Supporting European Aviation

EUROCONTROL

Cyber ~~Security~~ Activities

CEO conference

Patrick MANA
Cyber-Security Cell Manager – EATM-CERT Manager
16/05/2019

FOUNDING MEMBER SESAR JOINT UNDERTAKING

NETWORK MANAGER

Cyber : Why addressing it ?

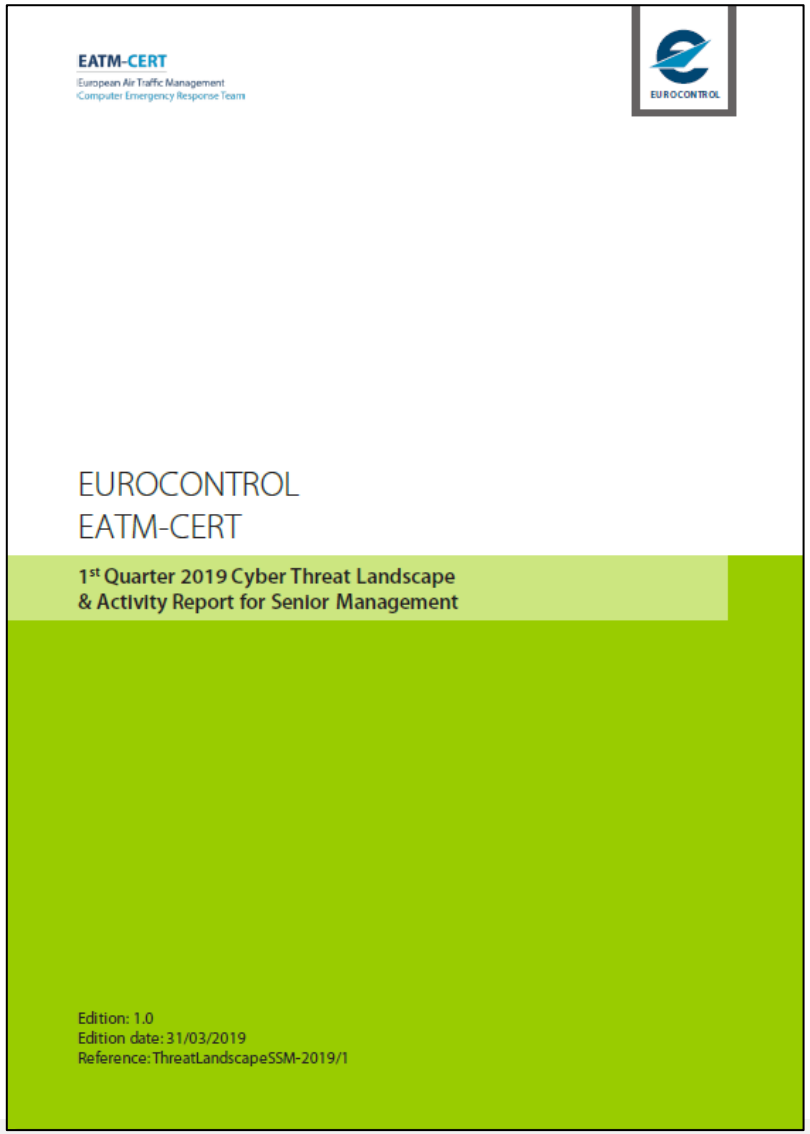
&

EC 1148/2016 (NIS Directive)

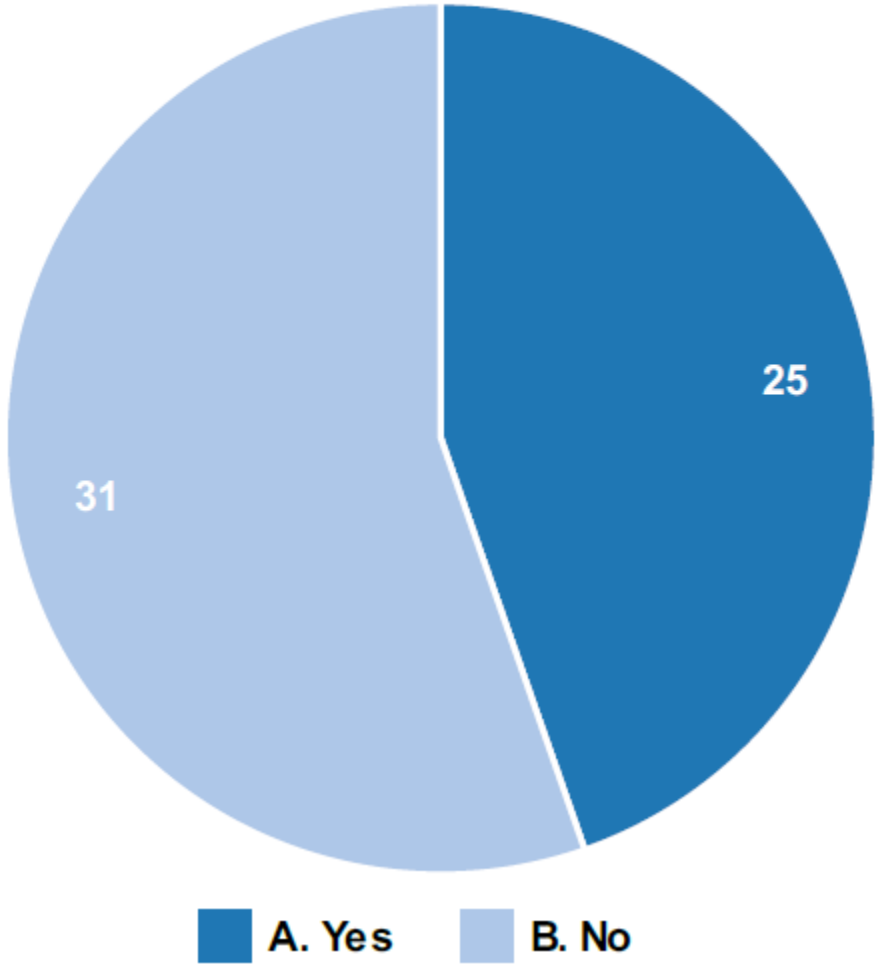
EC 373/2017

…

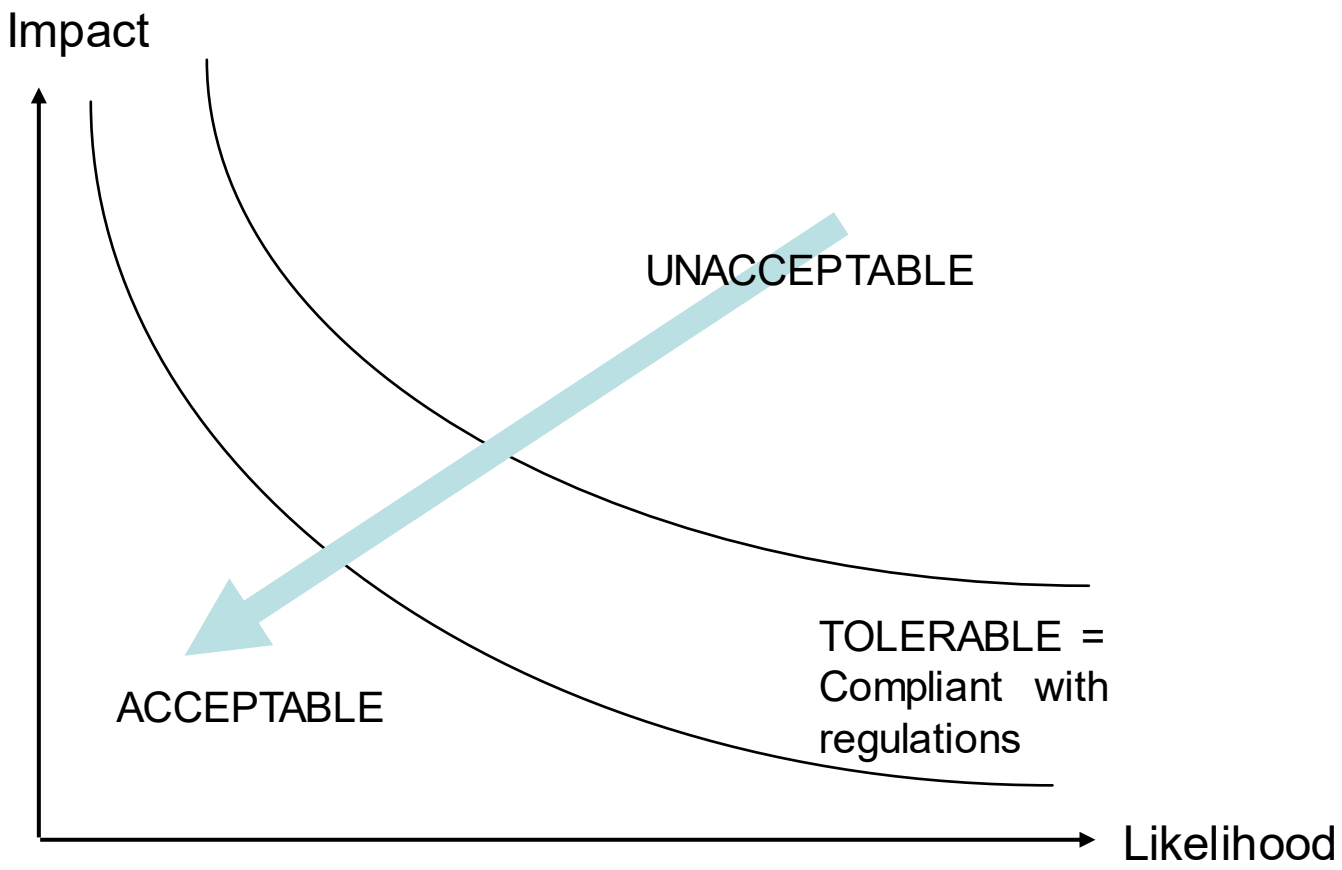
Raising Senior Management awareness



Are You (C-Suite) Receiving At Least A Quarterly Cyber Threat Landscape Report ?



Risk-based approach



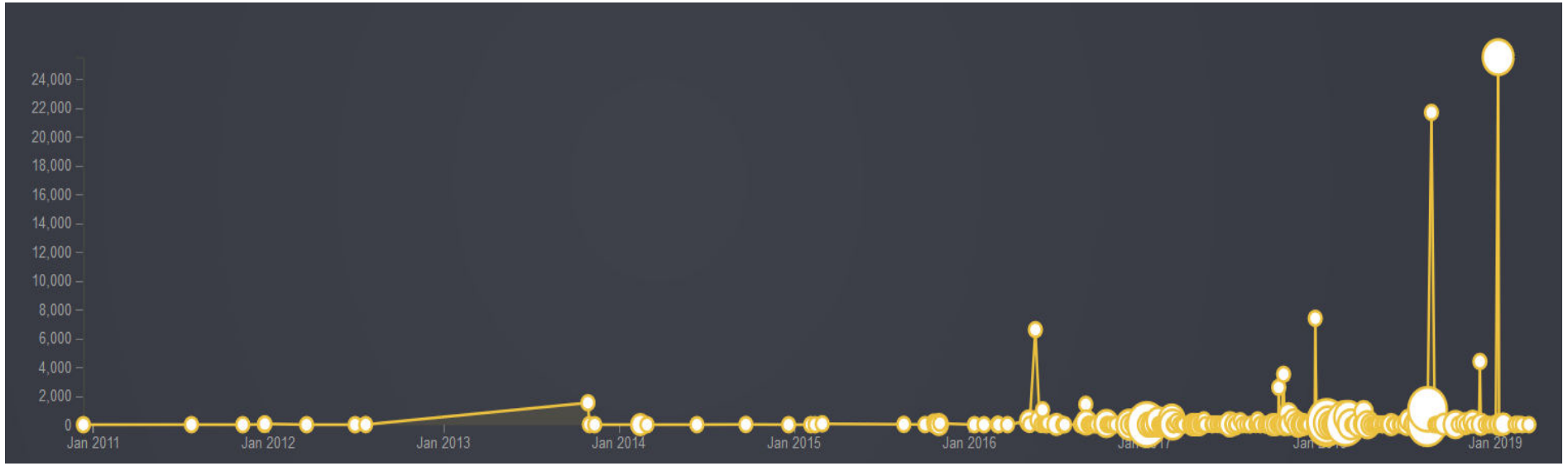
Likelihood of a cyber-attack:

Very difficult to assess

AND

Past experience not relevant

Cyber threat/risk dynamic



State-sponsored / Geo-political

Technical


Аэропорт
"Геленджик"
Геленджик
Approximate Ship Location
GPS Ship Location
2
WIRED (September 21st, 2017)


VEHICLE MINI GPS JAMMER

Cyber-crime … it's an industry

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

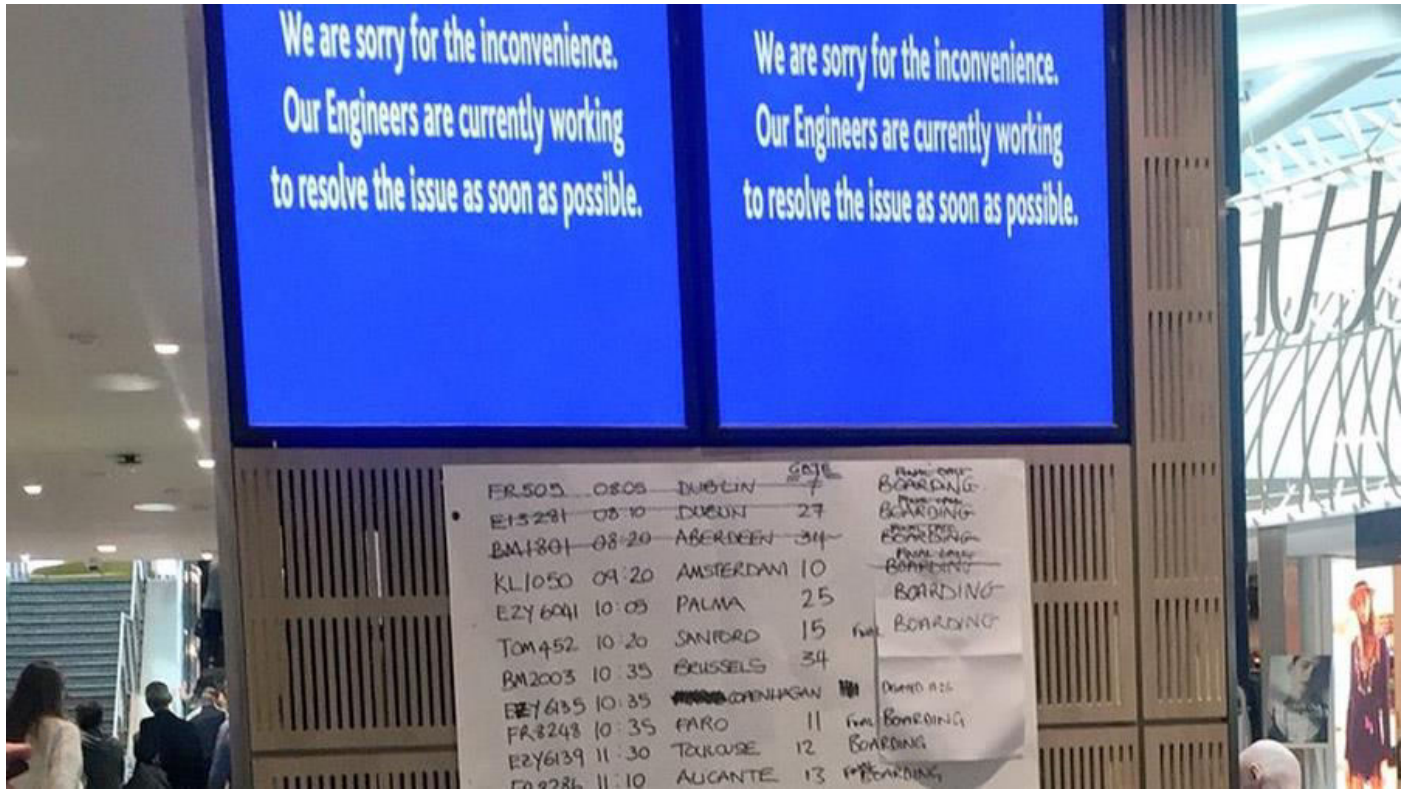
Professional Services

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

Cyber-crime: ransomware



Cyber-crime: Fraudulent e-mails impersonating EUROCONTROL

From: Veronique Martou] mailto:vmartou.eurocontrolcrco.int@gmail.com [
Sent: Tuesday, January 30, 2018 9:08 AM
To: XXXX
Subject: RE: Payment Query/Eurocontrol Charges

Dear Sirs,
we have sent a couple of emails to your accounts payable team without receiving any responses. please kindly avail us with the status of the invoices sent to you for the months of September to December 2017, to enable us reconcile our accounts and update your records in preparation of the upcoming audit of accounts. we regret all inconveniences and plead that you bear with us.note also that EUROCONTROL will not hesitate to take a strict enforcement measures and possible detention of your aircraft will be the inevitable consequence if you delay further to comply with this demands.

NB;PLEASE KINDLY FORWARD A COPY OF YOUR RESPONSES TO TO OUR ACCOUNTS TEAM AT r3.crco@euro-control.net FOR PROMPT ACTIONS.

thanks for your cooperation and understanding.

we await your prompt response.

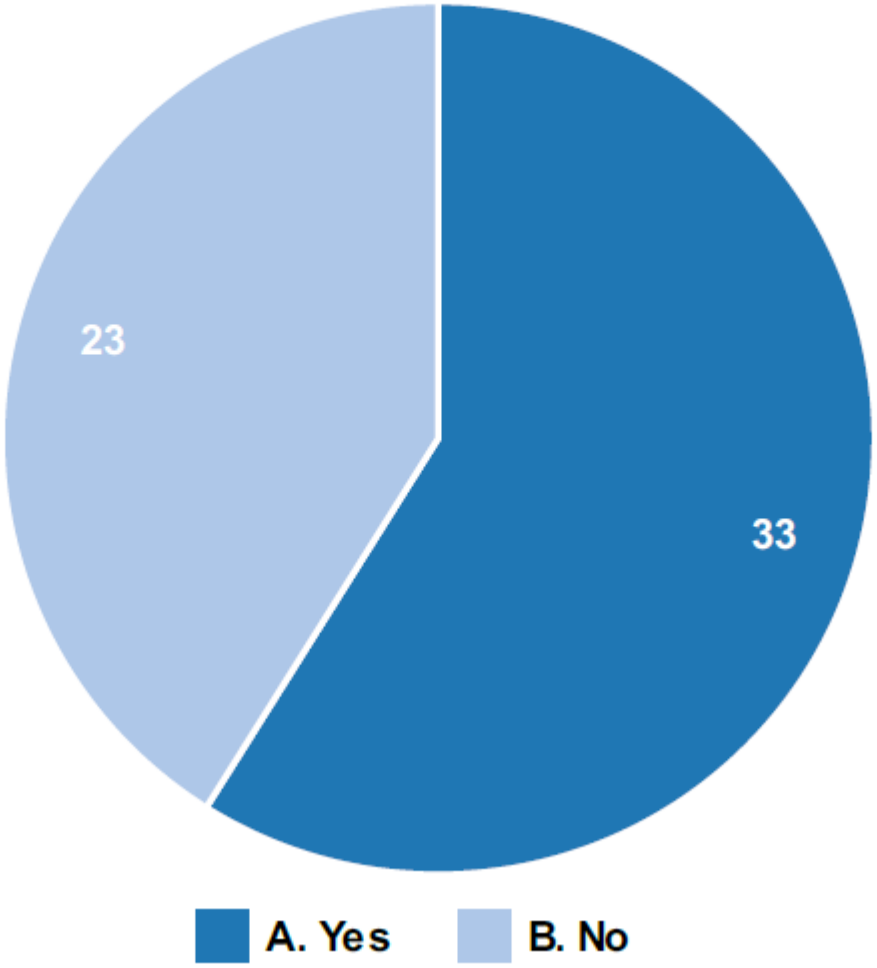
my best regards

Veronique Martou
Finance and Revenue Manager
Collection of Charges
CRCO/R4 EUROCONTROL
96Rue de la Fusee 1130
Brussels.
Email:r3.crco@euro-control.net

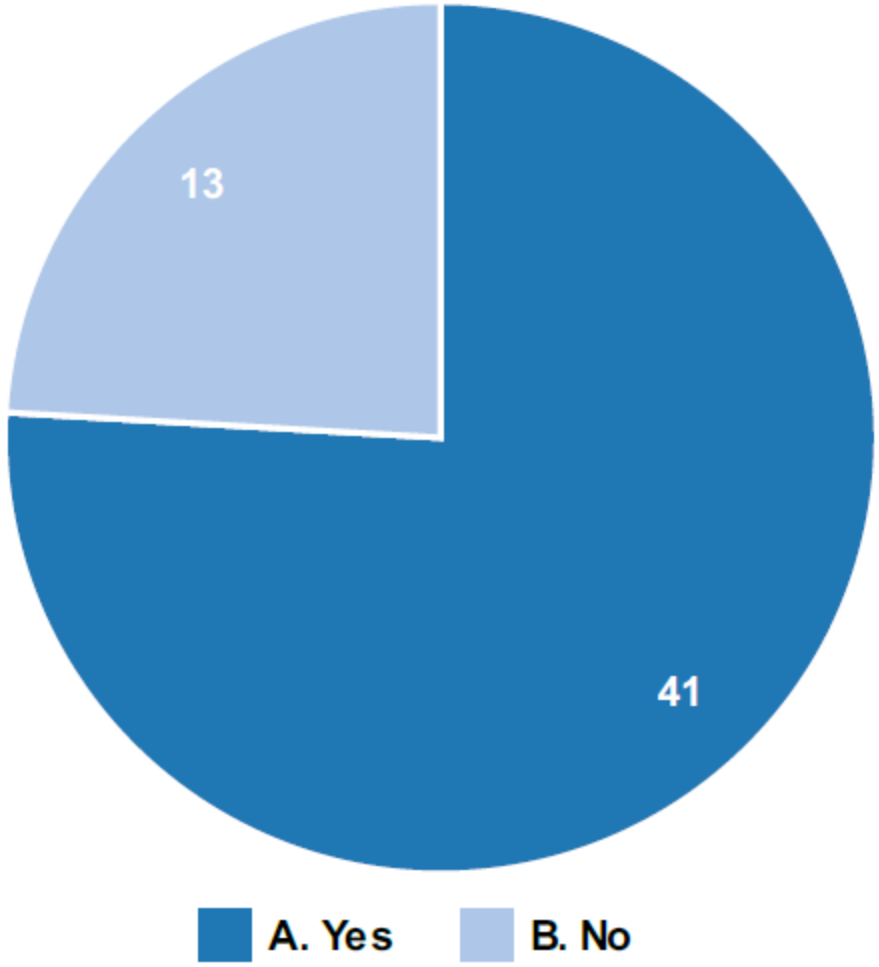
Cyber-crime: Fraudulent e-mails impersonating EUROCONTROL

Domain name	Domain closure: status	Attempts count
eurcontrolint.net	Suspended	50
eurocontroladmin.net	Suspended	29
euro-control-int.org	Suspended	13
euro-control.net	Suspended	8
eurocontolint.net	Suspended	5
euro-control.org	Suspended	3
euro-controlinc.com	Suspended	2
eurocontrotint.net	Suspended	2
eurocontroint.net	Suspended	1
eurocontrolints.net	Suspended	1

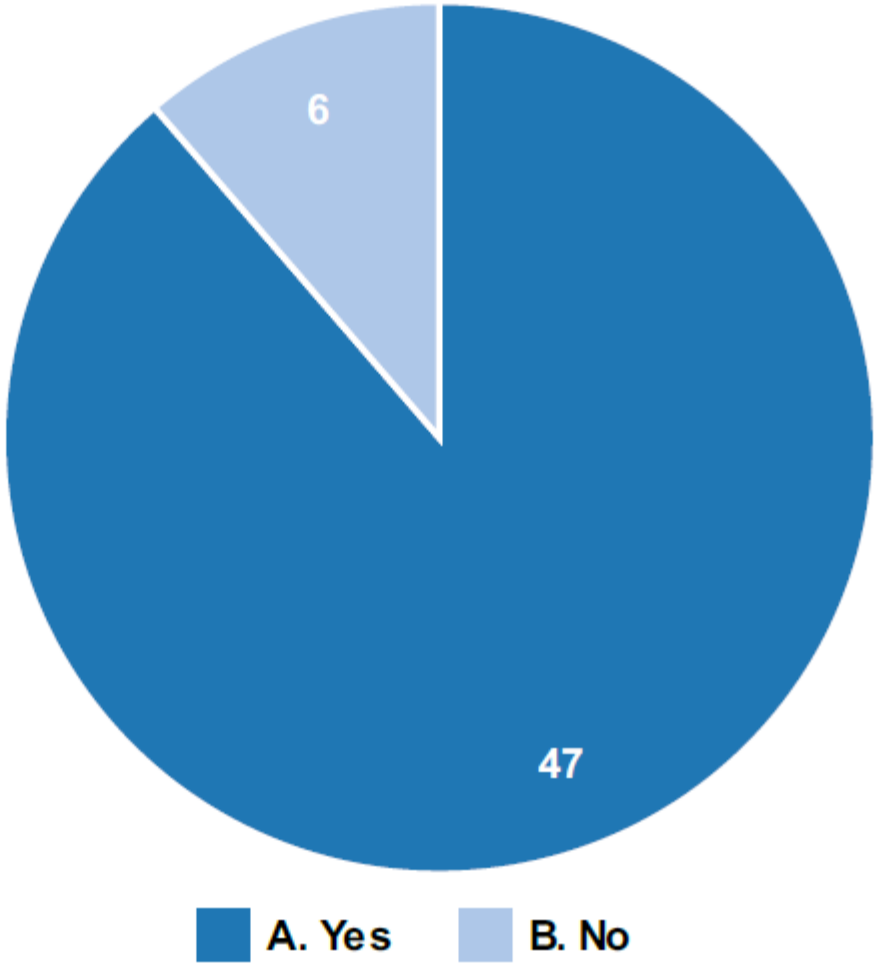
Are You (C-Suite) Informed About The Leaks Of Your Professional AND Personal Credentials (Login= Email + Password) ?



Are You (C-Suite) Aware Of Any Penetration Tests And Their Outcome Conducted On Your Organisation' Systems/Services ?



Is Your Organisation In Contact With Your National CERT ?



Hacktivism … more and more especially environmentalists

20:32 33%

standard.co.uk

Evening Standard.

Lifestyle › ES Magazine

How flygskam (or flight shame) is spreading across Europe

Fears over climate change have led many to rethink the way they travel and, in Sweden, they've even invented a new word for the shame associated with flying

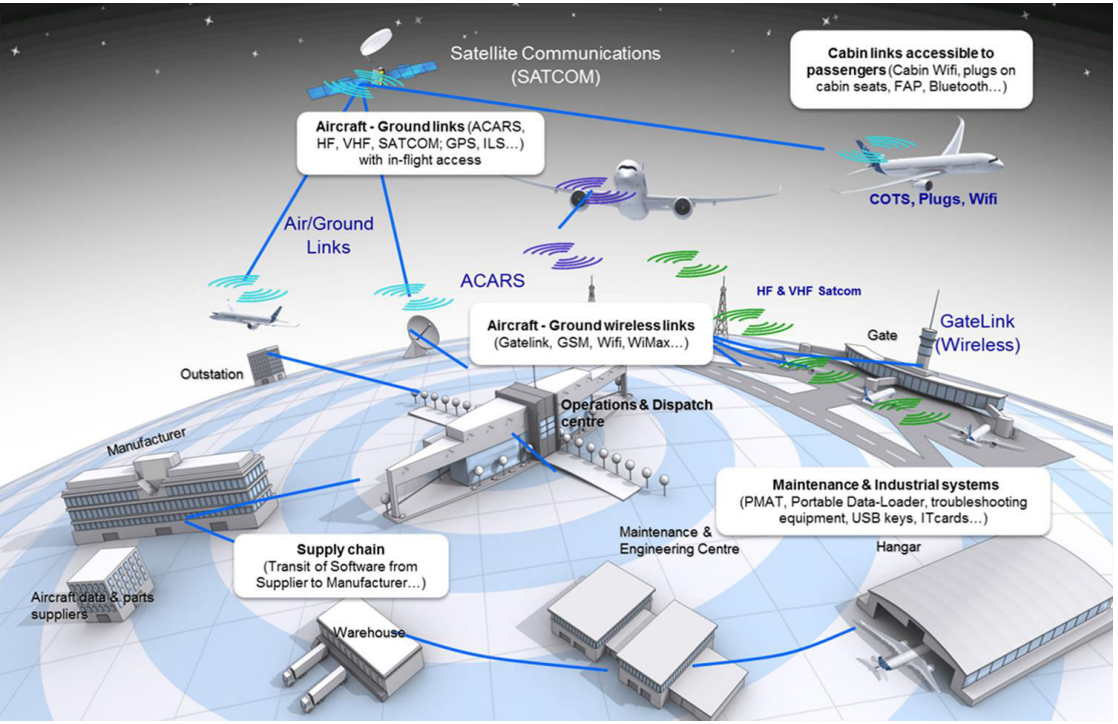
JULIANA PISKORZ | Wednesday 17 April 2019 13:07 |

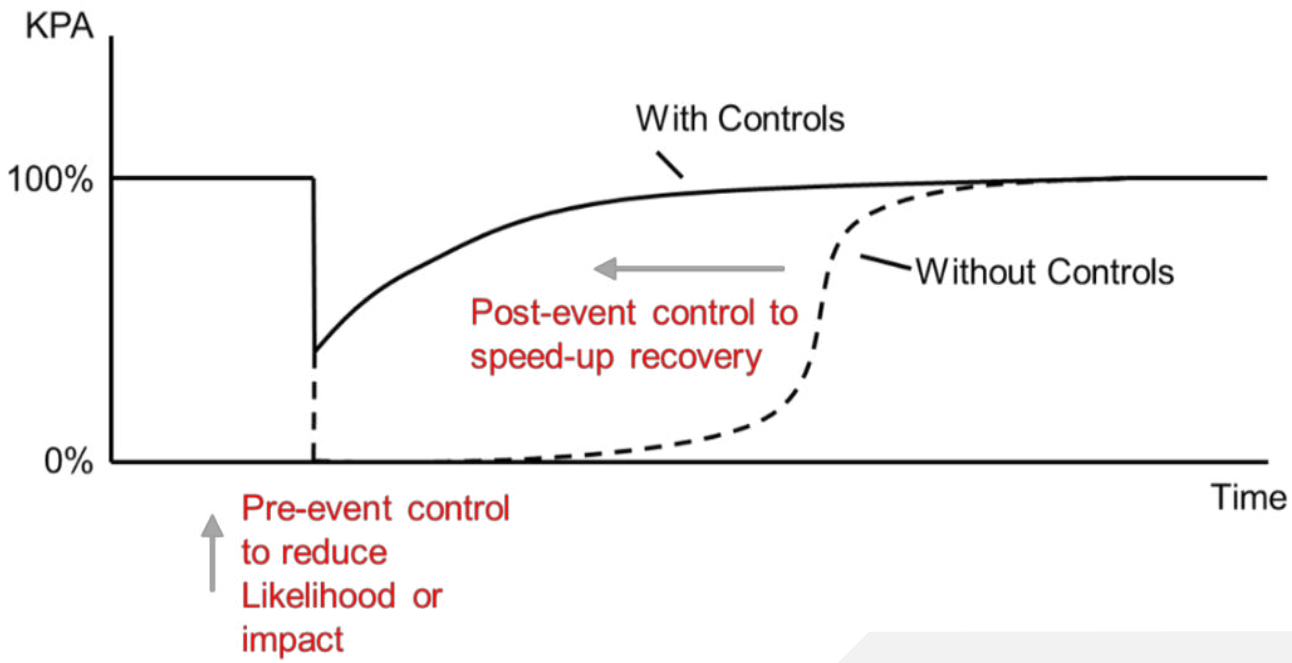
J'aime Click to follow ES Magazine

DISRUPT/DISTURB SERVICE

Can we control those attacks ???

No they **will** occur… only option: become resilient !

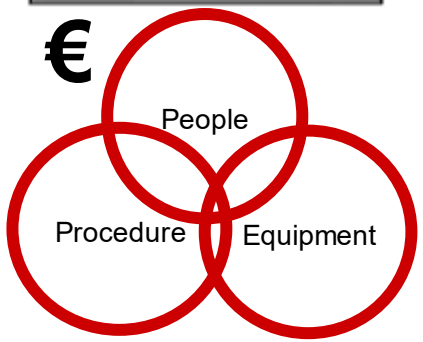




Challenges towards cyber-resilience

Change of culture/ mindset

ISMS



New regulatory framework

GDPR
NIS Directive
EC373/2017

Network:
AM
Guidance
Standards
Training

Safety

Safety:
- Never
a runni
- Open ess
- Stop e asa

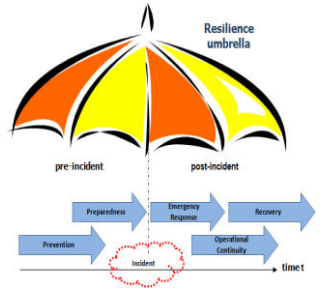
Versus

Security:
- Patch
- Locked access
- Encryption
- Observe attack

Not "if" but "w n"

k-based
roach
elihood ect
xternal nts

=
resilience

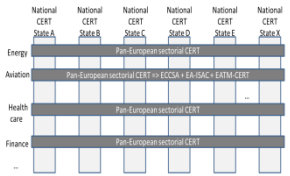


National

Cyber-attacks
ot Nationa

Avia n netwo

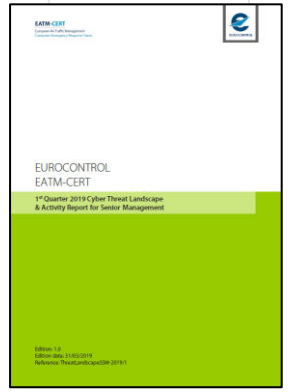
or
oordination:
Pan-European
Sectorial
Civil/MIL



+ TRUST -

Initial set of EATM-CERT services to ANSPs

1. Quarterly cyber threat landscape report for senior management

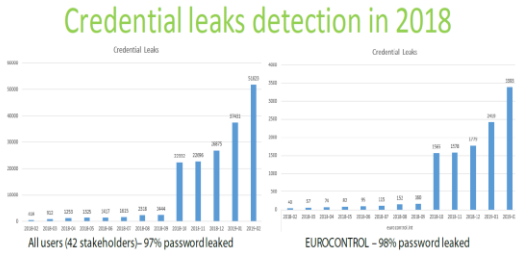


2. Bank transfer fraud

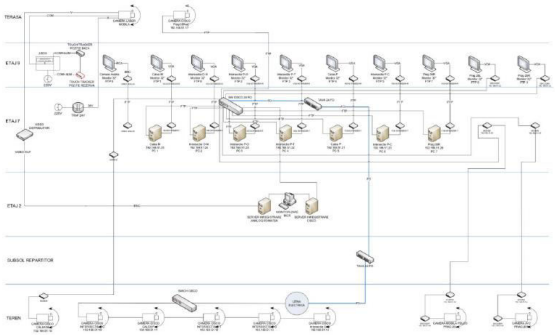
Domain name	Domain closure: status	Attempts count
eurcontrolint.net	Suspended	50
eurocontroladmin.net	Suspended	29
euro-control-int.org	Suspended	13
euro-control.net	Suspended	8
eurocontolint.net	Suspended	5
euro-control.org	Suspended	3
euro-controlinc.com	Suspended	2
eurocontrotint.net	Suspended	2
eurocontroint.net	Suspended	1
eurocontrolints.net	Suspended	1

3. Penetration test of ANSPs environment

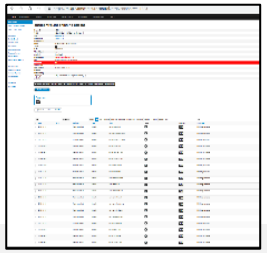
4. Credentials leaks detection



5. Information leaks detection

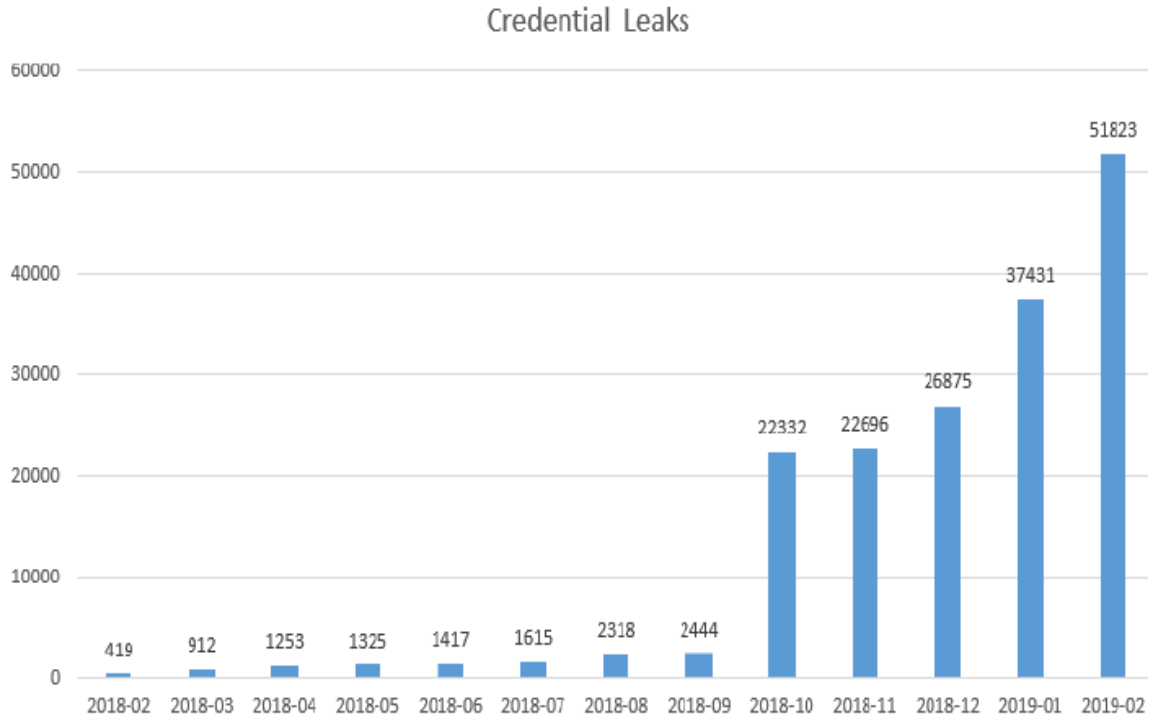


6. CTI and feeds for aviation

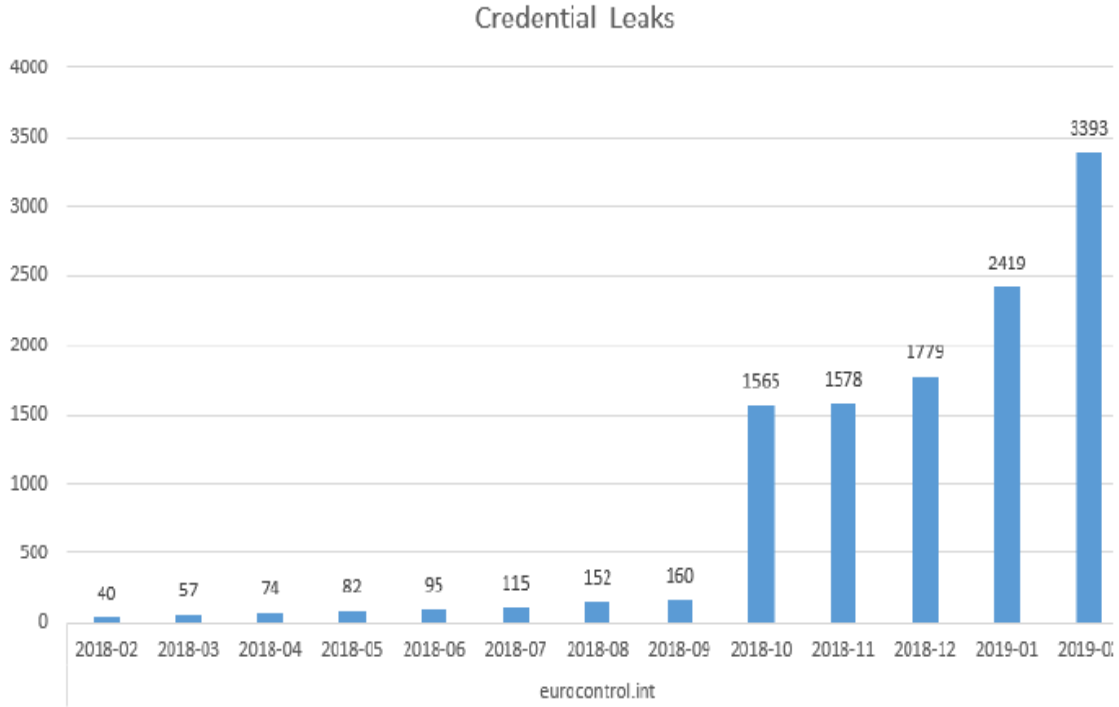


Credentials leaks service

Credential leaks detection in 2018

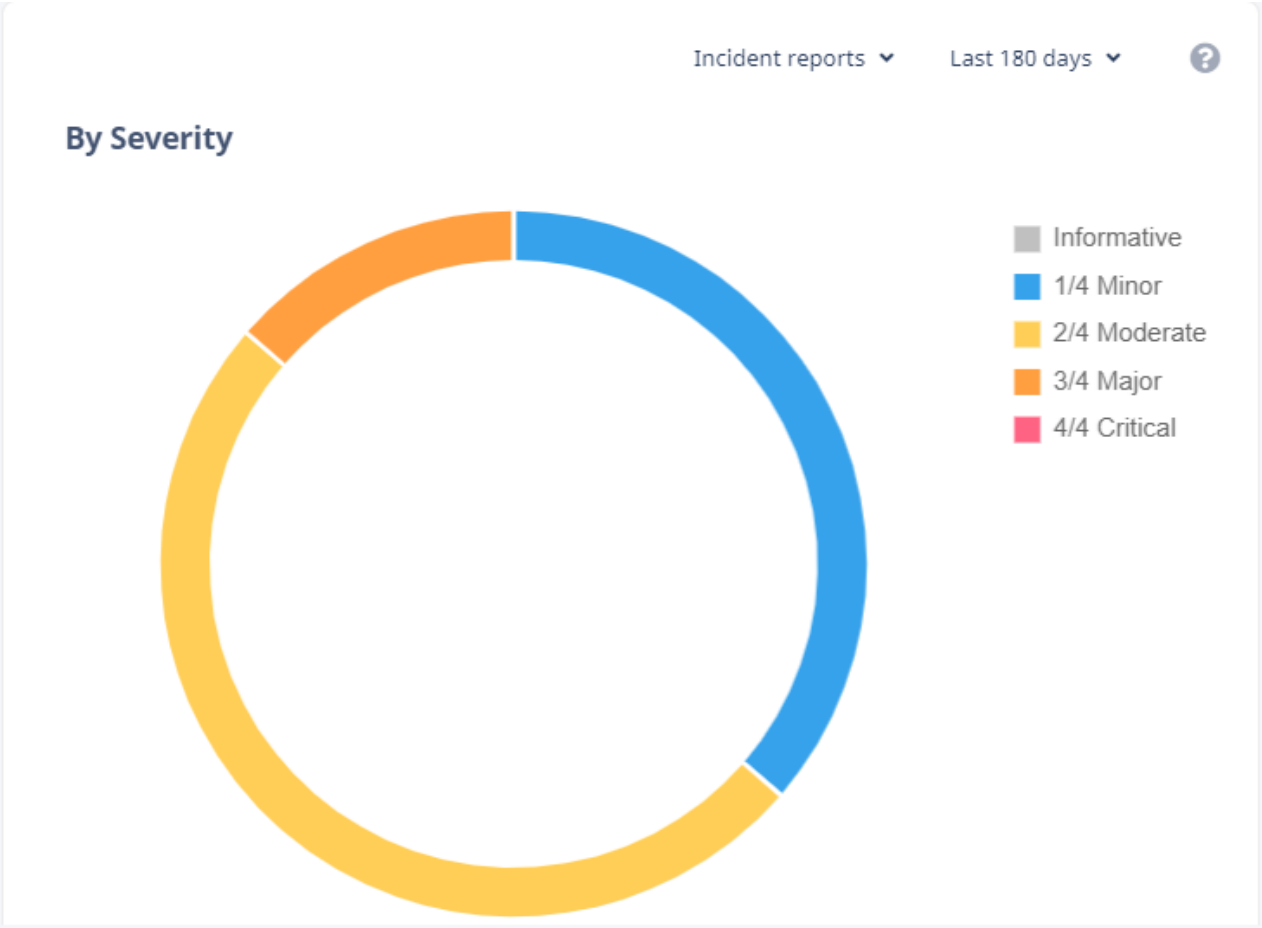


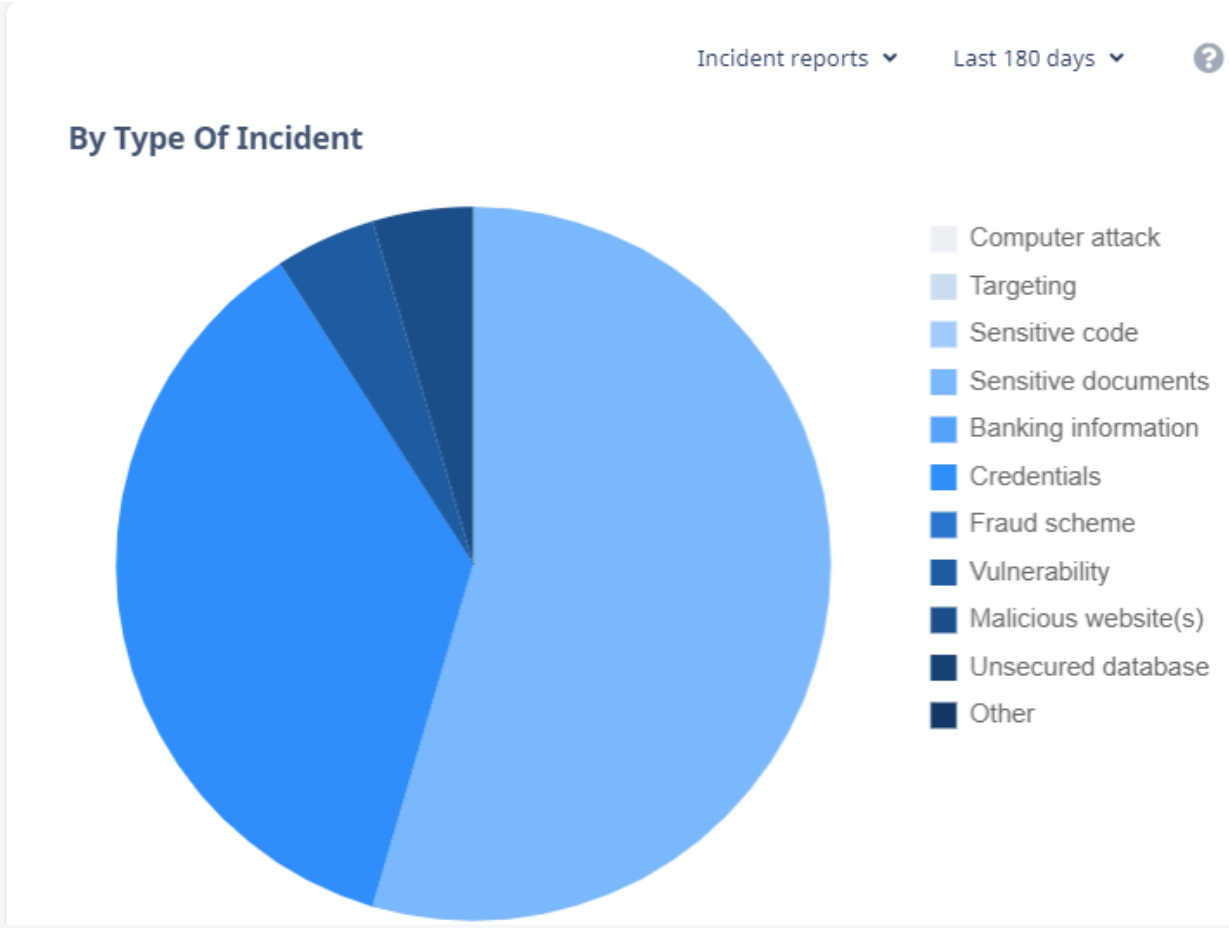
All users (42 stakeholders)– 97% password leaked



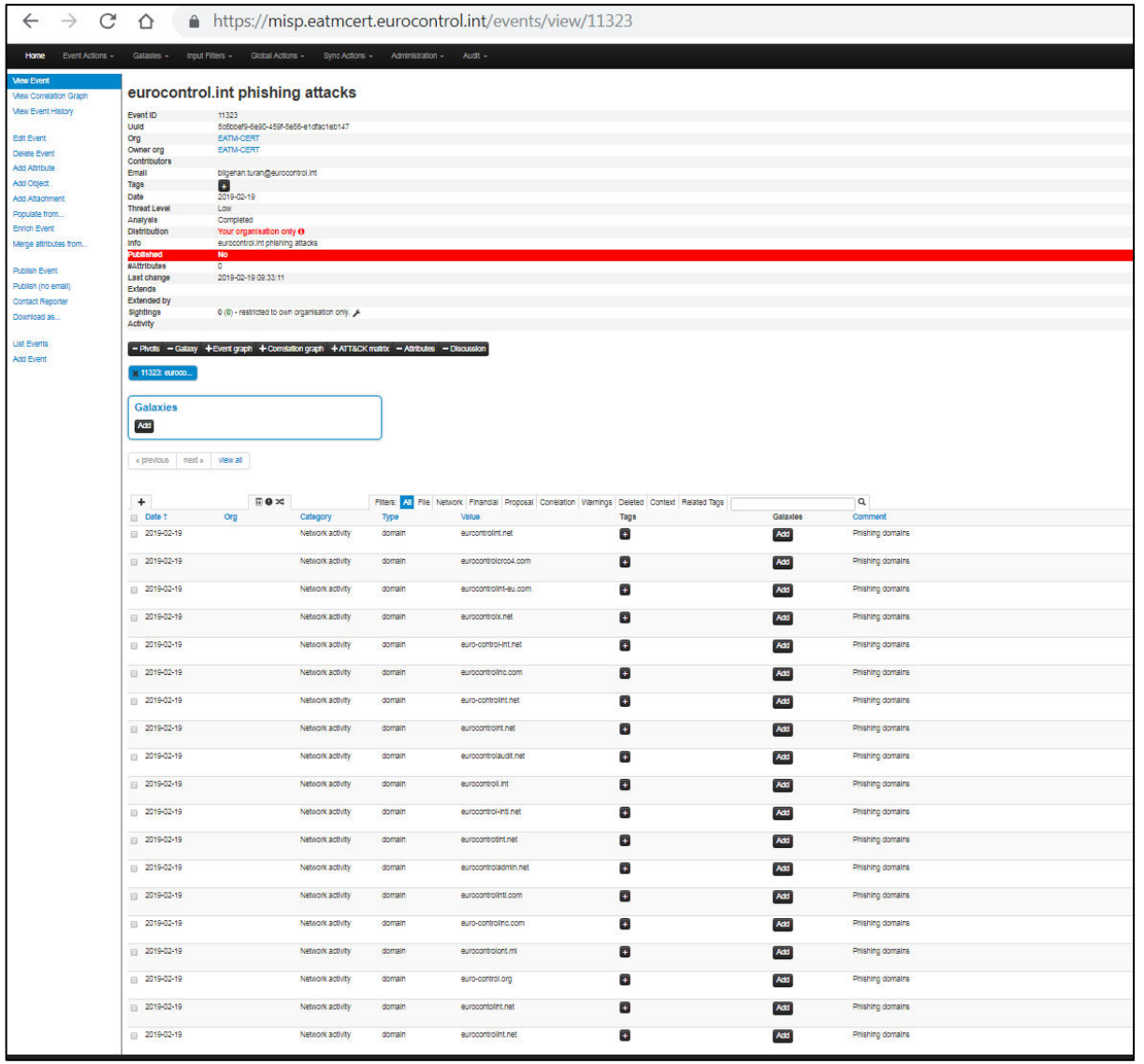
EUROCONTROL – 98% password leaked

Sensitive document leaks





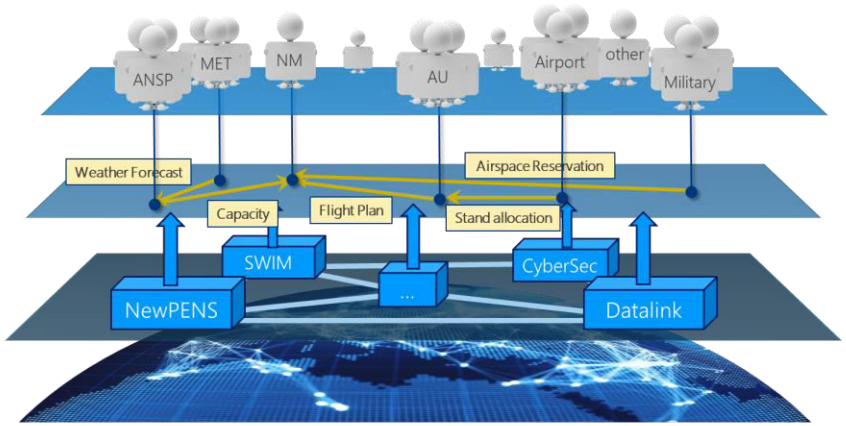
Cyber Threat Intelligence and feeds



MISP Threat Sharing

We are as strong as the weakest link

… so let's work together

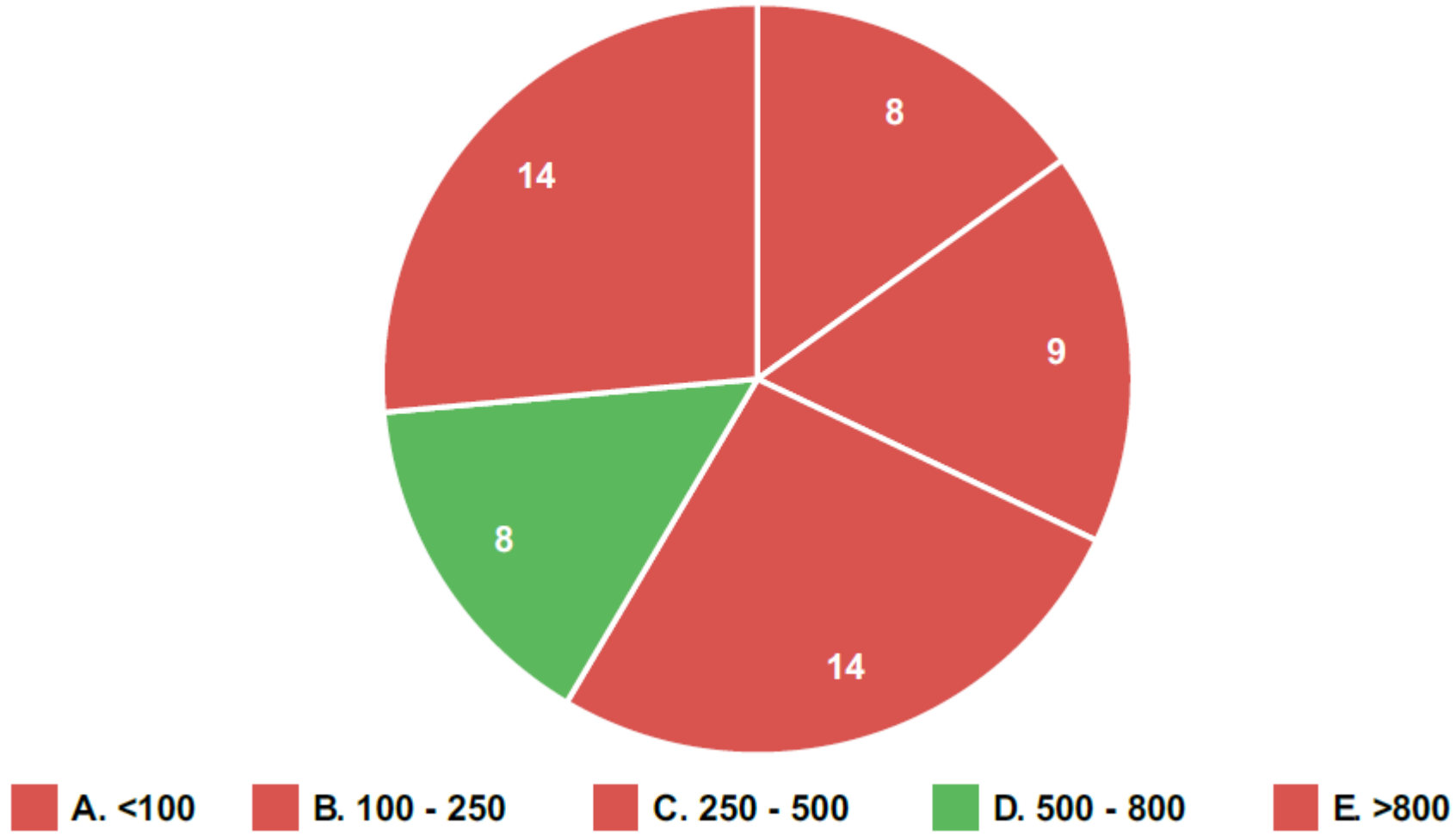


AIR TRAFFIC MANAGEMENT CYBER SECURITY SERVICES

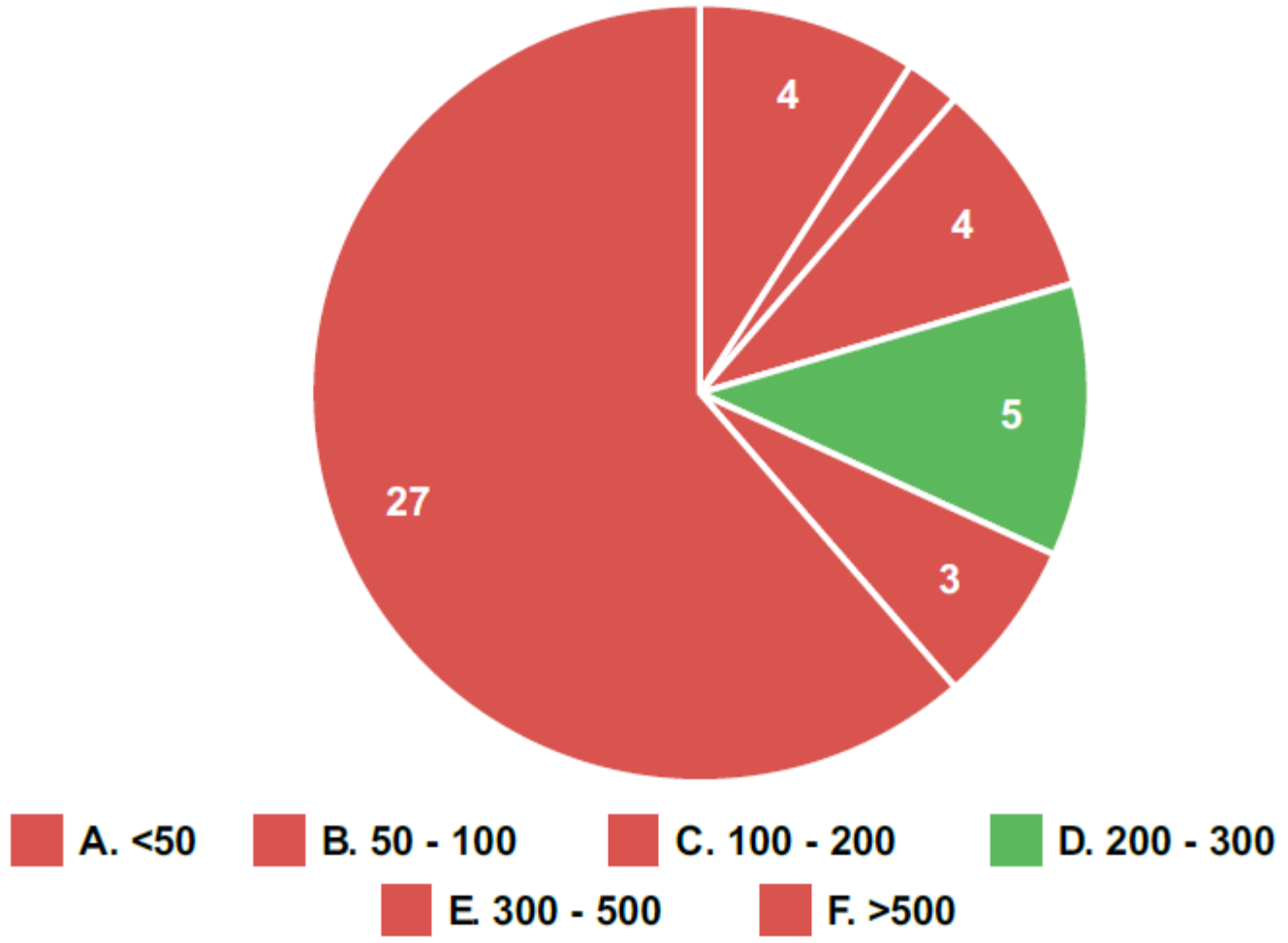
KEEP CALM & CALL EATM-CERT

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

In Your Opinion, How Many Illegitimate Attempts Per Hour To Enter Our Maastricht Upper Area Control Center, Occur?



In Your View, How Many Cyber-Attacks Happen Per Day On Tel-Aviv International Airport?



THANK YOU

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

+32.2.729.46.55