING

FUCK VIETNAM PHILIPPINES JOINT ACTION

#Op CHINA ACTION IS HONORABLE

VIETNAM THE PHILIPPINES ONLY THE UNITED STATES, JAPAN, RESTRICT CHINA'S PAWN

MAN TO BE LOW KEY

Airline forced to cancel flights in Alaska after cyberattack

By Associated Press

December 23, 2019 | 12:16pm

CYBER SECURITY NEWS · 4 MIN READ

Impact of Cyber Attacks on RavnAir More Damaging Than First Thought; Flights May Be Grounded for a Month

SCOTT IKEDA · JANUARY 14, 2020

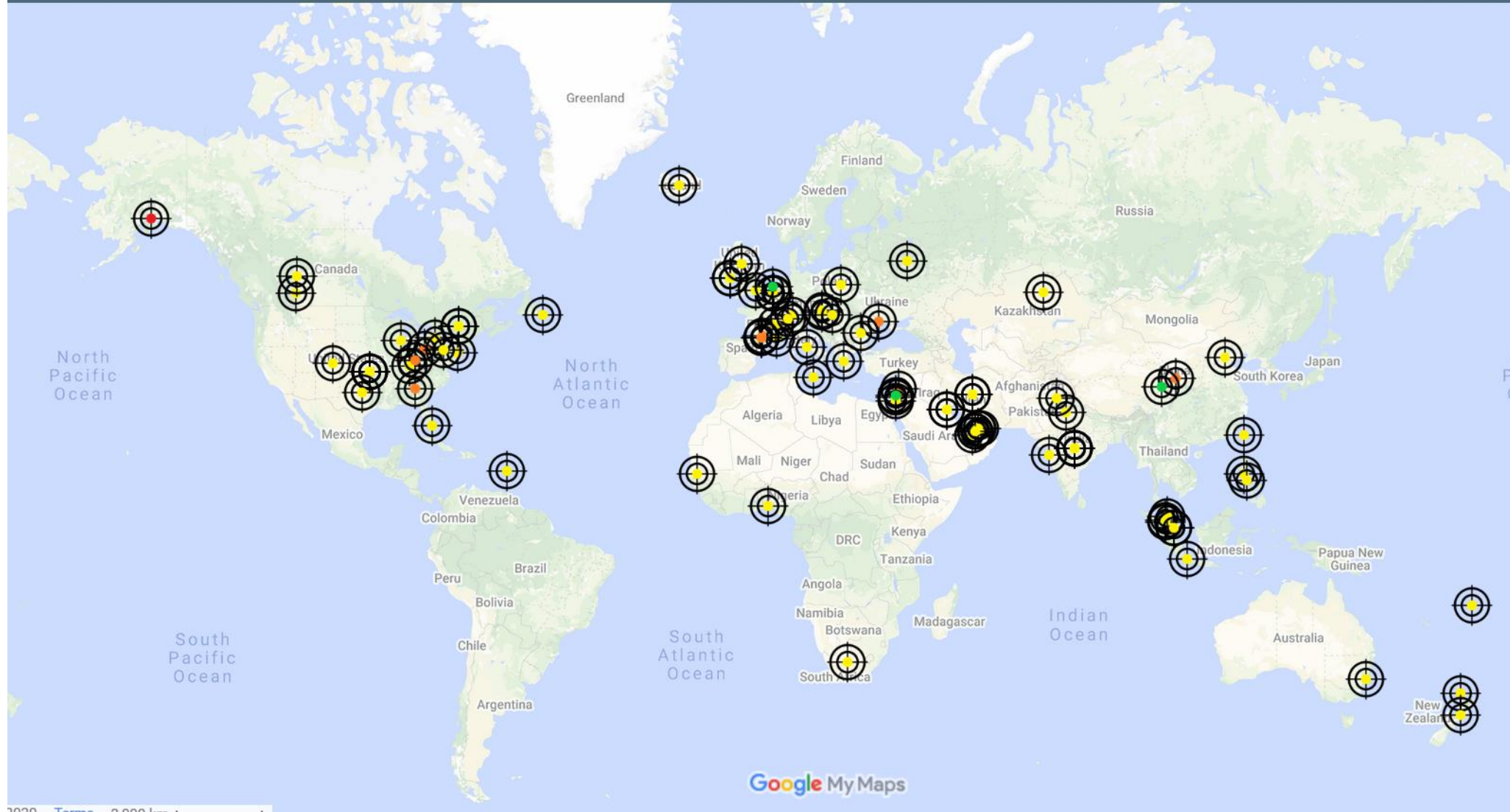
Arrival of international flights

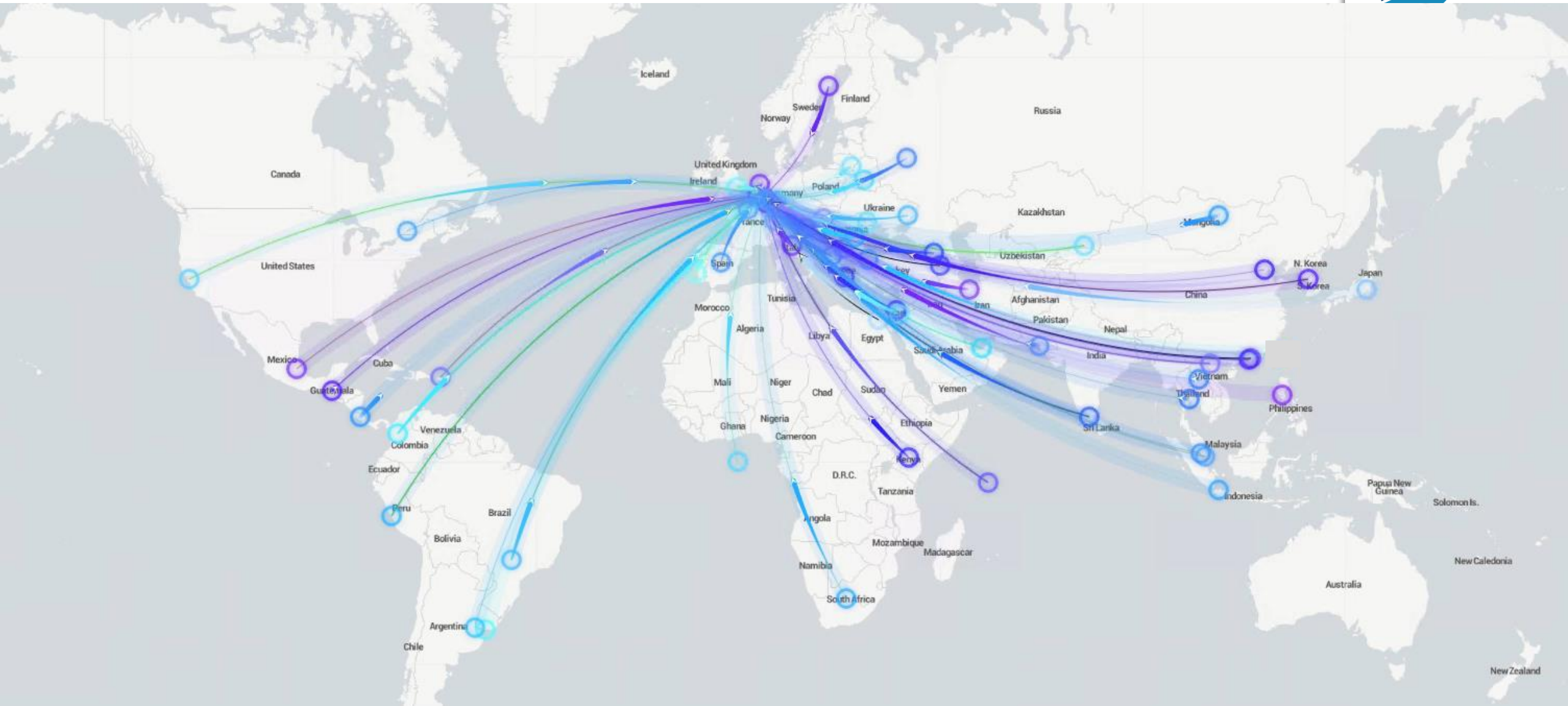
12:00	FR 2667 Kra
12:30	OS 619 Wie
12:40	8Q 288 Ista
13:00	LO 767 Wa
14:05	B2 849 Mi
14:40	LO 769 Wa
	PQ 746 Ba

ПРИБУТТЯ МІЖНАРОДНИХ РЕЙСІВ
INTERNATIONAL ARRIVALS

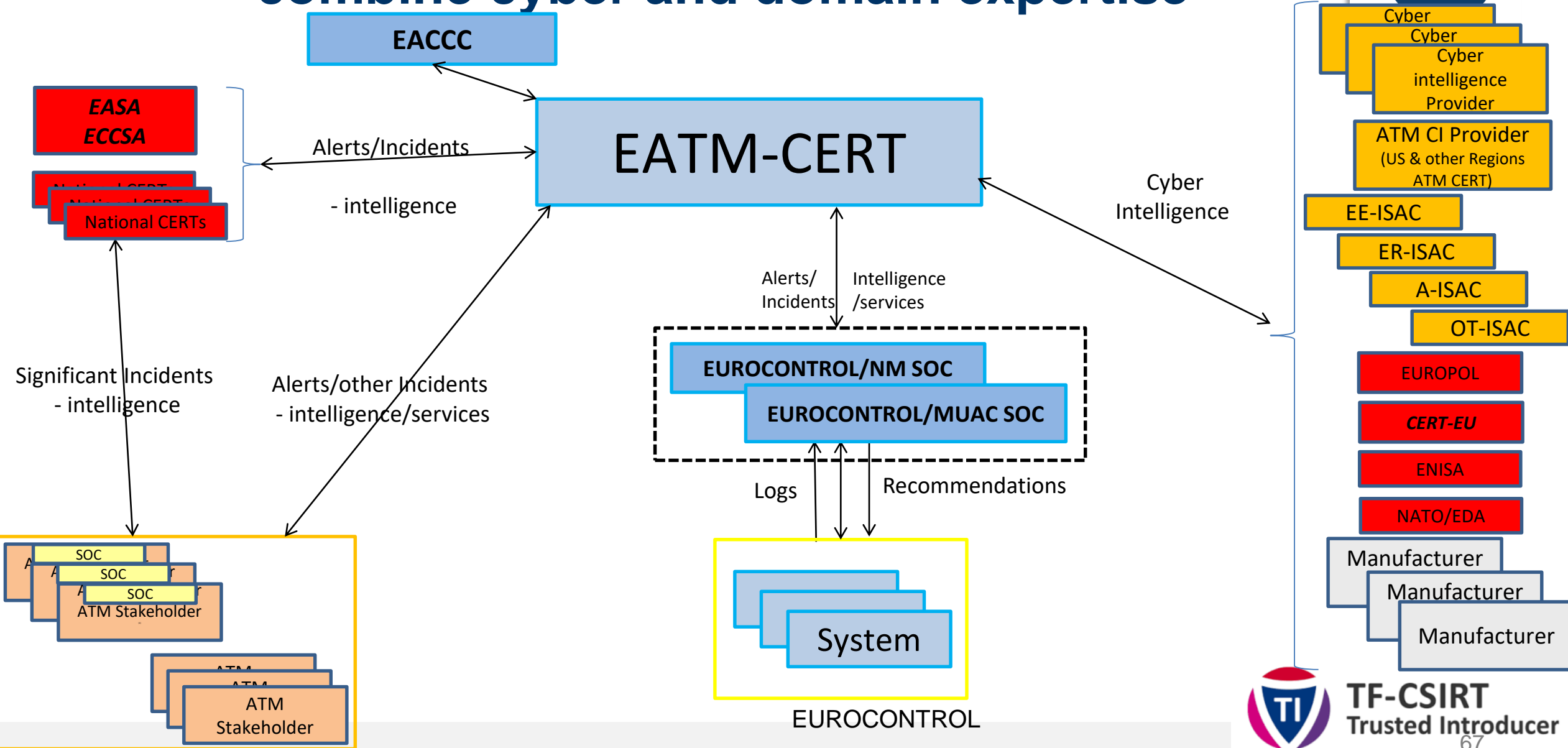
FATM-CERT Aviation Cyber Events Map

This map was created by a user. [Learn how to create your own.](#)





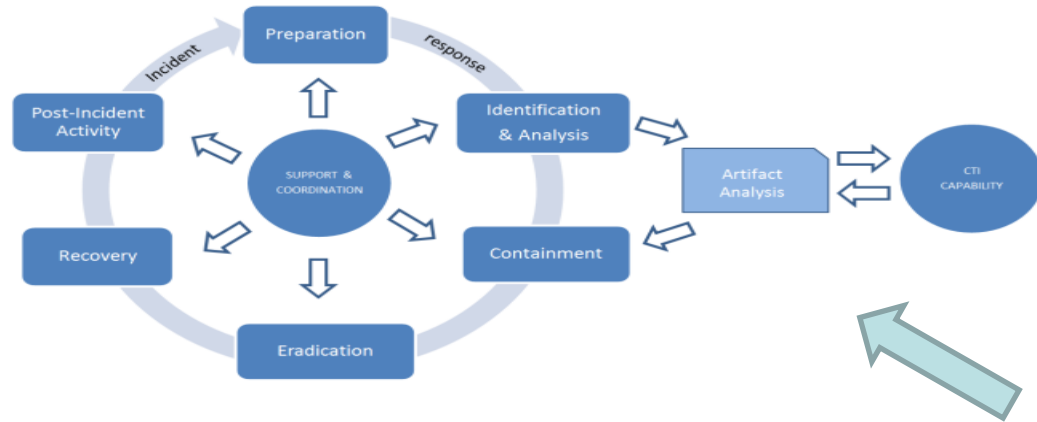
Regional sectorial (ATM) CERT: combine cyber and domain expertise



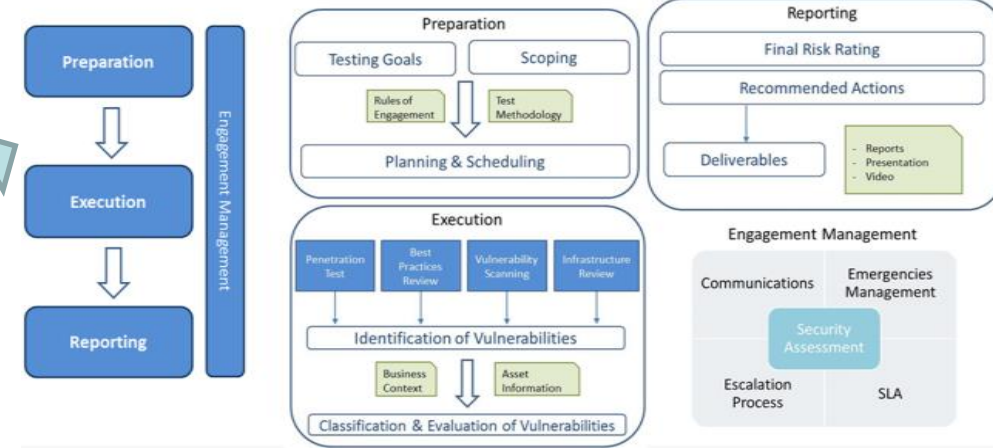
EATM-CERT: catalogue of services



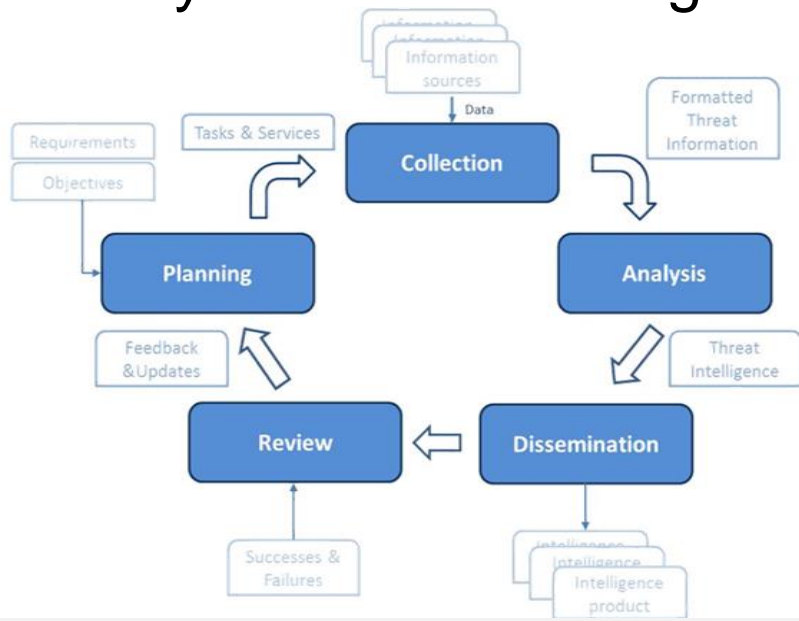
Incident Response



Security Assessment



Cyber Threat Intelligence



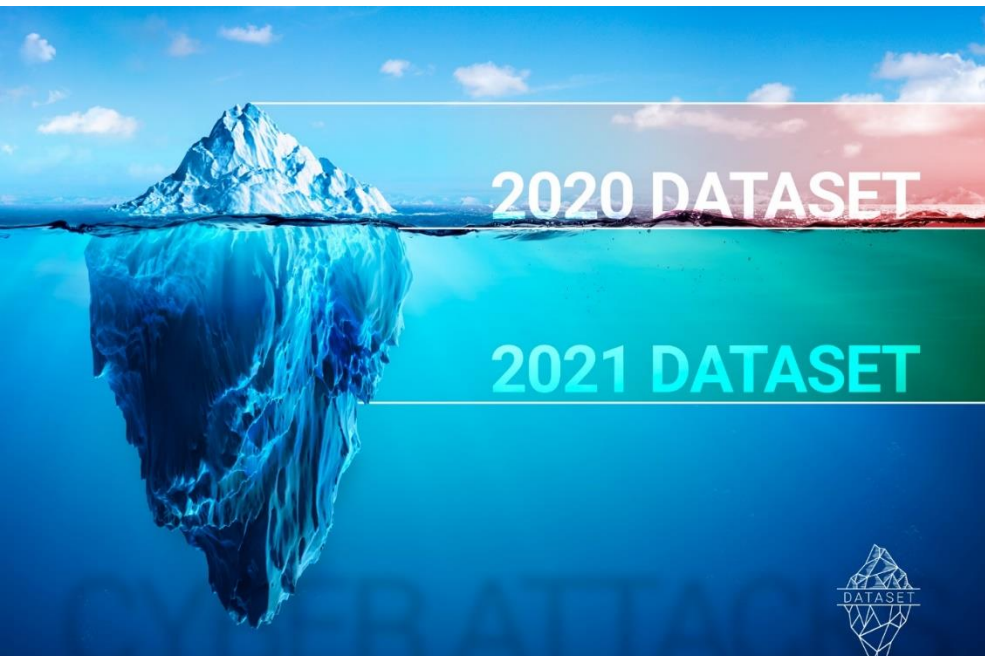
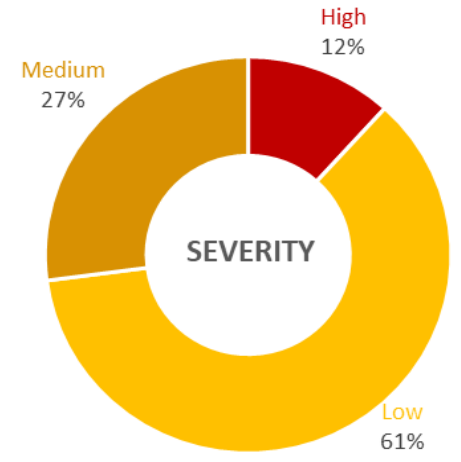
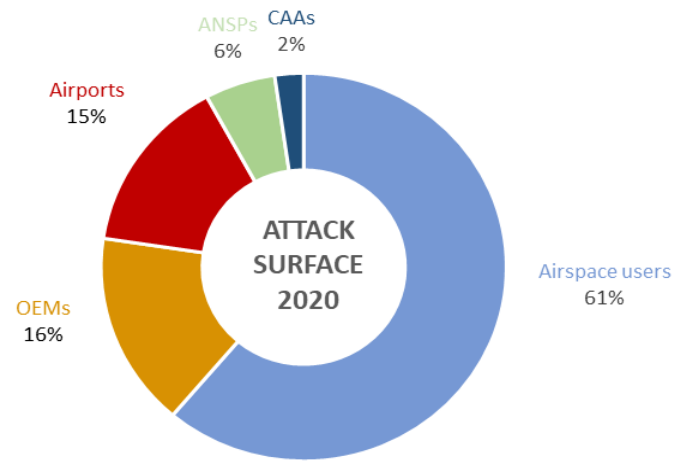
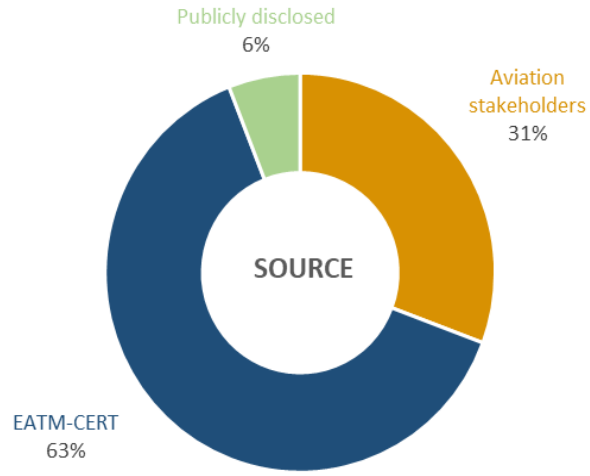
Alerts & Warnings



EATM-CERT services

1. Penetration test (EUROCONTROL services & products + Aviation stakeholders)
 2. Bank transfer scams via email
 3. Credentials leaks detection
 4. Sensitive document leaks detection
 5. Cyber Threat Intelligence (CTI) and feeds for aviation
 6. Quarterly cyber threat landscape report for senior management
 7. Annual report “cyber in aviation”
 8. Support to incident response / Artefacts analysis
 9. TLP:WHITE CTI tools – raising awareness
 - ✓ Cyber events map, tweeter
 10. Vulnerability scanning of Aviation Stakeholders
 11. IOC Scanner
 12. Training exercises (table-top & technical) - EACCC-CYBER22
- Soon
1. Phishing awareness campaigns
 2. Test of Anti-DDOS solutions

EATM-CERT 2021 report on cyber in aviation

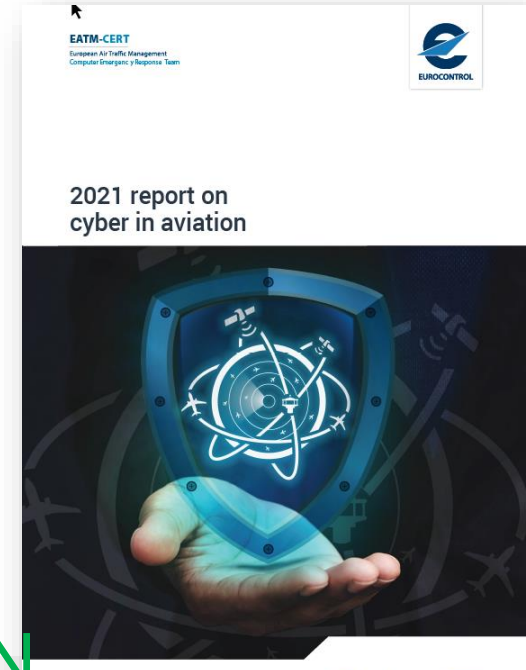


~200 events

~1.260 events



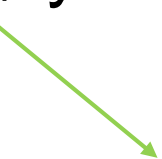
Report is
TLP:GREEN



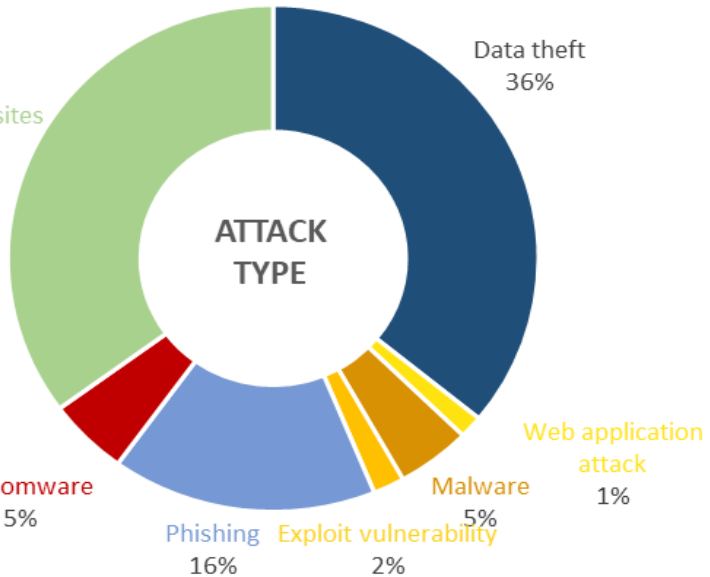
EATM-CERT 2021 report on cyber in aviation



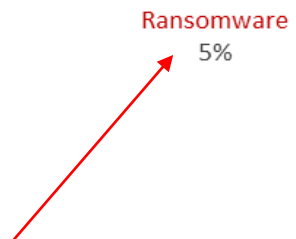
1 Bn\$/y



Fraudulent websites
35%

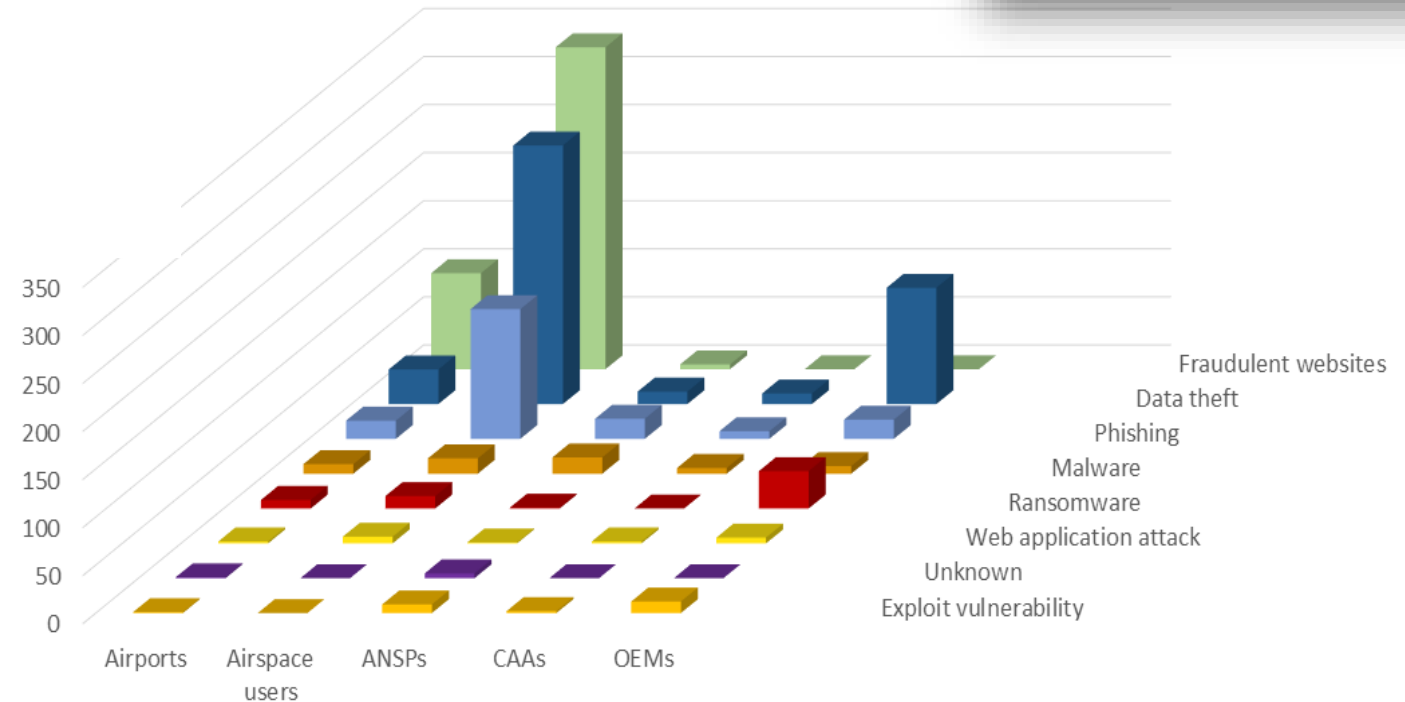


=once a week

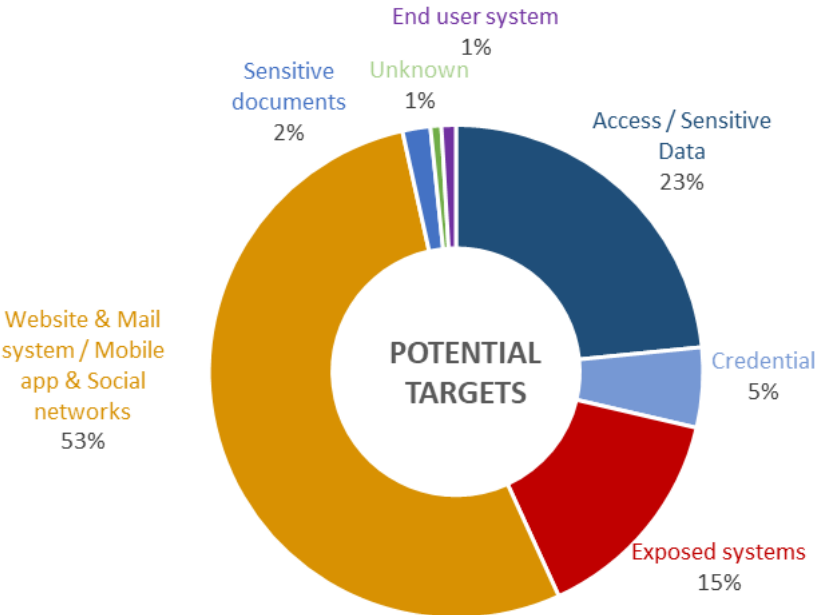
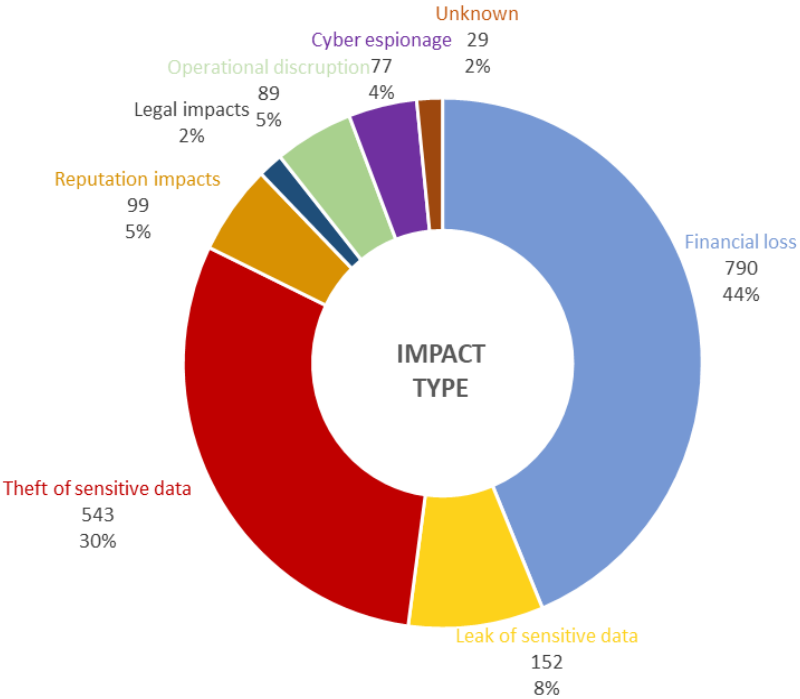


all

Phishing
16%



EATM-CERT 2021 report on cyber in aviation



KEY CYBER THREAT INDICATORS

Fraudulent websites impersonating airlines (IATA and A4E)



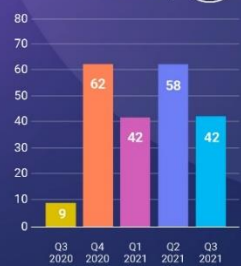
Fraudulent websites impersonating aviation stakeholders



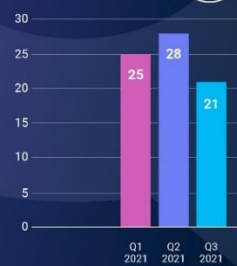
Publicly reported incidents/events (collected by EATM-CERT on the public internet)



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



Ransomware affecting aviation (worldwide - Source: EATM-CERT & A-ISAC)



EATM-CERT credential leak monitoring service users



EATM-CERT Malware Information Sharing Platform (MISP) users



EATM-CERT vulnerability scanning service users



EUROCONTROL EATM-CERT

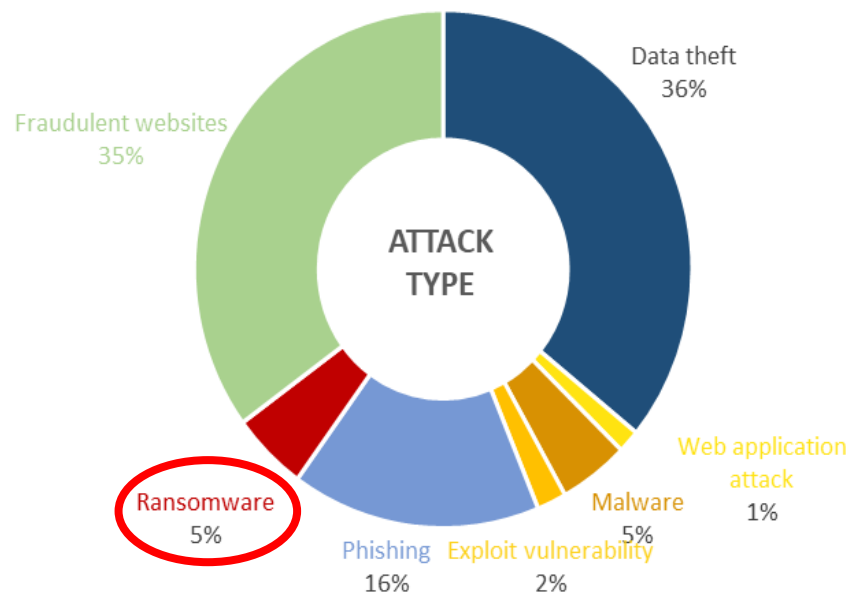
3rd Quarter 2019 Cyber Threat Landscape & Activity Report for Senior Management

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



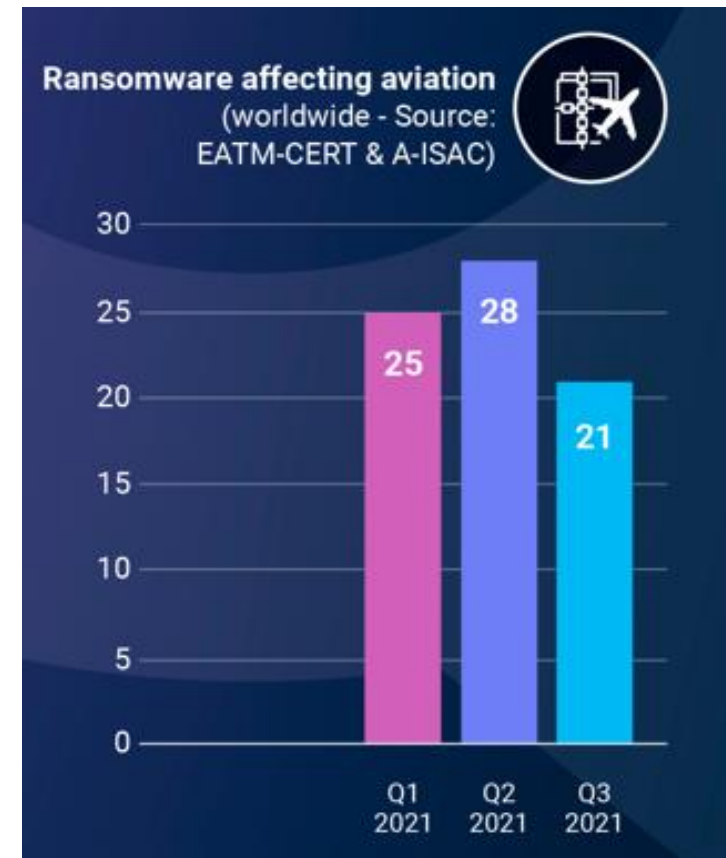
Ransomware in aviation (global)

2020
One/week

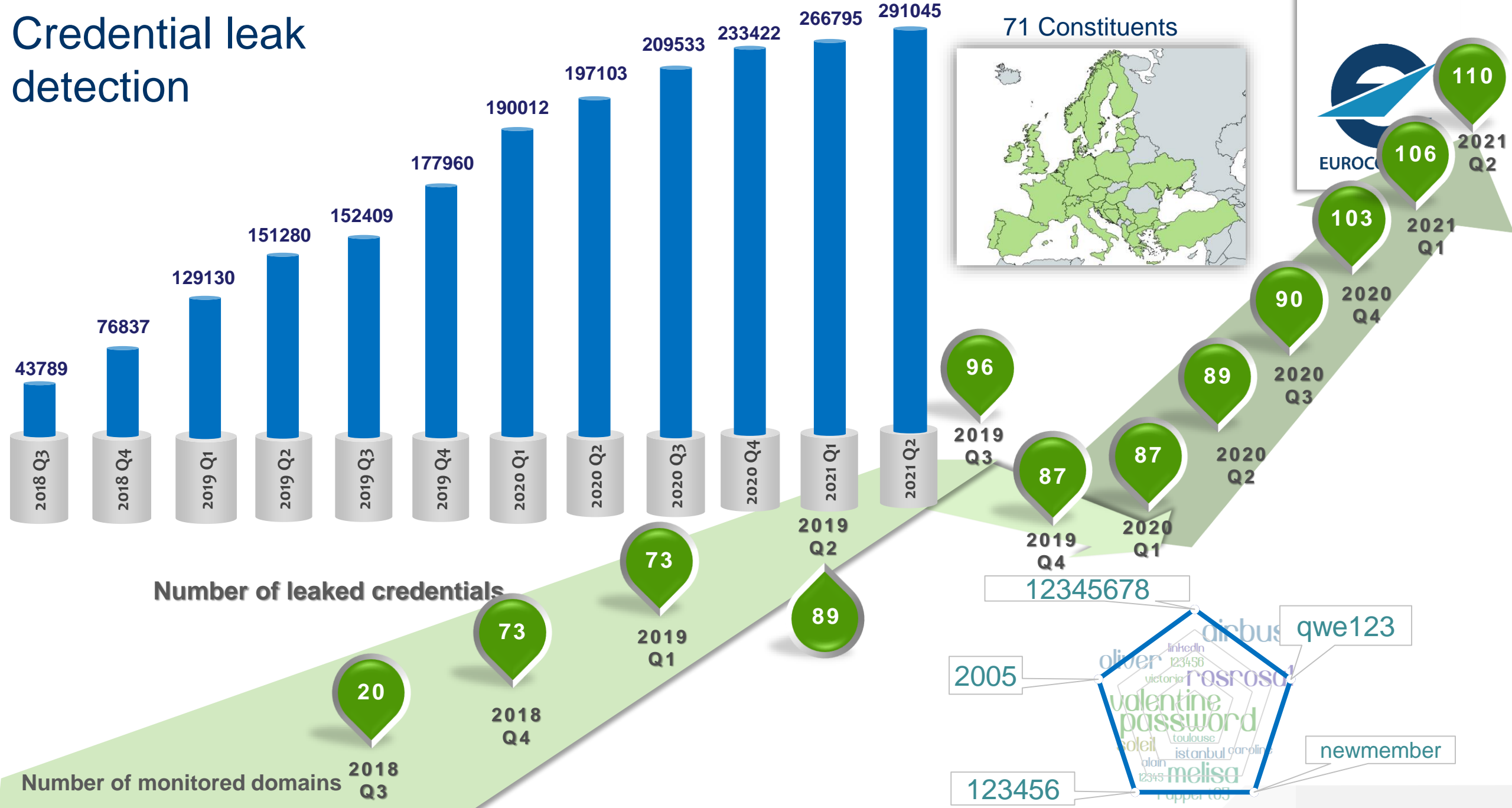


Out of 1.260 events

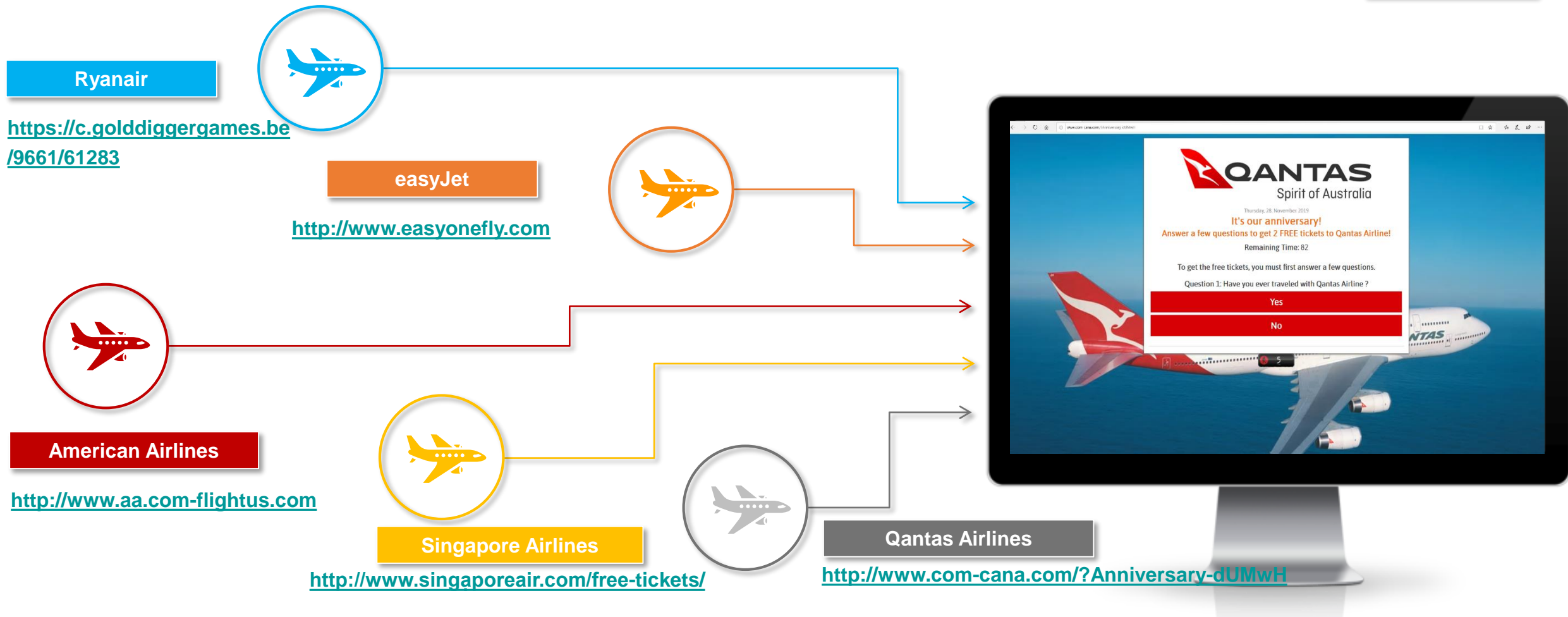
2021
Two/week



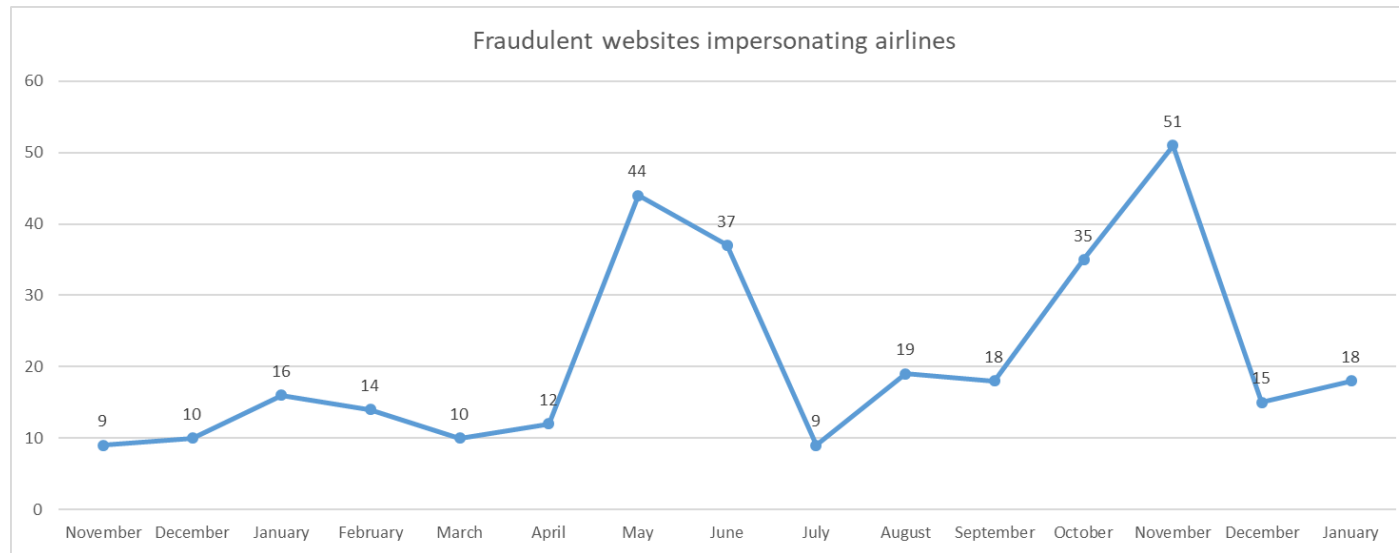
Credential leak detection



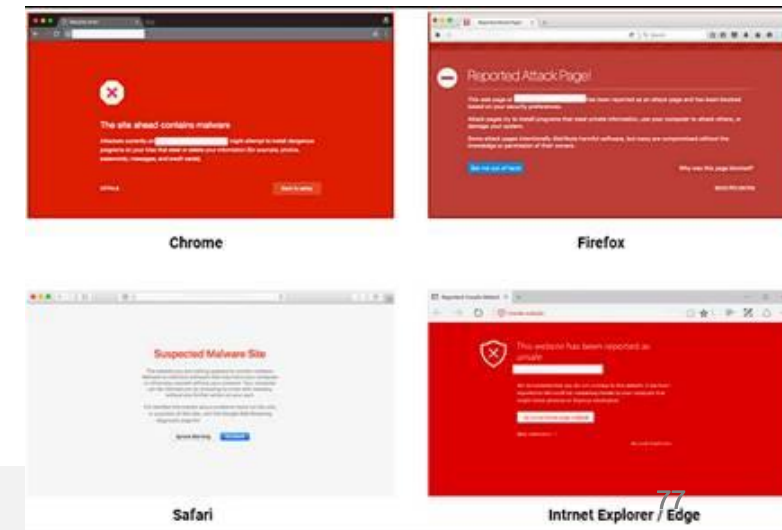
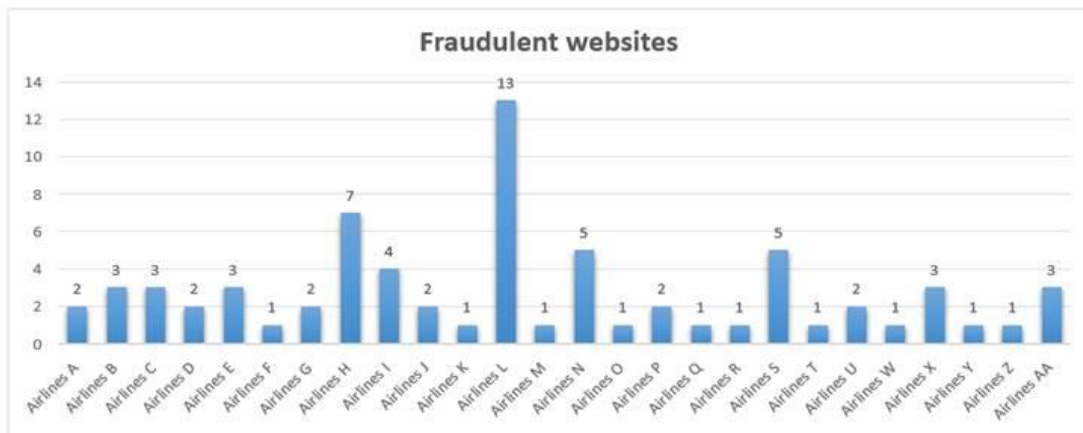
Fraudulent websites impersonating airlines



Fraudulent websites impersonating airlines



Financial impact in 2019: ~1Bn\$ (IATA)



Fraudulent websites



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



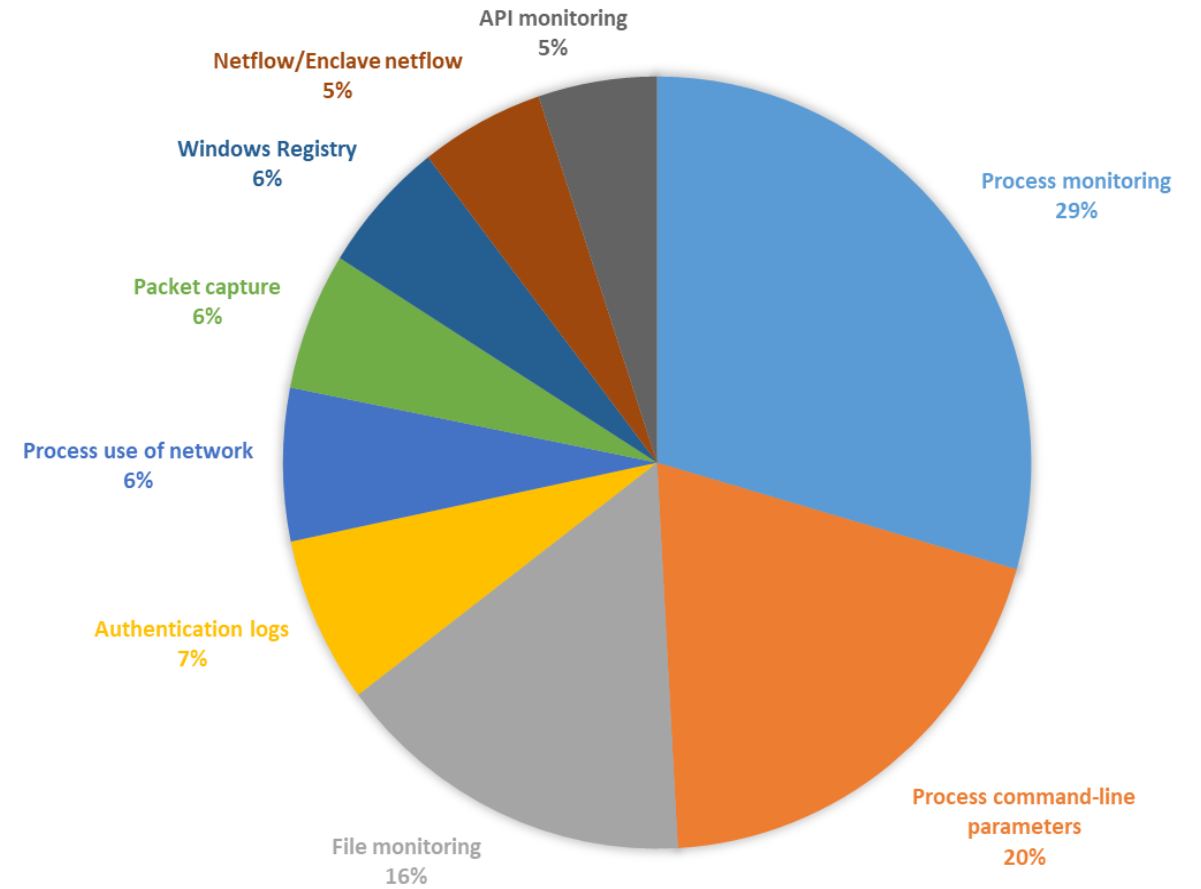
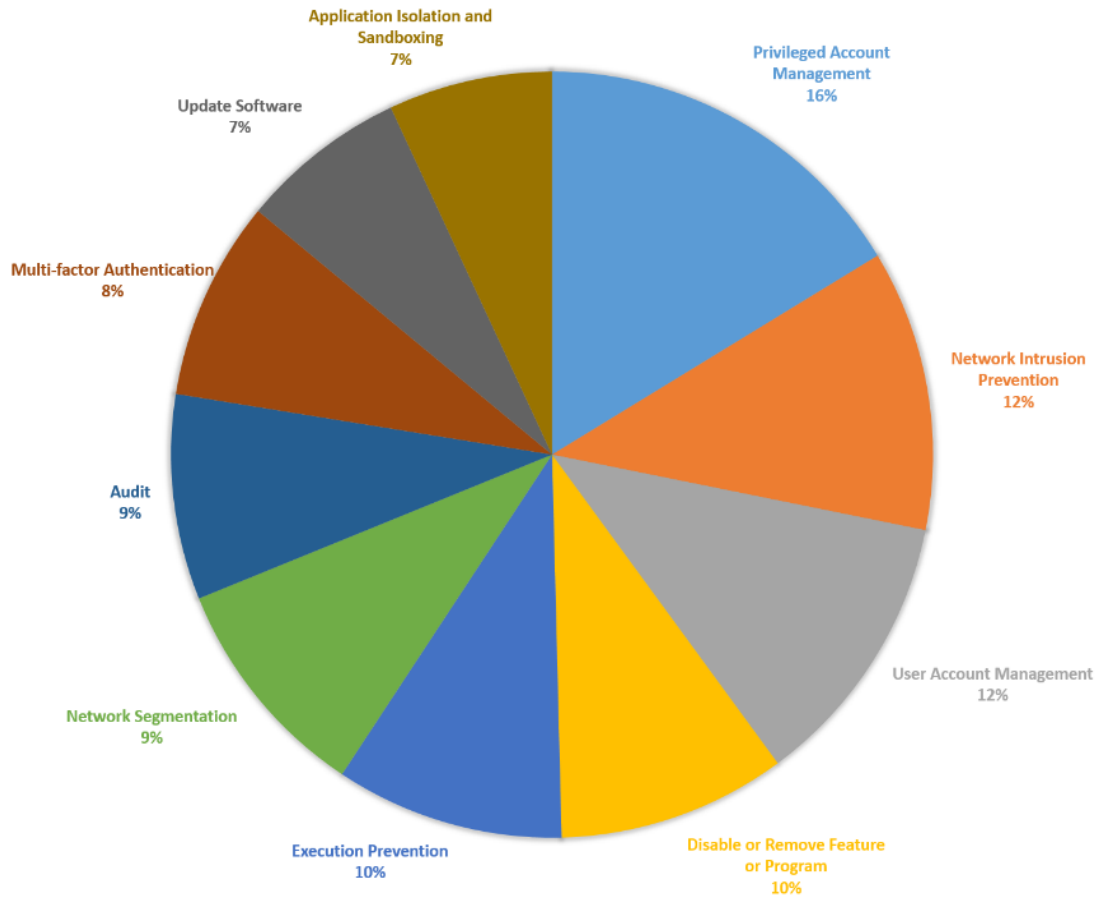
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
Spearphishing Attachment	Command-Line Interface	Registry Run Keys / Startup Folder	Scheduled Task	Obfuscated Files or Information	Credential Dumping	System Network Configuration Discovery	Remote Desktop Protocol	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		
	Mshhta	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							
				Mshhta							
				Network Share Connection Removal							
				Process Hollowing							
				Regsvr32							
				Rootkit							
				Template Injection							

List of APTs targeting aviation

APT 1	APT 2	APT 3
APT 10	APT 14	APT 18
APT 20	APT 27	APT 29
APT 33	APT35	APT 37
APT 39	APT 41	APT15
Axiom	Berserk Bear	Clever
Conference Crew	DNSSpionage	Equation
FIN6	FIN7	FIN11
HangingGarden	Ke3chang	Leafminer
Leviathan	Longhorn	Lucky Cat
Molerats	MuddyWater	Ocean Buffalo
Patchwork	Pioneer Kitten	Razor Tiger
Roaming Tiger	TeleBots	Tropic Trooper

Top 10 Mitigation Means

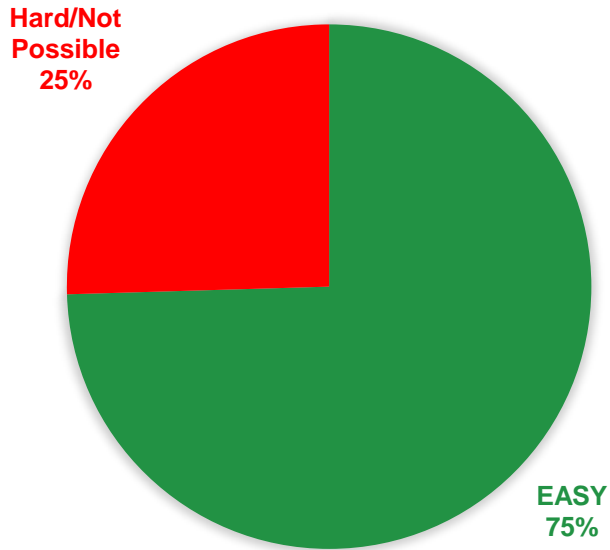
Top Detection Means



Surprise



MITIGATION POSSIBILITY



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

Q&As





ITEM 5 - Wrap-up and Closing

Speaker: Muna Alnadaf (ICAO)