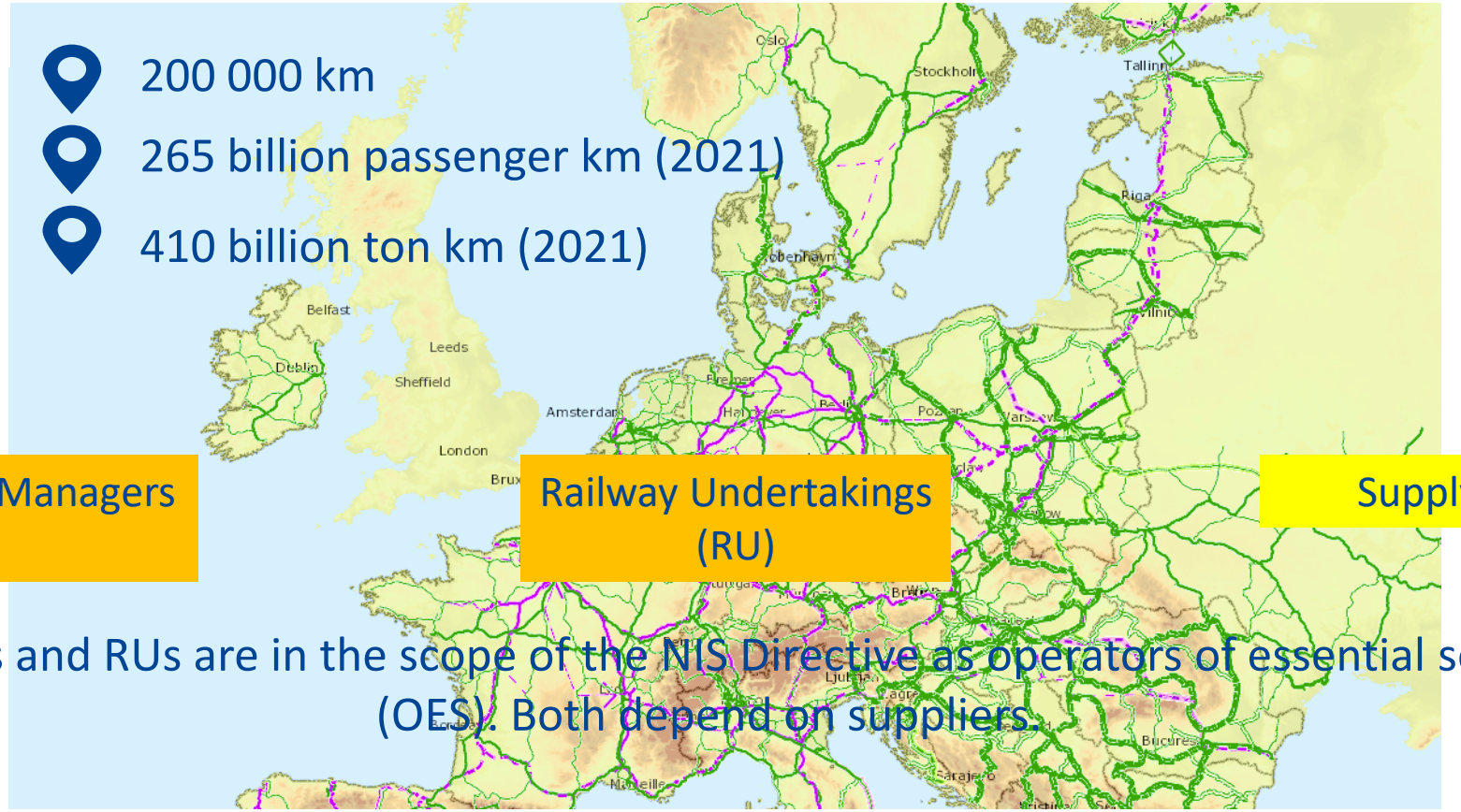

2nd
TRANSPORT CYBERSECURITY
CONFERENCE
European Commission
#TransportCybersecurity

Session 1 - Threat landscape: Navigating cybersecurity challenges in transport

The European Railway Network: a critical asset to be protected against cyber threats

Josef Doppelbauer
Executive Director
ERA

Railway System of the European Union



- 200 000 km
- 265 billion passenger km (2021)
- 410 billion ton km (2021)

Infrastructure Managers (IM)

Railway Undertakings (RU)

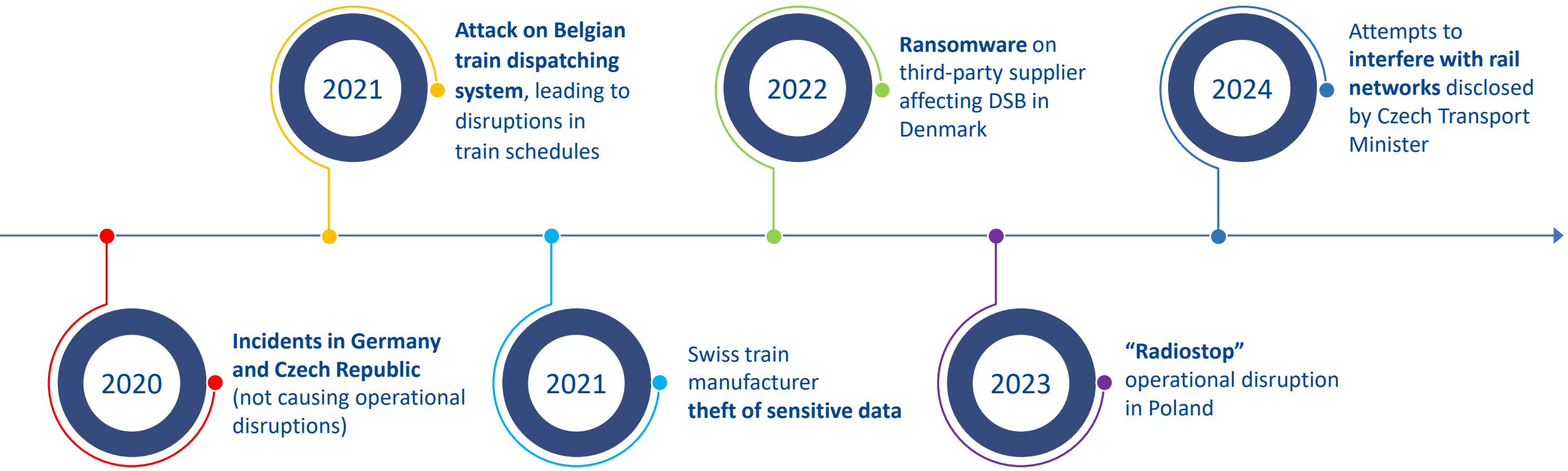
Supply Chain

Both IMs and RUs are in the scope of the NIS Directive as operators of essential services (OES). Both depend on suppliers.

Technical systems in the railway system subject to Cyber Attacks fall in two broad categories:

- IT systems (including ticketing)
- OT (operational technology) systems – implementing also safe control functions, and their communications protocols

The Railway Sector Under Attack?

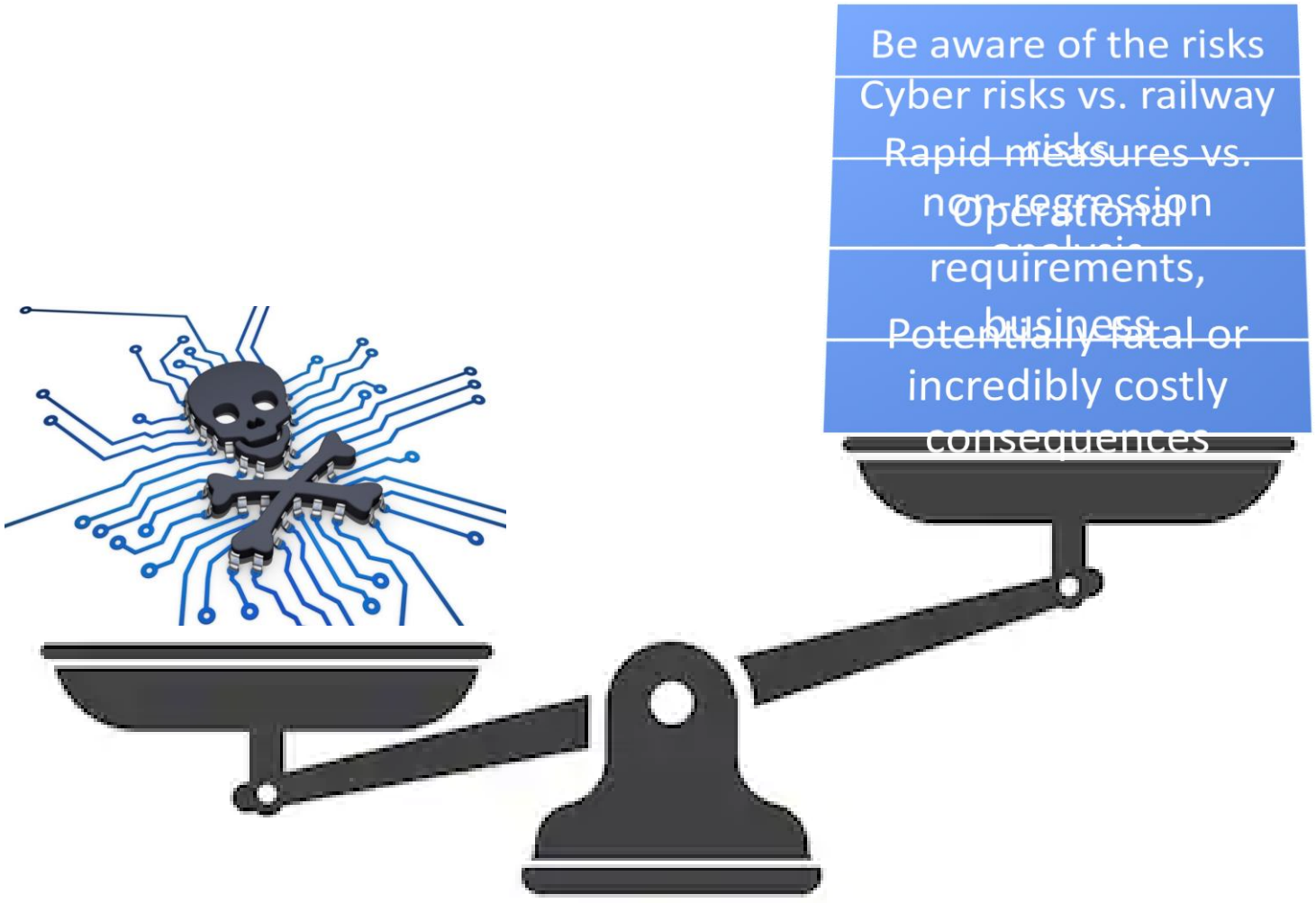


Transformation of the Railway System

Digital technology can be disruptive in **all aspects of the transport chain,** also helping to integrate transport modes (seamless multi-modal transport)

- From analog to **digital systems** - physical vs. digital infrastructure; generalization of electronic components and information and communication technologies, drastically increased **connectivity**
- From proprietary HW to **COTS**; SW: move to **open SW** (IOT devices?); appearance of **cloud-based systems**
- National systems vs. European integration (**cross-border risks**)
- Modal siloes vs. **multimodality** – intercommunication of threats
- Application of **Artificial Intelligence** (AI) techniques

The Need to Balance



What has happened since 2018?

- *More and more incidents are targeting the railway sector: rail stakeholders becoming slowly but surely aware of the cybersecurity threats targeting them*
- *On-going sharing initiatives should be further promoted, and leaders pushed to commit more budget and resources*
- *EU transversal Cybersecurity regulation (NIS2, CRA) is helping as it is overall applicable to railway sector; only few additional requirements related to interoperability need to be covered by TSIs*
- *ERA is closely collaborating with ENISA to ensure adequateness and consistency*
- *Harmonisation is progressing thanks to standardisation effort in IEC, capitalising on CENELEC initial effort: International Standard 63452 will pave the way for a unified methodology about railway cybersecurity risk assessment*
- *Conformity will be the next key topic: compliance of Operators of Essential Services at first, and presumption of conformity for digital products and services then*

Session 1 – Threat landscape: Navigating cybersecurity challenges in transport

Incident reporting and response: developing effective incident response plans for cyber incidents

Paul Bosman
Head of Network Manager
Infrastructure
EUROCONTROL

Supporting European Aviation

EUROCONTROL

Incident reporting and response:

Developing effective incident response plans for cyber incidents

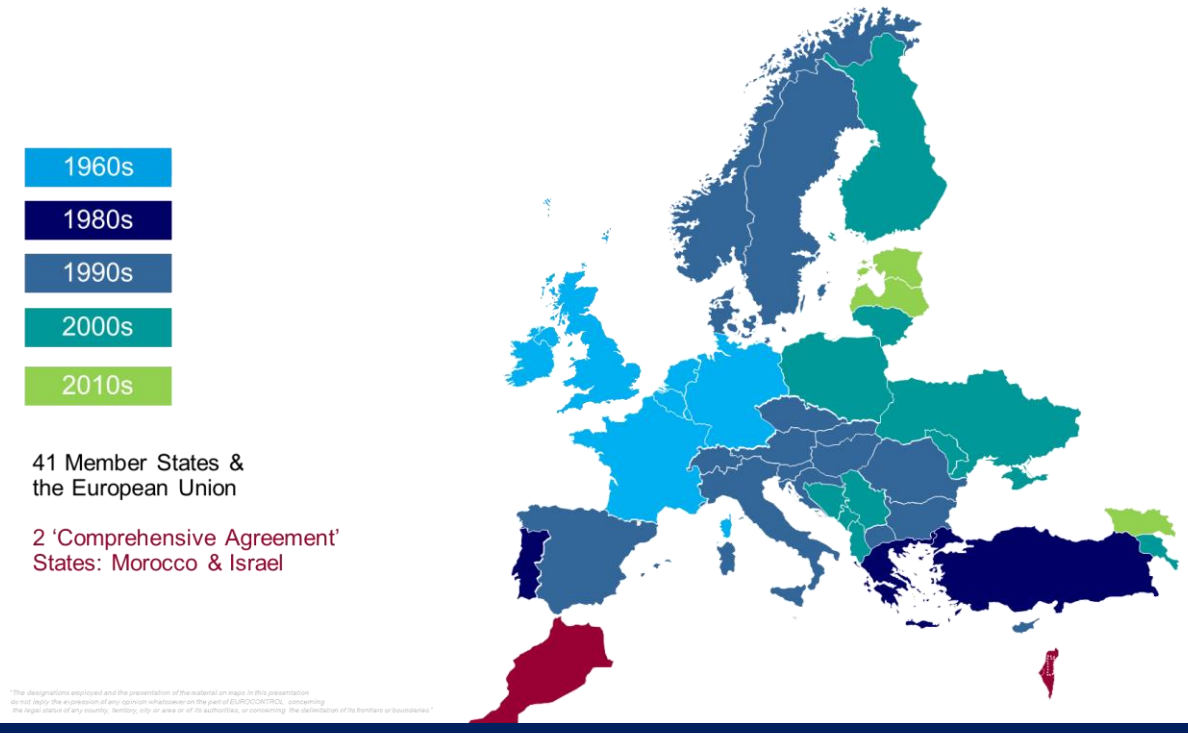
Paul BOSMAN
Head of ATM Infrastructure Division
EUROCONTROL, Network Manager

sesar

sesar

NETWORK MANAGER

EUROCONTROL



- Manage 11 Million flights/year
- Collect ~9Bn€ of route & terminal charges/year
- Support realisation of Single European Sky

European Network key challenges: Growth, sustainability & resilience

EUROCONTROL – Cyber intelligence eco-system

Aviation Stakeholders

Aviation Supply chain

National CERTs/cyber security centers

Cyber intelligence Providers

EUROPOL

A-ISAC

ENISA

EE-ISAC

NATO

ER-ISAC

OT-ISAC

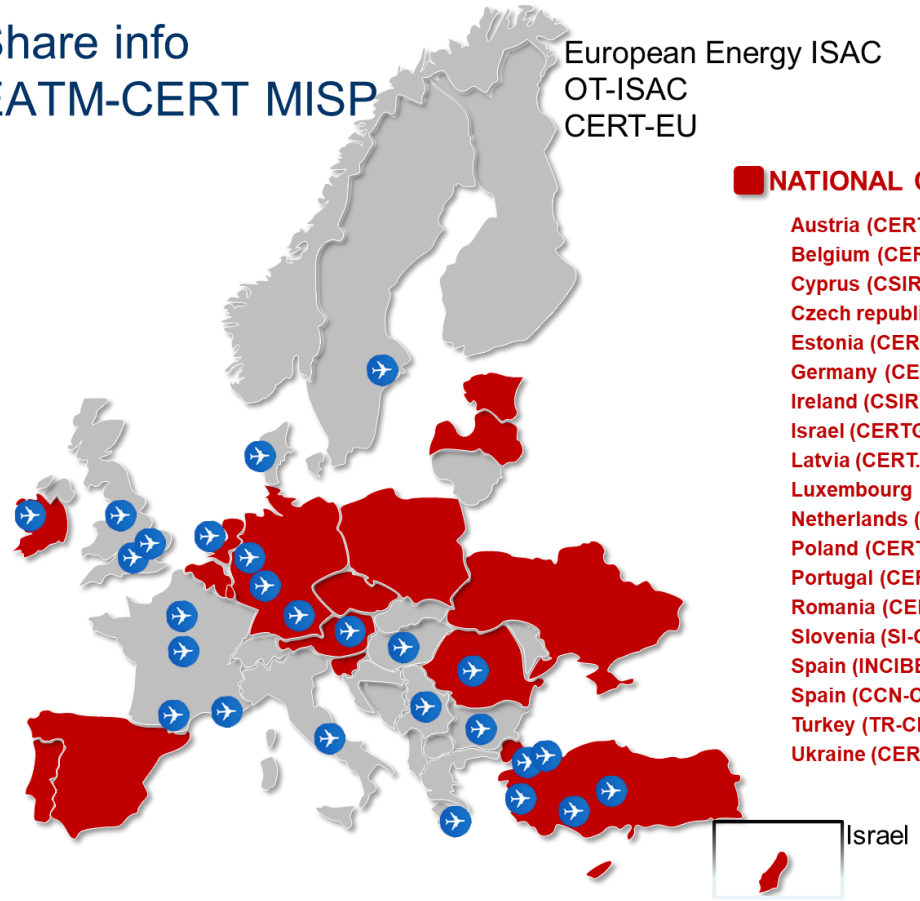
TF-CSIRT
Trusted Introducer

Aviation stakeholders

Austria – Austrocontol (ANSP)
Belgium – DHL
Bulgaria - BULATSA (ANSP)
Denmark - NAVIAIR (ANSP)
Finland – Fintraffic (ANSP)
France - CERT-AIRBUS A/C
France - Groupe ADP
France - DSNA
France – Air Caraïbes
Germany - DLH – Lufthansa Group
Germany - Frankfurt Airport
Germany – Munich airport
Greece - HANSP
Hungary - HungaroControl (ANSP)
International - IATA
International – AMADEUS
Ireland – Shannon airport
Ireland – Dublin Airport
Italy - Aeroporto Di Roma
Mexico - Aero Mexico Airlines
Netherlands - Schiphol Airport
Portugal – SATA (airline)
Romania - CAA-RO
Serbia - SMATSA (ANSP)
Sweden - Swedavia (airports)
Turkey - CERT-THY (Turkish Airlines)
Turkey - DHMI (ANSP)
Turkey - IGA Istanbul Airport
Turkey - Celebi Ground ops
Turkey – SGIA Airport
UK - British Airways
UK - Heathrow Airport
UK – Manchester Airport Group

Share info
EATM-CERT MISP

European Energy ISAC
OT-ISAC
CERT-EU



NATIONAL CERT/NCSC

Austria (CERT.at)
Belgium (CERT.be)
Cyprus (CSIRT-CY)
Czech republic (CSIRT.cz)
Estonia (CERT-EE)
Germany (CERT-Bund)
Ireland (CSIRT-IE)
Israel (CERTGOVIL)
Latvia (CERT.LV)
Luxembourg (CIRCL)
Netherlands (NCSC-NL)
Poland (CERT.GOV.PL)
Portugal (CERT-PT)
Romania (CERT-RO)
Slovenia (SI-CERT)
Spain (INCIBE-CERT)
Spain (CCN-CERT)
Turkey (TR-CERT)
Ukraine (CERT-UA)

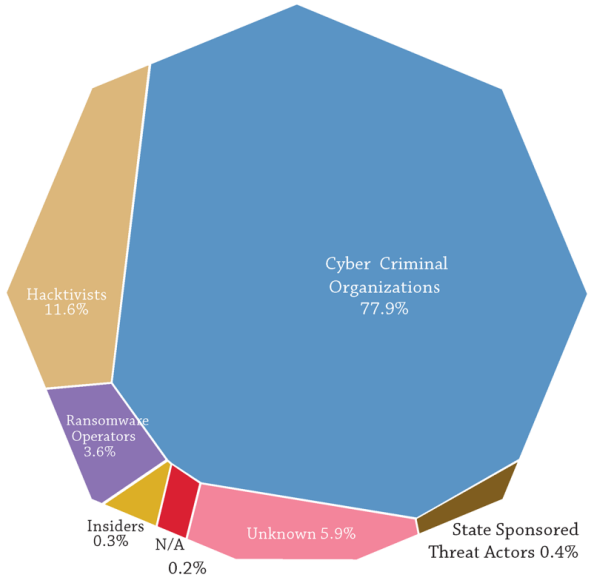
All as strong as the weakest link

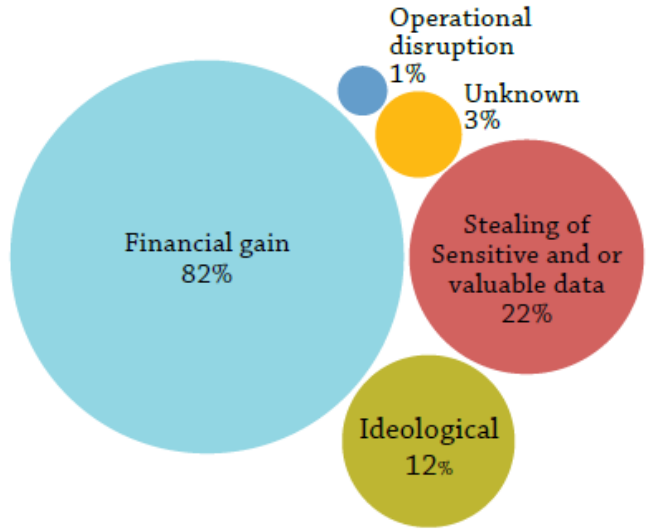
Know the aviation cyber threat landscape

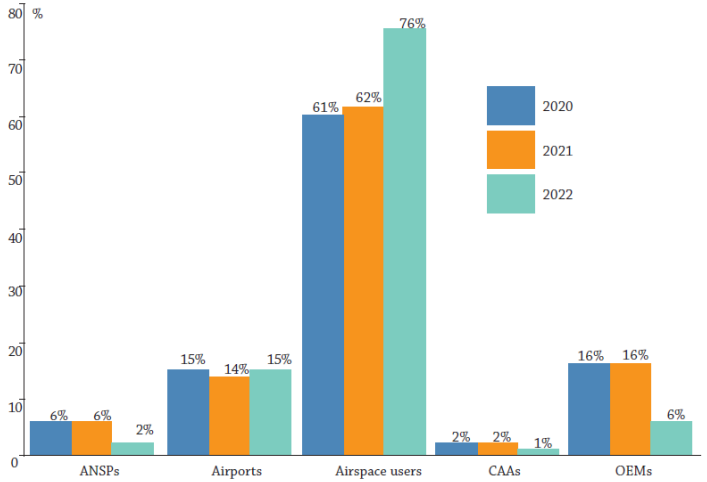
TLP:GREEN

- **Cyber-criminals** Bns€ of losses /year
- Conflicts (Ukraine + Gaza) :
  - ~680 **DDoS** on aviation in 2023 (world)
  - 62 DDoS in January 2024 (Europe)
- **Ransomware**: ~2/week
- **Basic** threats there (e.g. phishing)

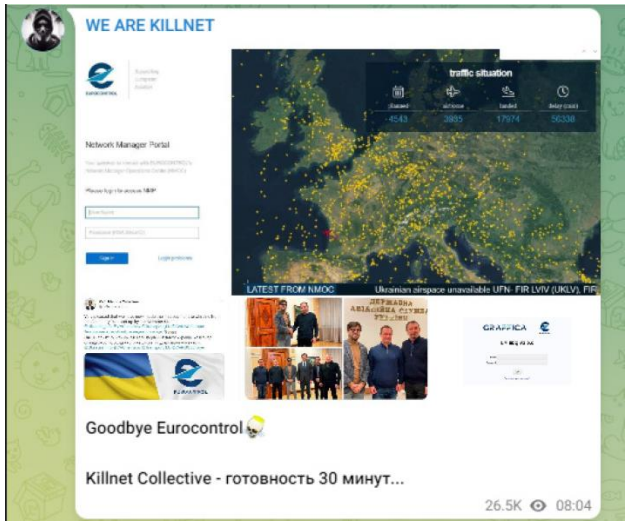
No impact on safety of flights



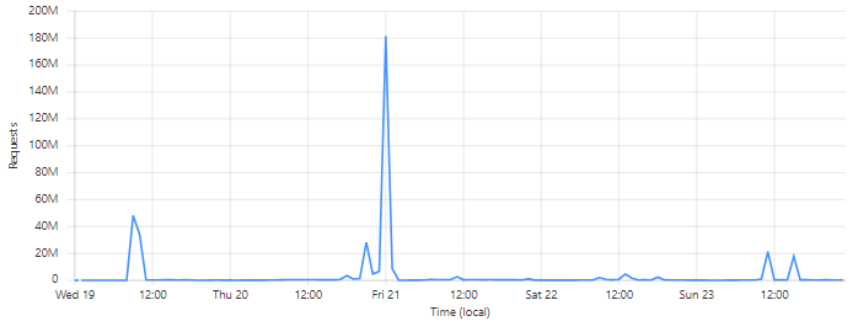




DDoS attacks on EUROCONTROL



Total requests
403.28M



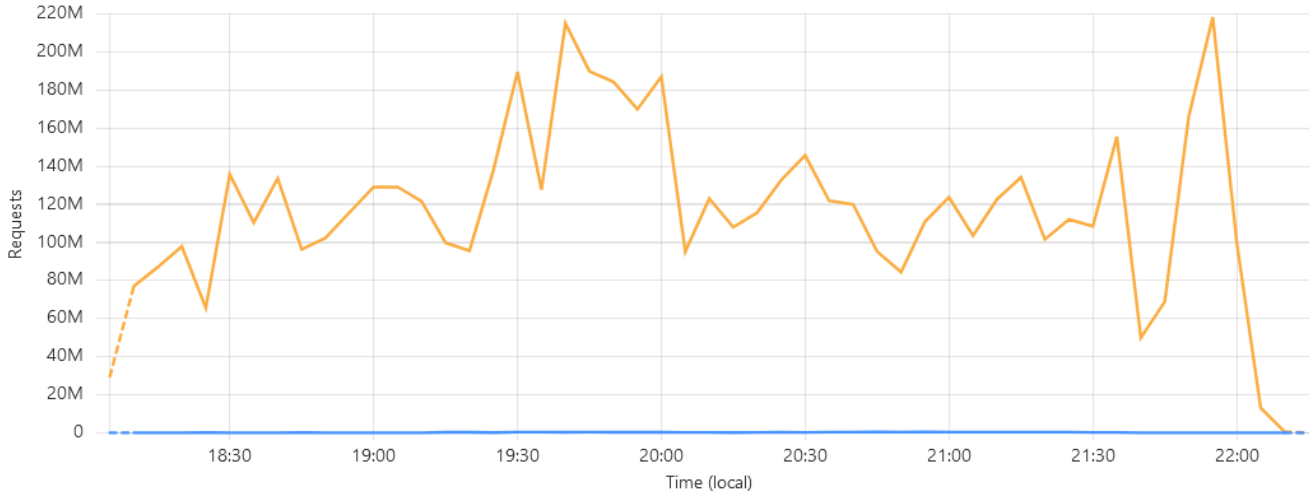
DDoS – April 2023 – 100 hours

TLP:GREEN

Requests summary

Served by | Cache status | Country | Host | HTTP method | Path | ...

Total	Served by Cloudflare	Served by origin
5.87B	5.86B	8.98M



DDoS – March 2024

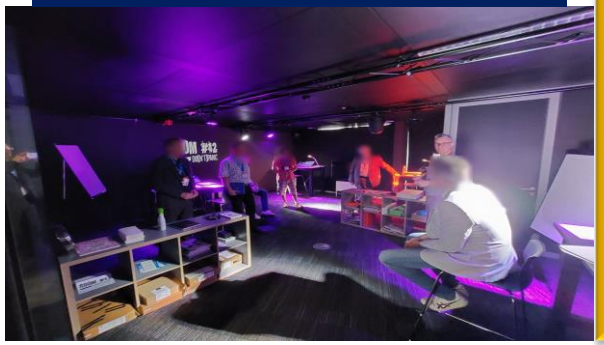
No shortage of lessons learned

Get the organisation ready and committed

Senior management commitment

Information Security Management System
Part-IS compliance

Training
Cyber crisis management



Always plan ahead

It wasn't raining when Noah built the ark

Technical training: Capture The Flag

Session 2 - Understanding the cybersecurity regulatory framework

Management of information security risks impacting aviation safety

Gian Andrea Bandieri

Section Manager

Cybersecurity in Aviation

& Emerging Risks

EASA

EASA
European Union Aviation Safety Agency

Management of information security risks impacting aviation safety

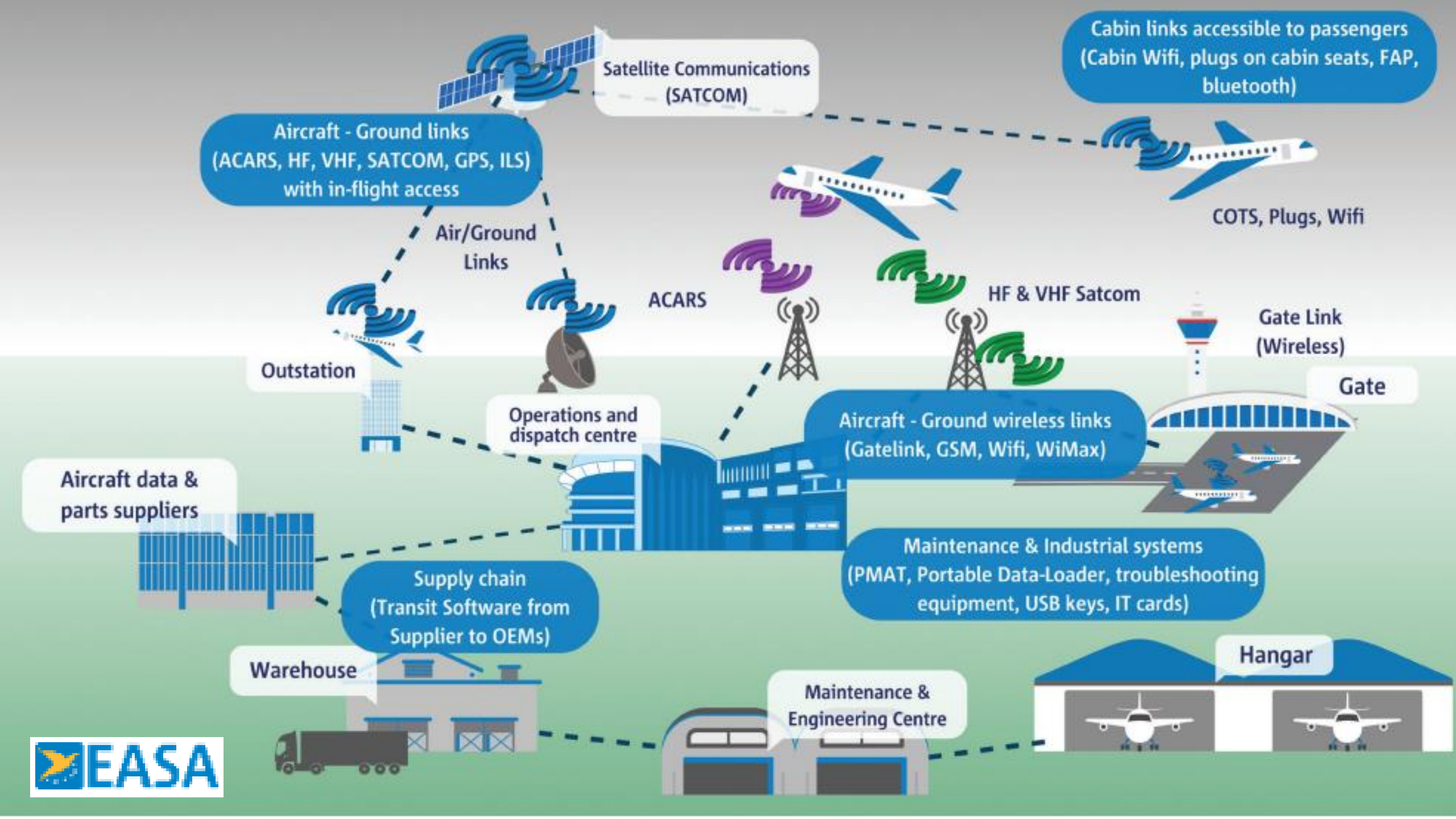
Gian Andrea Bandieri

Section Manager Cybersecurity in Aviation and Emerging Risks

2 May 2024

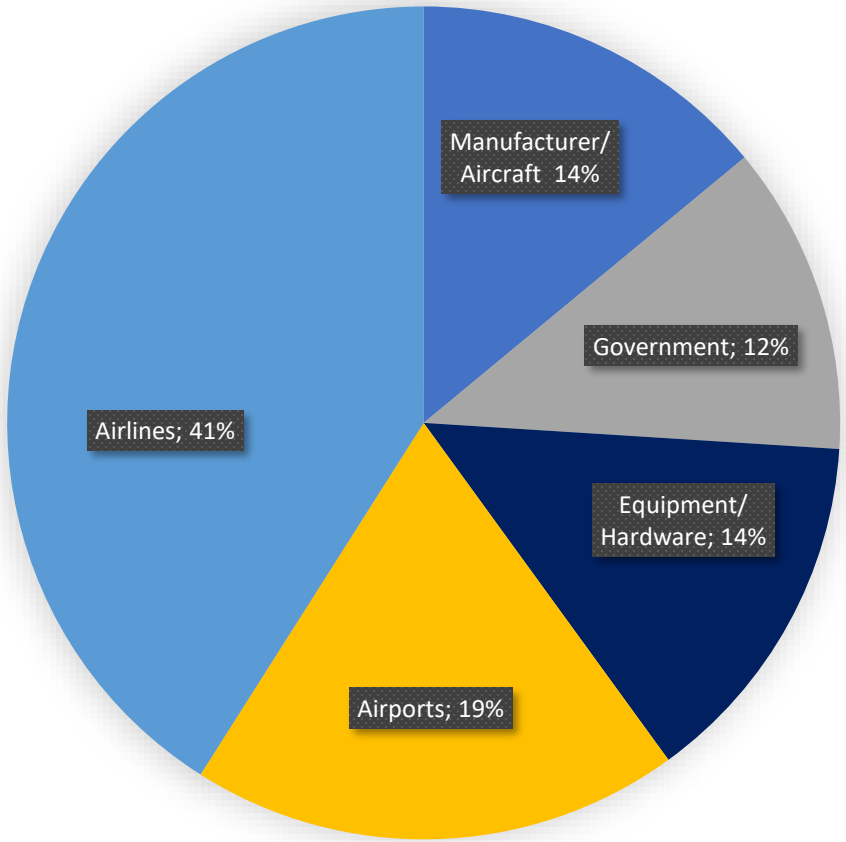
Your safety is our mission.

An Agency of the European Union

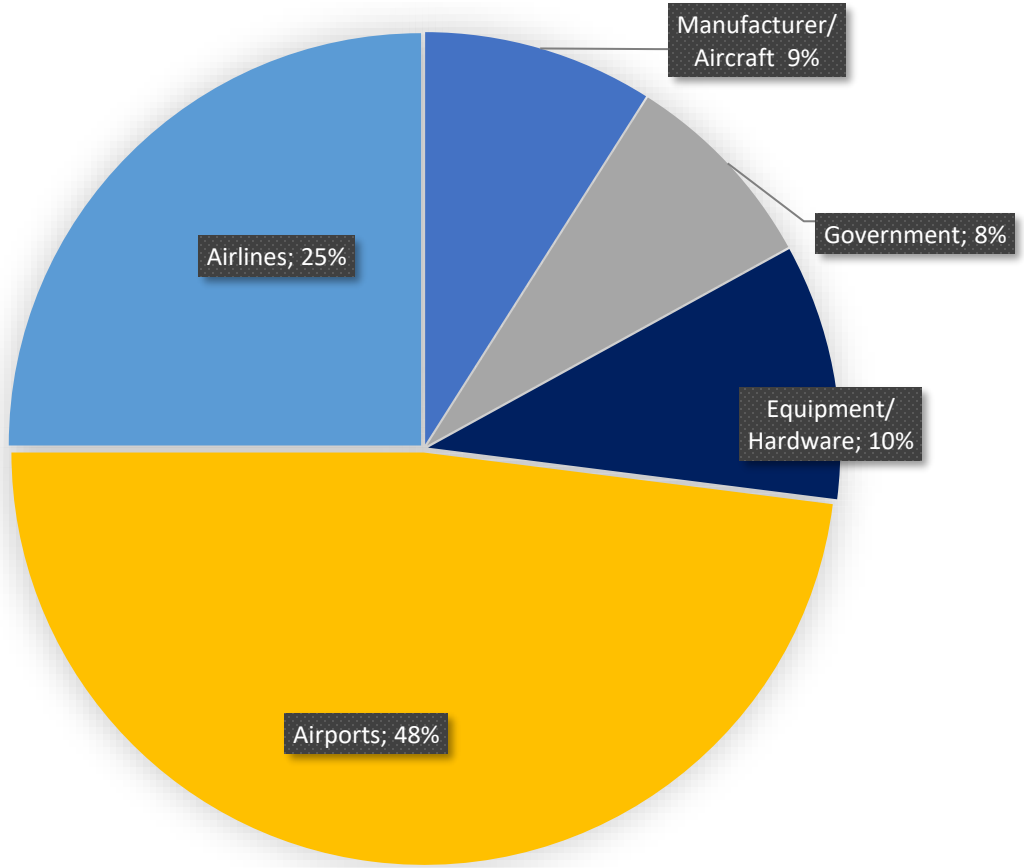

Satellite Communications (SATCOM)
Cabin links accessible to passengers (Cabin Wifi, plugs on cabin seats, FAP, bluetooth)
Aircraft - Ground links (ACARS, HF, VHF, SATCOM, GPS, ILS) with in-flight access
COTS, Plugs, Wifi
Air/Ground Links
ACARS
HF & VHF Satcom
Gate Link (Wireless)
Outstation
Gate
Operations and dispatch centre
Aircraft - Ground wireless links (Gatelink, GSM, Wifi, WiMax)
Aircraft data & parts suppliers
Maintenance & Industrial systems (PMAT, Portable Data-Loader, troubleshooting equipment, USB keys, IT cards)
Supply chain (Transit Software from Supplier to OEMs)
Warehouse
Hangar
Maintenance & Engineering Centre
EASA

Cybersecurity risks matter to you – EU data

116 attacks by target organisation in 2022



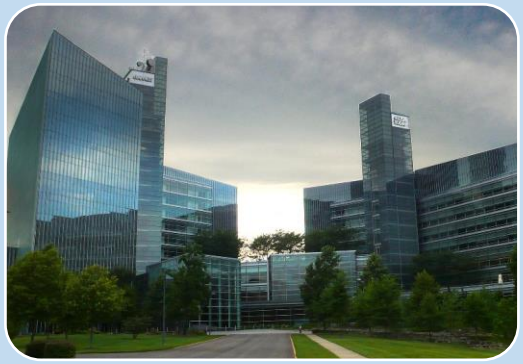
175 attacks by target organisation in 2023



Making EU aviation cyber resilient

Products (Aircrafts, Engines, …)

- Transition from case by case approach to mandatory on all products now done.
- Requirements incorporated into CS and AMC in July 2020



Organisations (People, Processes)

- **Part-IS** Regulations published in October 2022 and February 2023
- AMC/GM published on 12 July 2023

Information Sharing

- Create a community to
  - Share knowledge
  - Perform Analysis
  - Collaborate
  - Reinforce the system

Capacity building & Research

- To have competent and well aware workforce
- To monitor the current Threat Landscape
- To understand the future Threat Landscape

What we want to achieve with Part-IS

Objective	Protect the aviation system from information security risks **with potential impact on aviation safety**
Scope	Information and communication technology systems and data used by Approved Organisations and Authorities for civil aviation purposes
Activity	- **identify and manage** information security risks related to information and communication technology systems and data used for civil aviation purposes; - **detect** information security events, identifying those which are considered information security incidents; and - **respond** to, and **recover** from, those information security incidents

Proportionate to the impact on aviation safety

Part-IS ISMS is inspired by existing Framework and Regulations

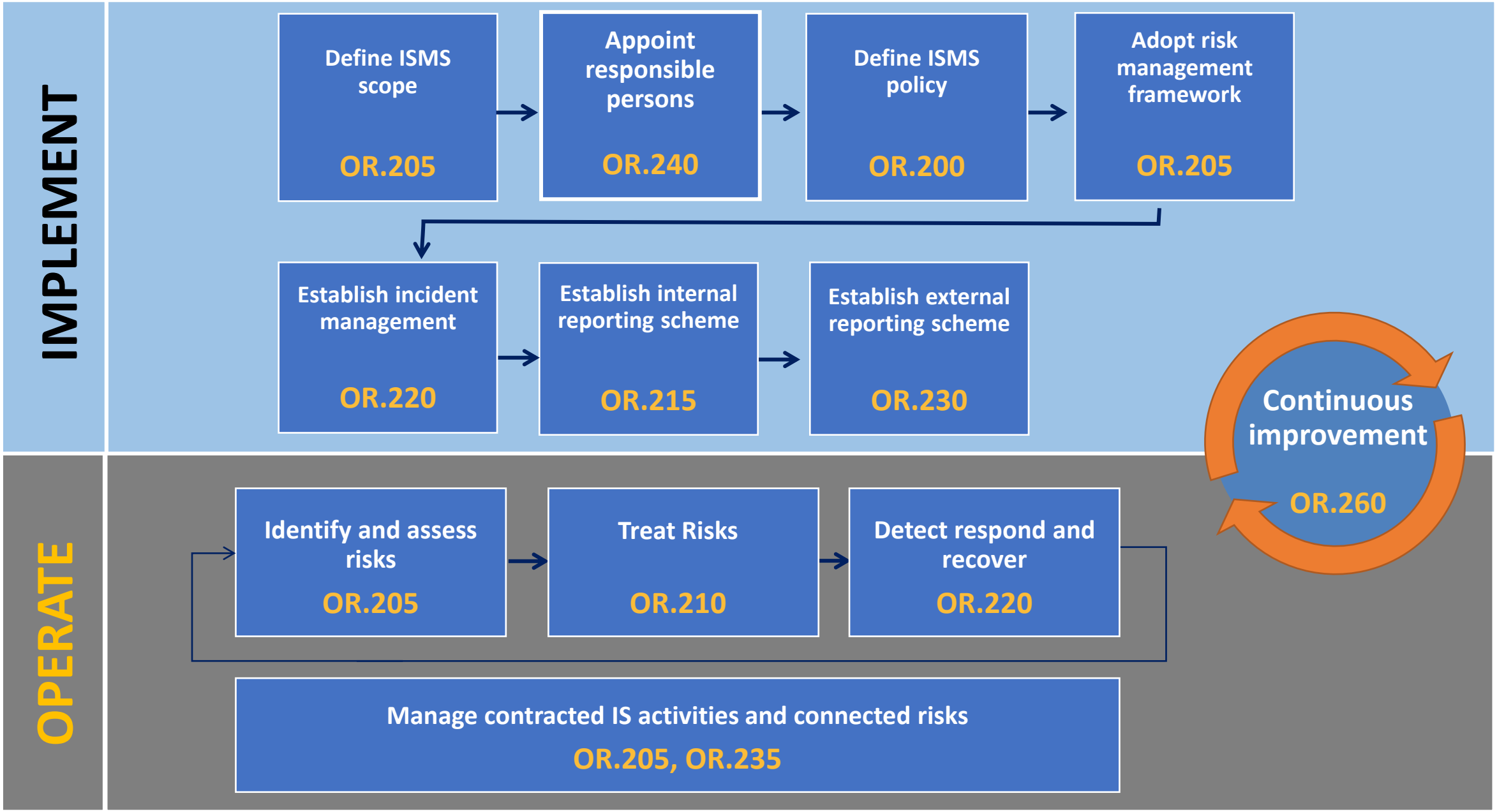
IS.OR.200 Policy on information security	IS.OR.205 IS Risk Assessment	IS.OR.210 Information Security Risk Treatment	IS.OR.220 Detection, Response, Recovery of Incidents
IS.OR.215 IS Internal Reporting Scheme	IS.OR.230 IS external reporting scheme	Implement authority measures as immediate reaction to Incidents or Vulnerabilities	IS.OR.225 Response to findings by the authority
IS.OR.235 Contracting of IS management activities	IS.OR.240 Personnel requirements	IS.OR.245 Record-keeping	IS.OR.200 Compliance monitoring

IS.OR.250 Information security management manual (ISMM)

IS.OR.255 Changes to the information security management system

IS.OR.260 Continuous improvement

Legend: NIST Framework | ISO 2700x | EASA Basic Reg. | Occurrence Reporting Reg.


IMPLEMENT
Define ISMS scope
OR.205
Appoint responsible persons
OR.240
Define ISMS policy
OR.200
Adopt risk management framework
OR.205
Establish incident management
OR.220
Establish internal reporting scheme
OR.215
Establish external reporting scheme
OR.230
Continuous improvement
OR.260
OPERATE
Identify and assess risks
OR.205
Treat Risks
OR.210
Detect respond and recover
OR.220
Manage contracted IS activities and connected risks
OR.205, OR.235

EASA
European Union Aviation Safety Agency

Part-IS Implementation Workshop 2024

Cologne, November 7 - 8

SAVE THE DATE

Registration opens in July 2024!

Your safety is our mission.

An Agency of the European Union

EASA
European Union Aviation Safety Agency

Thank you for your attention

Join our Community:

Contact us at:
cybersec@easa.europa.eu

easa.europa.eu/connect

20 YEARS

Your safety is our mission.

An Agency of the European Union

Session 2 - Understanding the cybersecurity regulatory framework

EU Railway regulatory framework in support of cybersecurity

Thomas Chatelet

Project Officer

ERTMS

ERA

Status update on cybersecurity

02.05.24 | 2nd Transport Cybersecurity Conference, Brussels

EUROPEAN UNION AGENCY FOR RAILWAYS

Photo: Adobe Srock / by _Serjiob74

EUROPEAN UNION AGENCY FOR RAILWAYS

Cybersecurity @ERA

Regulation considerations

- Monitor relevant activities related to **cybersecurity in the railway context**
- Cover safety requirements of the rail system, e.g. the assessment of **safety consequences originated by security threats**
- Reflect the above in **Technical Specifications for Interoperability** and **Common Safety Methods**

Cooperation building

- Close relationship with **ENISA** and **European Commission**
- Cross-fertilisation with **EASA** and **EMSA** to develop a transport cybersecurity policy
- Dialogue with **National Cybersecurity Agencies** (e.g. ANSSI, BSI)
- Support **sector-led Information Sharing initiatives**

EUROPEAN UNION AGENCY FOR RAILWAYS

Cybersecurity risk assessment

To cover safety requirements of the rail system, including the assessment of safety consequences originated by security threats

- **Security threats based on physical access to assets outside of scope**
- **ERTMS inherent threats considered**
- **Safety AND Security Management Systems**

Process oriented

Acknowledgement of cybersecurity issues that might influence safety

Rail Standards

Reference to IEC/CENELEC Standards with provisions on cybersecurity: 63452 / 50126, 50129, 50159, 50701

CSM-RA application guide

Reference in the CSM for Risk Assessment Application Guide to Cybersecurity risk assessment

Cybersecurity for interoperability

Scope of application

Relevance of cybersecurity not pertinent for all TSIs (e.g. Noise)

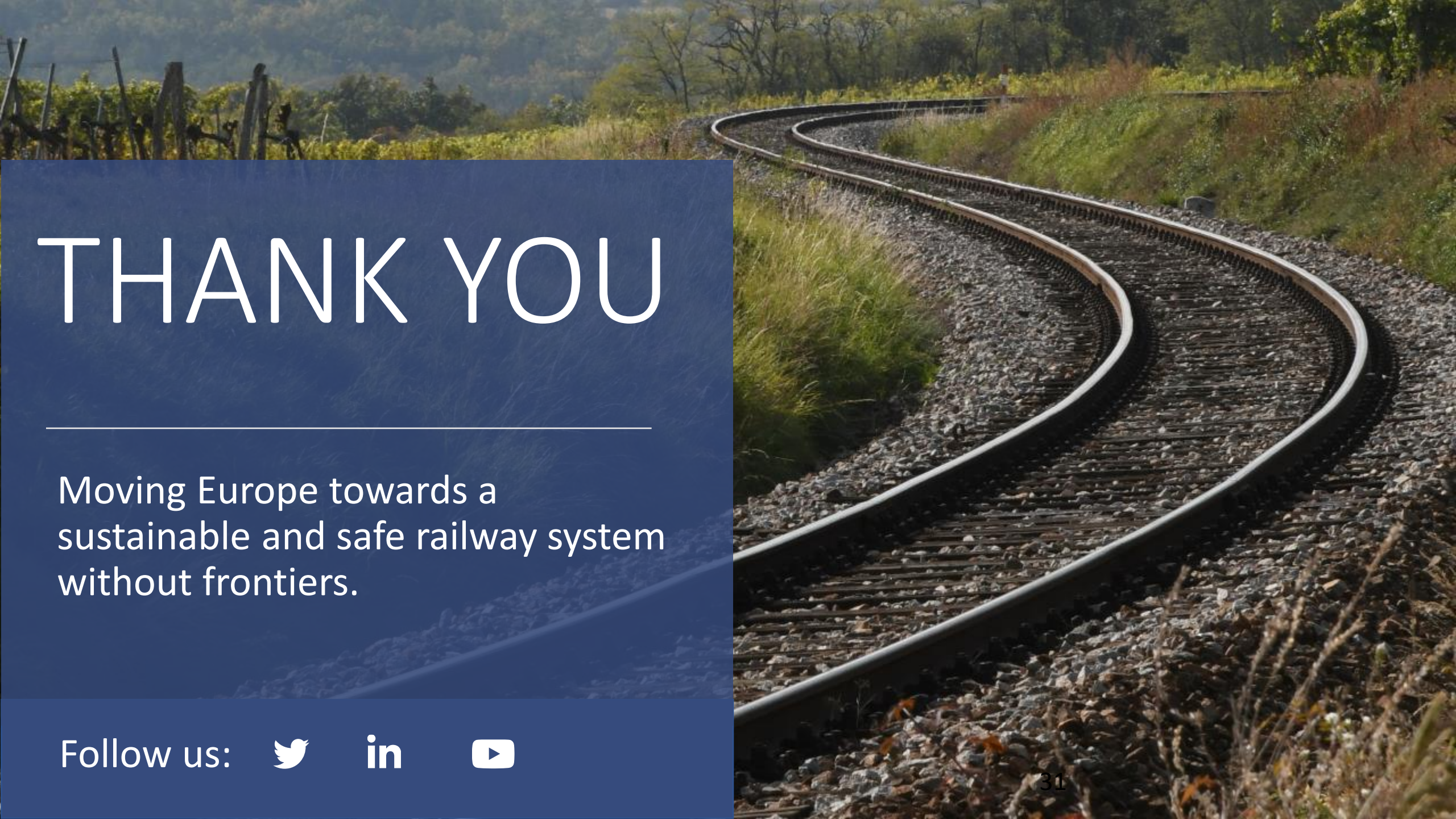
Guiding principles

High level design requirement versus specific/component requirement

Thorough review needed

Support from rail stakeholders and ENISA

ERA-ENISA collaboration



THANK YOU

Moving Europe towards a sustainable and safe railway system without frontiers.

Follow us:

Session 3 - Cybersecurity in transport design, supply chains and emerging technologies

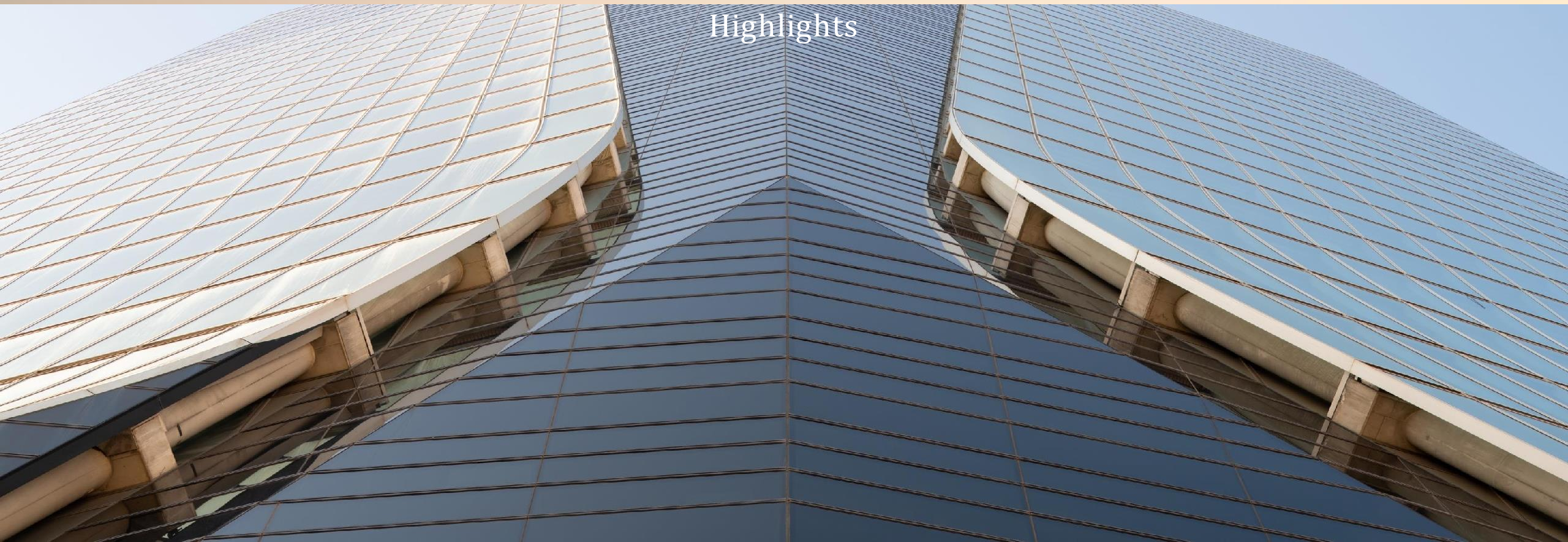
Cybersecurity in supply chains and third parties to prevent vulnerabilities

Omar Marouf
Head of Group Cybersecurity
Risk Management
CMA-CGM

BETTER WAYS CMA CGM

CMA CGM GROUP

Highlights



The CMA CGM Group

The CMA CGM Group, led by Rodolphe Saadé, is a global player
in sea, land, air and logistics solutions,
employing more than 155,000 staff members worldwide,
including nearly 6,000 in Marseille, where its head office is located.

CMA CGM, is a family-owned company, driven by a unique set of human and entrepreneurial values, and implements a long-term, coherent and ambitious business strategy.

GLOBAL PLAYER

IN SEA, LAND, AIR AND LOGISTICS SOLUTIONS

Our transport and logistics activities

SHIPPING SOLUTIONS

CMA CGM · APL · ANL · CNC · MERCOSUL LINE

END-TO-END LOGISTICS SOLUTIONS

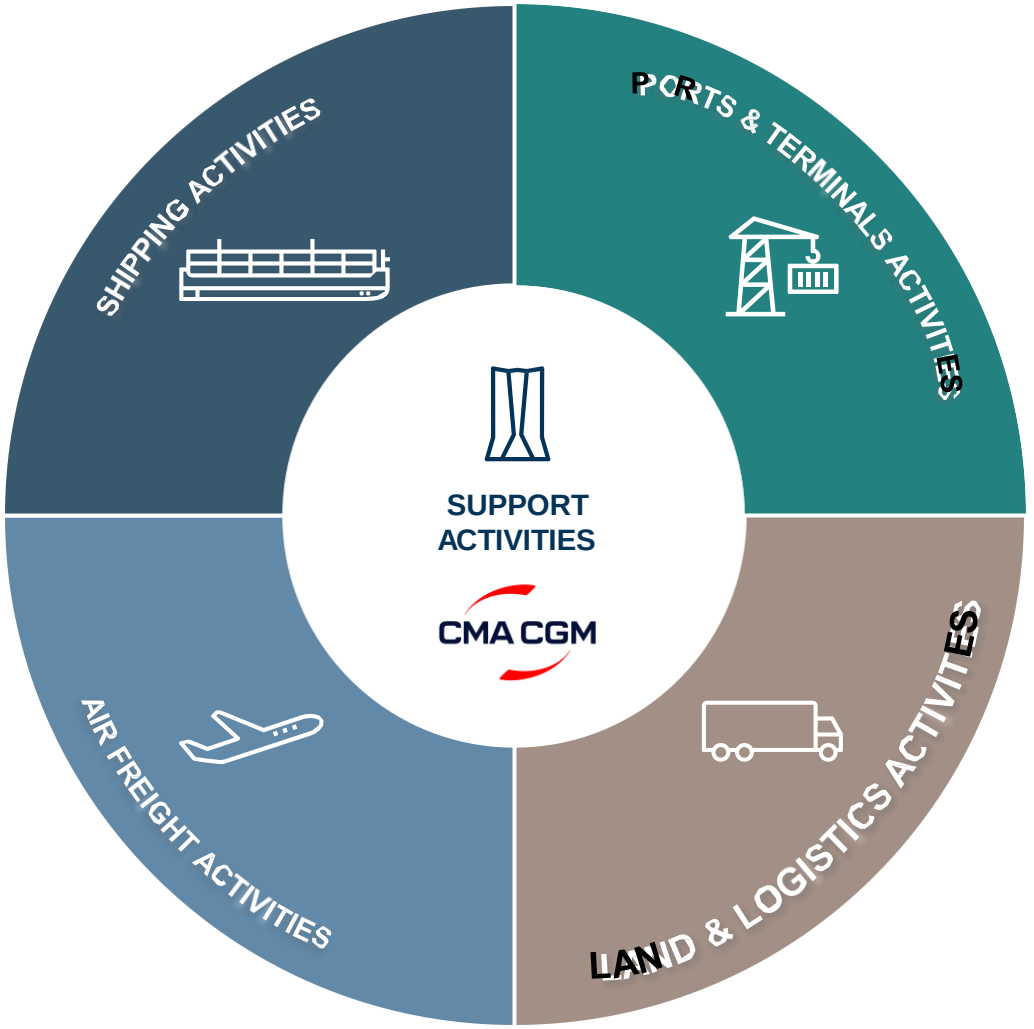
CEVA LOGISTICS · colis privé

AIR FREIGHT SOLUTIONS

CMA CGM AIR CARGO

TERMINALS

CMA TERMINALS · TERMINAL LINK · CMA BEIRUT TERMINAL



APL: North America, ANL: Pacific, CNC: Intra-Asia, Mercosul Line: South America

Our global presence

160
countries

+620
vessels

750
warehouses

6
aircraft
already in operation
12 in 2026

+400
offices

+420
Ports served
across 5
continents

13,304
Crew members

+20 M
TEU transported (2023)

277
shipping services

+50
port
terminals
in operation
in 28 countries

+155,000
staff members
worldwide

Shipping

CMA CGM has one of the world's largest shipping networks.
Goods are carried in containers on our CMA CGM, APL, ANL, CNC and Mercosul Lines ships.

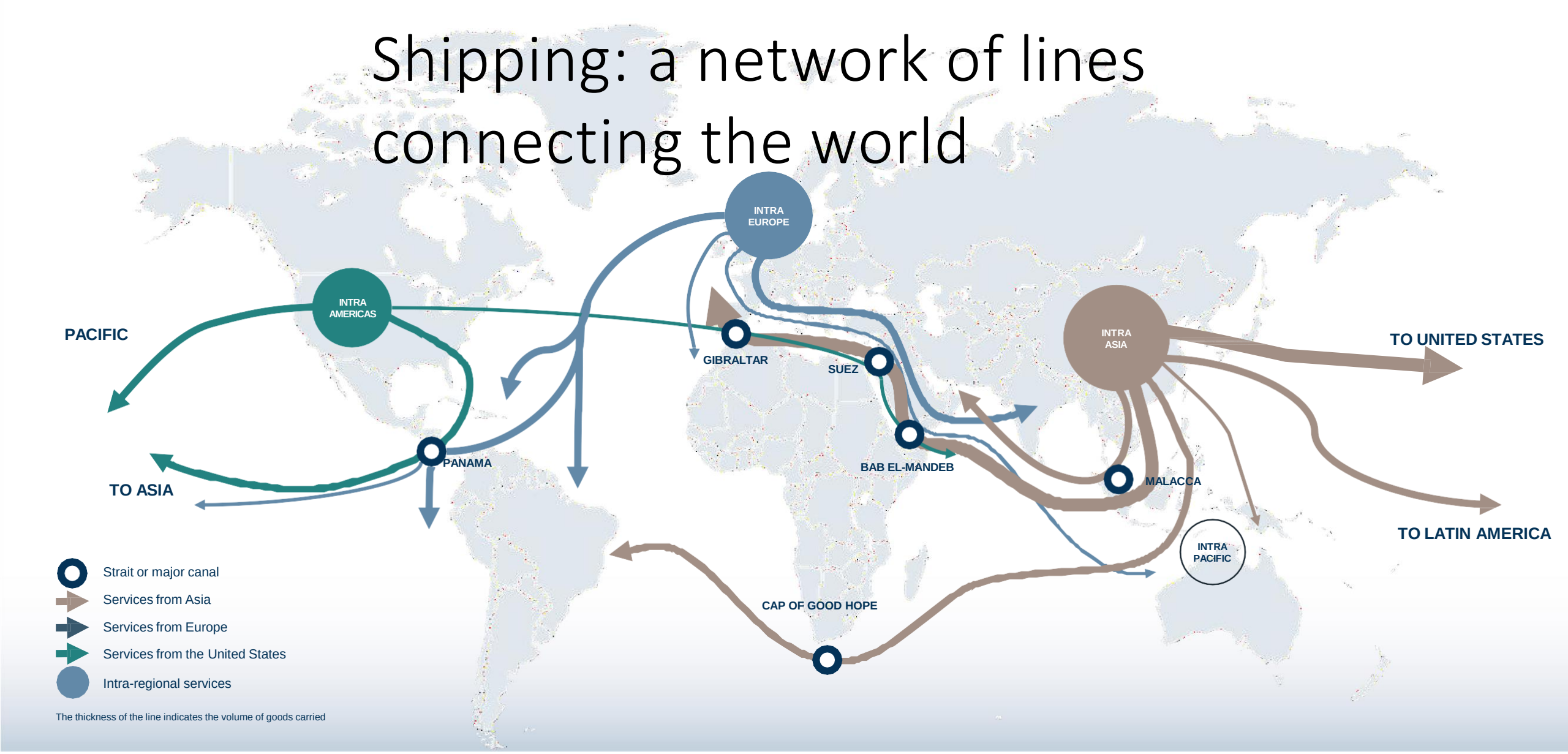
+620
vessels

+50
port terminals
in operation in 28 countries

+20 M
TEU transported
(2023)

+420
ports in 5 continents
277 shipping services

Shipping: a network of lines connecting the world



Logistics

CMA CGM Group's subsidiary CEVA Logistics is one of the world's leading providers of logistics services. We support our customers with a comprehensive range of air freight, shipping, inland transport and contract logistics solutions.

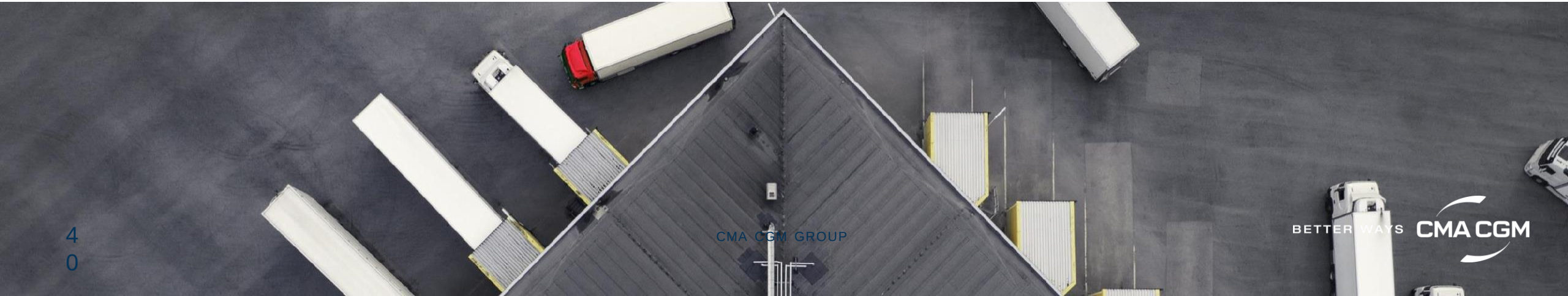
5,5 M
vehicles transported

0.5 M
metric tons
of air freight

26 M
metric tons
of inland freight

1.15 M
TEU

10,4 M
m2 of storage
space



Air Cargo

CMA CGM AIR CARGO is France’s number 1 cargo airline and has been supplementing the Group’s transport solutions since 2021.

CMA CGM AIR CARGO remains committed to providing high quality, reliable and sustainable air transport solutions to carry its customers’ freight.

6
aircrafts in service
12 aircrafts by 2027

+100
pilots

Global coverage

13
Spacialized products

- TRPM – Overview
- Suppliers & Third parties management

TPRM – SCOPE & ENGAGEMENT RULES

IN

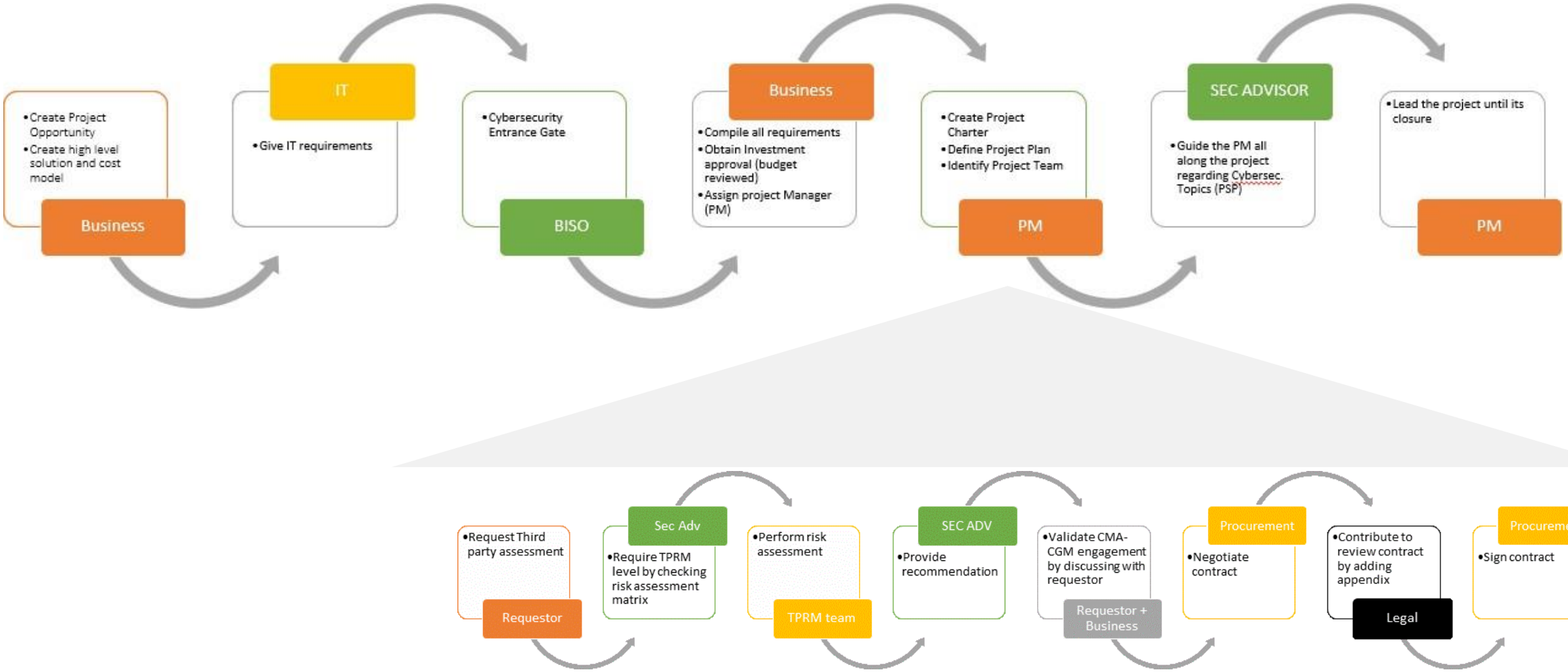
1. New IT projects (on-premise or cloud):
   - In case of multiple bid applicants - RFP
   - One pre-selected supplier (Qualification)
2. Existing procurement known supplier if contract renewal*
3. Proof Of Concept on an exception basis**

* No assessment for an existing supplier contract
** Security Advisor will study its on case-by-case basis: *Guidelines to Proof of Concept* on the "*Requirements in projects*" part of the CyberSecurity Compass Sharepoint

OUT

Rules	Justification
1. Applications already in production (ongoing contract with the supplier)	Too late to apply TPRM because a contract is already signed. Depending on the context a risk assessment or a security audit should be performed on the application itself
2. Unofficial projects without a Business Owner, **a project framework** and Security Advisor implication	Security Advisor must be involved, a Business Owner must be clearly identified and **a project must be validated**
3. Projects for which the target architecture has not yet been defined/decided	Target architecture must be defined first (no TPRM to assess On-premise vs Cloud, IaaS vs PaaS vs SaaS, Public vs Private vs Hybrid Cloud, etc)
4. POCs outside of TPRM exceptions:	Too early to apply TPRM, there is no official project
5. Standalone software installed locally on workstation or mobile device	Standalone software approval is out of TPRM scope

TPRM HIGH LEVEL PROJECT MANAGEMENT PROCESS



IN CASE OF MULTIPLE BID APPLICANTS (TPRM for RFP)

TPRM trigger by Security Advisor

1

Prerequisite's reception
(see prerequisites slide)

Bid applicants questionnaire* answers & BitSight report analysis

2

3

One cybersecurity advice report for all applicants

When required meeting with stakeholders to explain residual risks

4

* : 2 different use case security questionnaires (data processing only, On-premise/Cloud based)

Cybersecurity advice report – RFP case

EXAMPLE

Security advice

Red

Third party security level is too low, risks cannot be short/mid term mitigated, business should not contract with the applicant/supplier

xx%

Applicant 1

Findings:

- xxxxx

Risks cannot be mitigated by short/mid term

Orange

Third party security level is not enough, risks must be short/mid term mitigated by establishing an action plan or must be accepted by the business

xx%

Applicant 2

Findings:

- xxxx

Short-mid term action plan to mitigate risks:

- Third party must xxxxxxxxxx

Green

Third party has shown an acceptable security level in the context for this project

xx%

Applicant 3

Findings:

- xxxx

Date of the cybersecurity advice report release:

Procurement phase : RFP

Name of the project:

Business Owner:

Pre-risk assessment of the project (CIA, etc.):

Name of the applicants/suppliers :
Applicant 1
Applicant 2
Applicant 3

CMA CGM

BETTER WAYS

ANL APL CNC MERCOSUL LINE LA MÉRIDIONALE CEVA LOGISTICS COLIS PRIVÉ CMA CGM AIR CARGO WHYNOT MEDIA

Session 3 - Cybersecurity in transport design, supply chains and emerging technologies

The impact of emerging technologies on cybersecurity

Olivier Lepretre
Cybersecurity Director
EUROSTAR

The Impact of Emerging Technologies on Cybersecurity

2nd May 2024

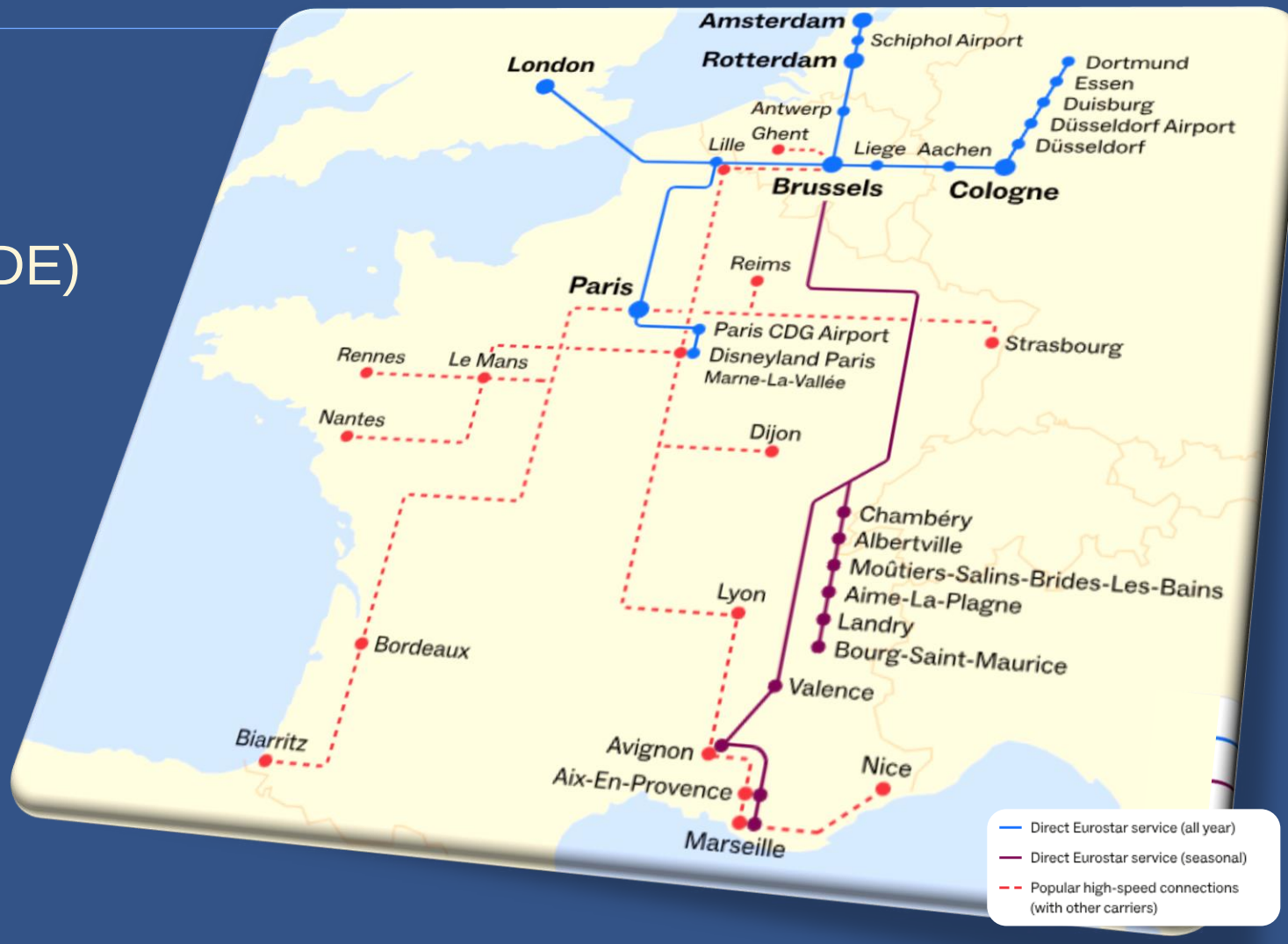
Olivier Lepretre

eurostar

Eurostar | At a glance

www.eurostar.com

- 5 countries (UK, FR, BE, NL & DE)
- 28 direct destinations
- Fleet of 51 trains
- 18,6 million passengers (2023)
- Revenue €1,53bn (2022)
- EBITDA €332 million (2022)



The strictest security regime of any train operator in Europe (UK routes)

Emerging Technologies | Let's step back

Static page ->
eCommerce, Web 2.0, 3.0

SSL/TLS, Captcha,
Firewall

SMS, Emails, Web ->
Anywhere, Anytime

Mobile Device Mgmt,
Unified Endpoint Mgmt

Device Intelligence, Edge
processing

Hardening, Network
segmentation, SSE

Decentralized and flexible computer power ->
Change context of perimeter security, responsibility model

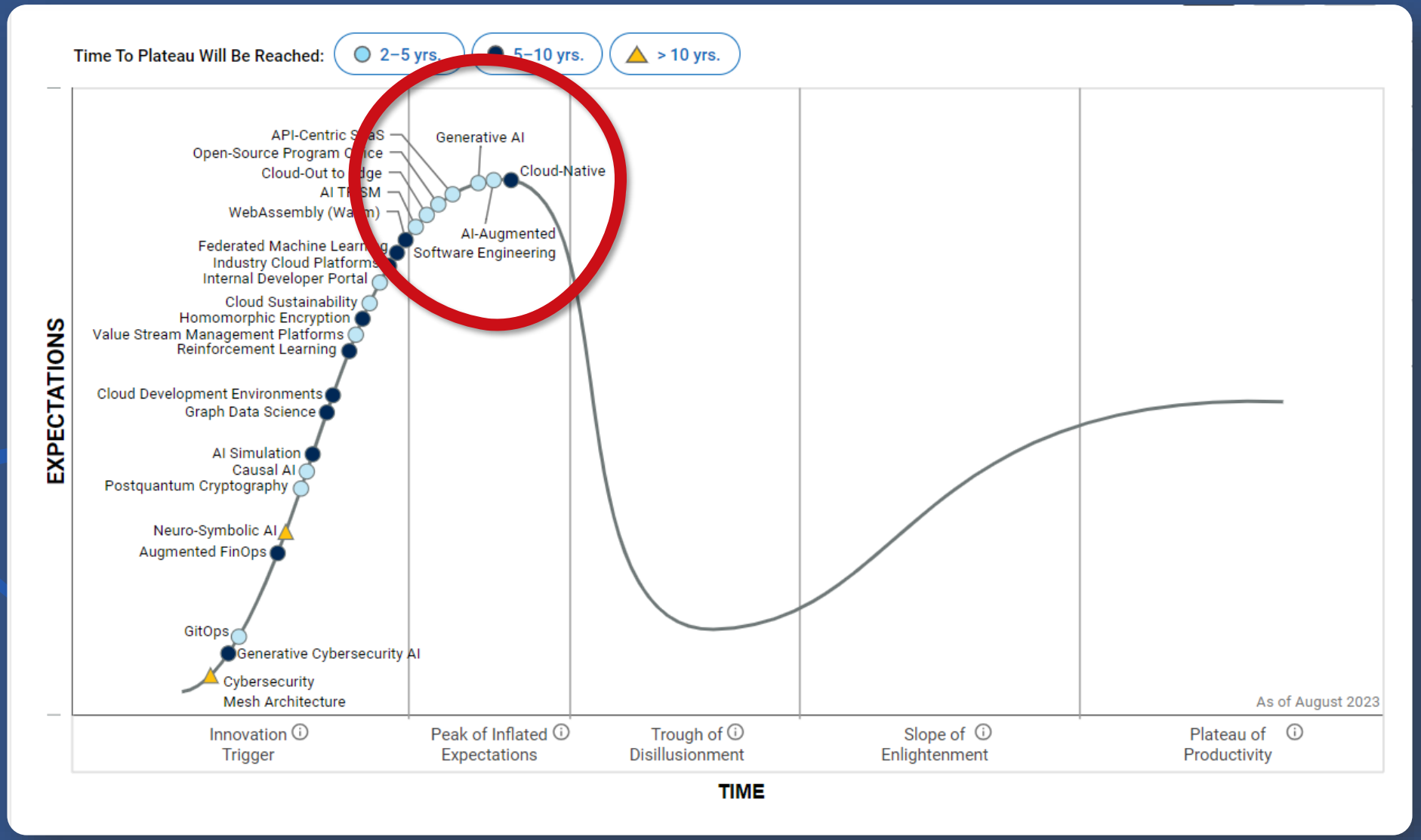
Access Mgmt, DLP, Governance, WAF, CASB

Broadband access ->
Remote access

VPN, SASE, VDI, MFA

Emerging Technologies | Today

Source: Gartner | Hype Cycle for Emerging Technologies, 2023



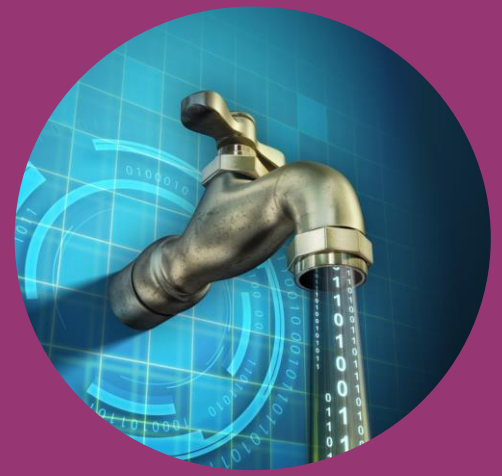
Artificial Intelligence | New Threats ?

Lowering the barrier to entry for attackers, increasing the sophistication and automation of attacks, and decreasing time-to-exploit

- Social Engineering
- Malware code generation
- Vulnerability discovery
- Disinformation

- Data poisoning
- Data leakage
- Evasion
- Model extraction

- Deep fakes
- Voice mimic
- Writing style
- Synthetic identity



- Security & Privacy
- Intellectual Property
- Quality of training data
- Ethical considerations

Artificial Intelligence | New Opportunities !

Strengthen cybersecurity capabilities and threat detection with AI, Improve collaboration, invest in human expertise

Definition and Enforcement of Principles & Guardrails

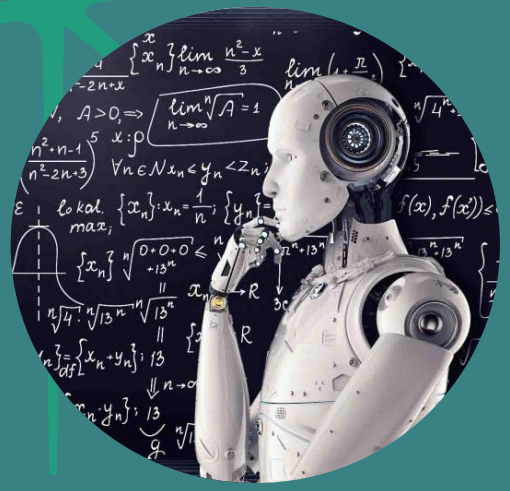
Implementation of AI Powered Tools

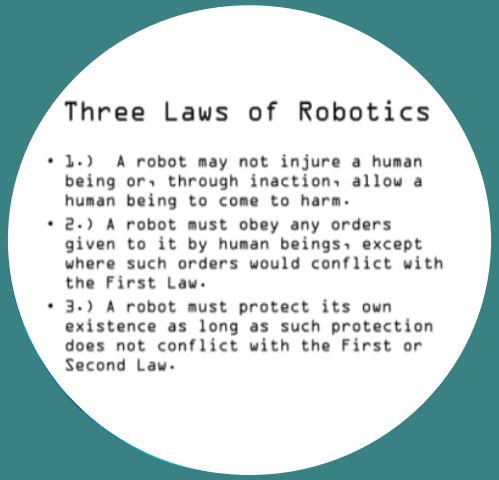
Maintenance of Skilled Human Oversight

Use of Closed Model(s) for Augmented Generation

Improved Data Quality

Standardized Strategies for Managing AI-related Risk





Serverless Architecture

Software defined Perimeter

Strong coding

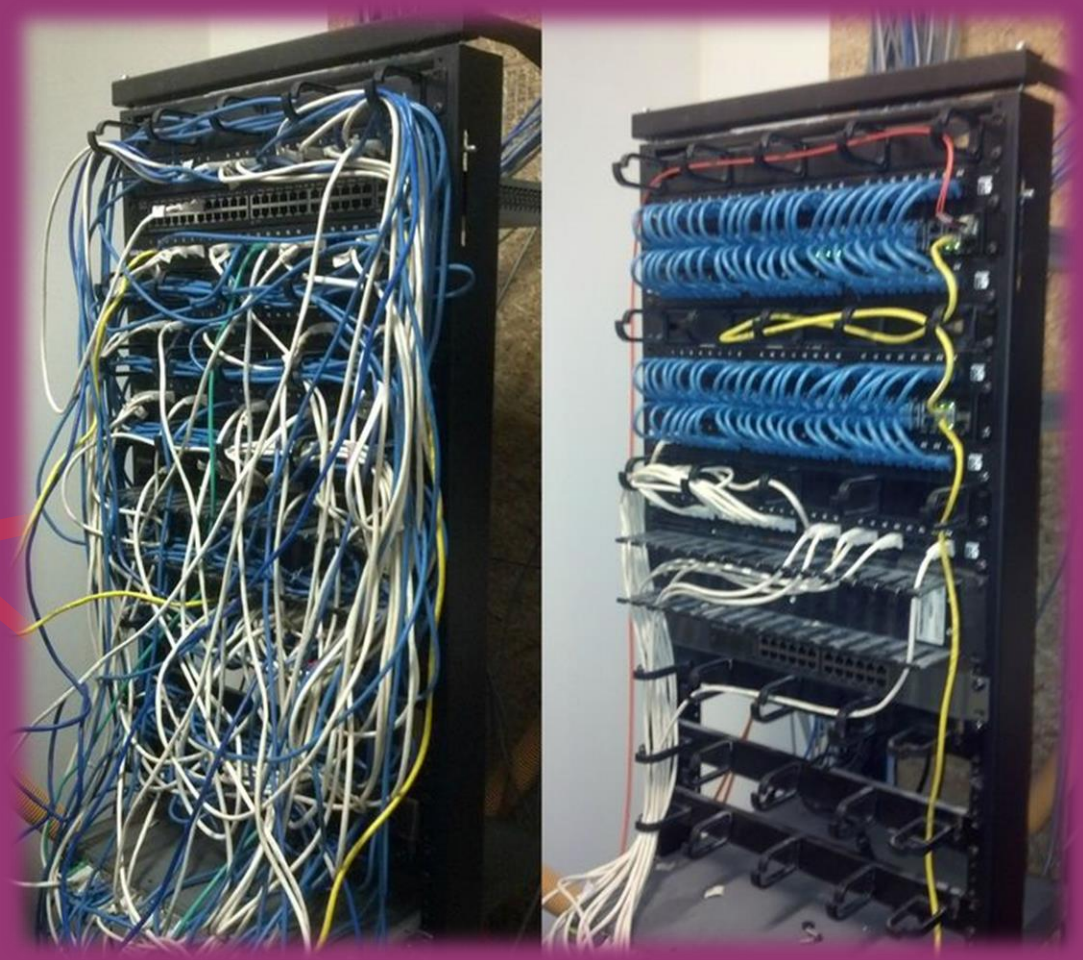
Behavioral protection

Biometric Authentication

Password less

Emerging Technologies

More opportunities !



Adaptive networks

Software Defined

NaaS

Zero (Explicit) trust models

Emerging Technologies

More opportunities !

Quantum computing

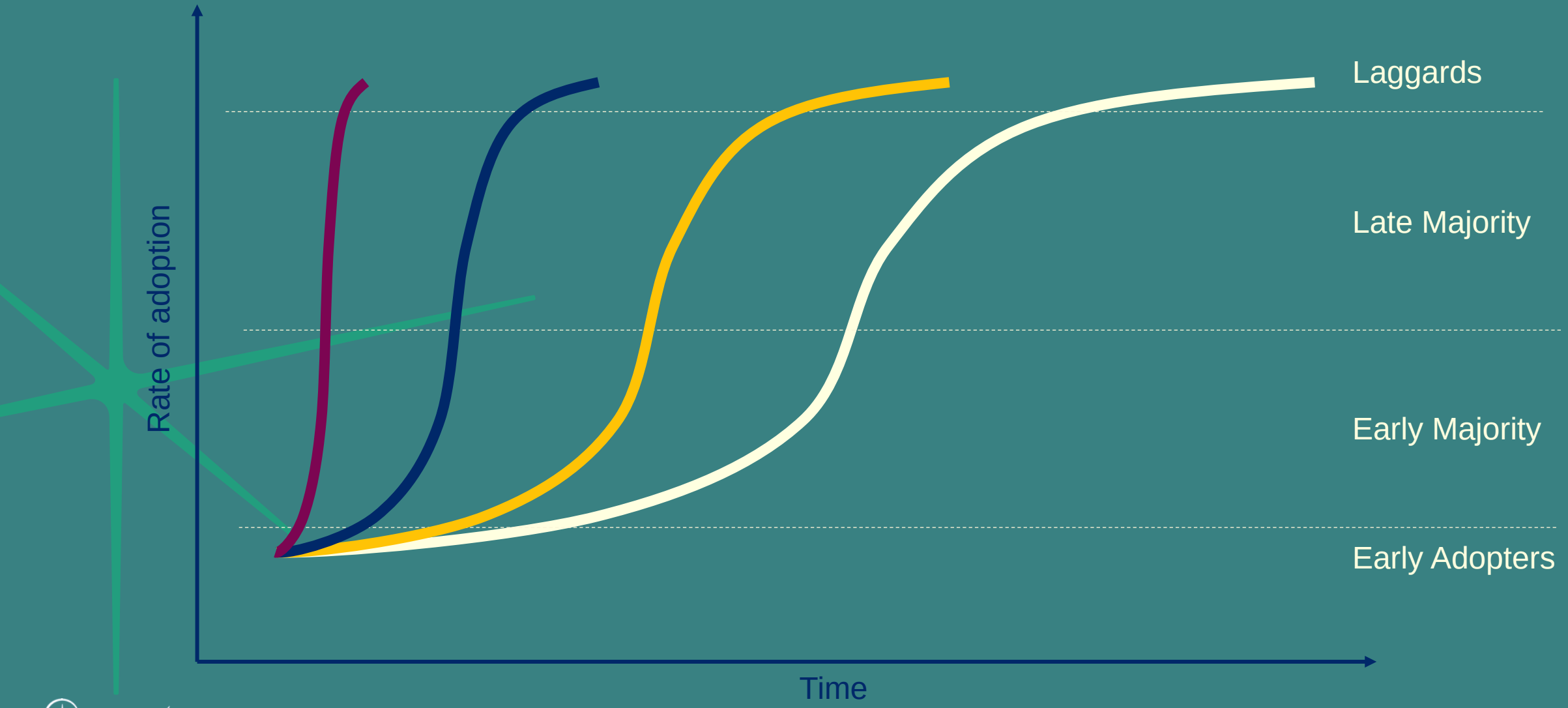
Quicker decryption

Stronger encryption

...

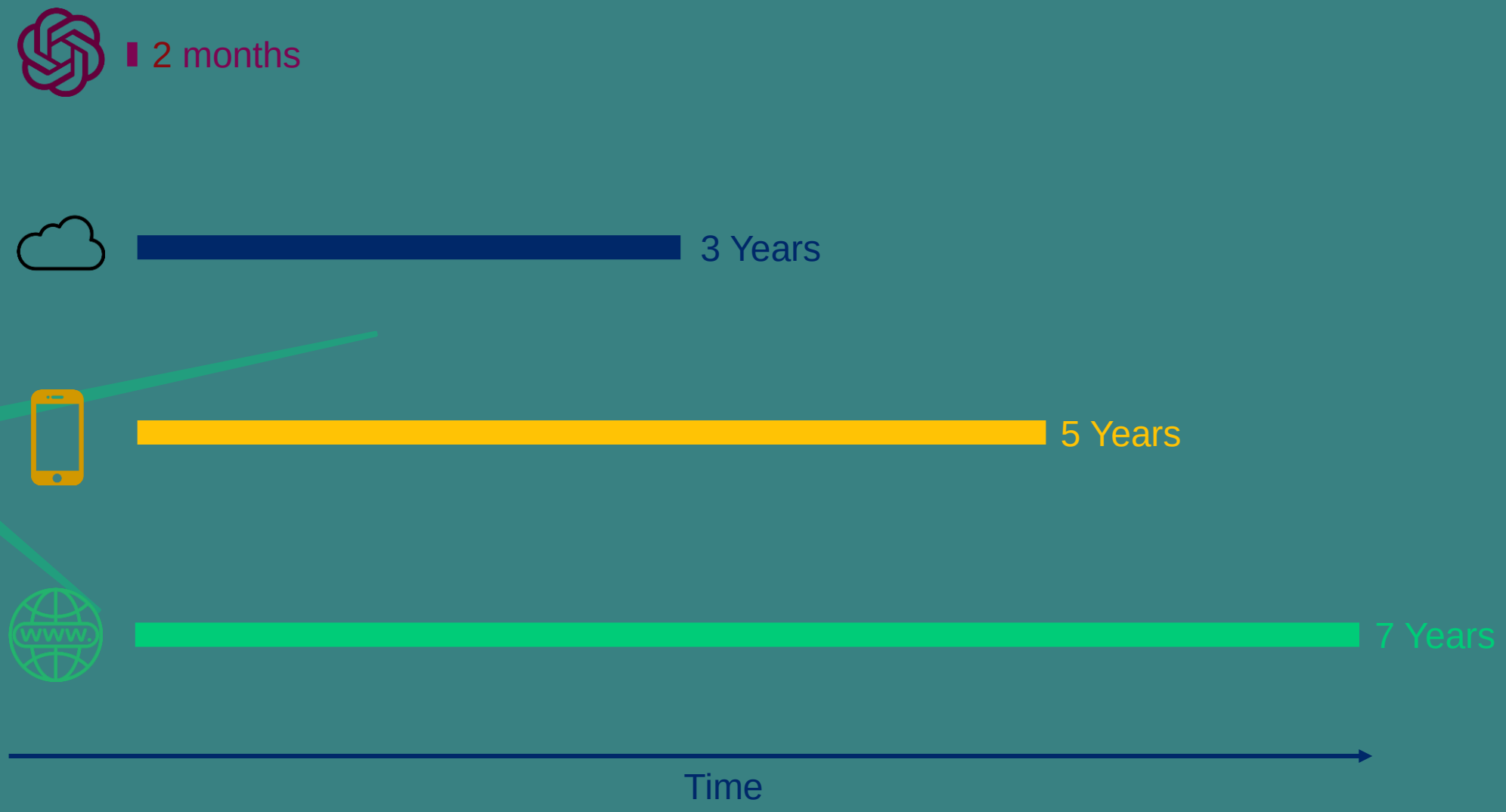
Emerging technologies | Speed of adoption

The S-curve

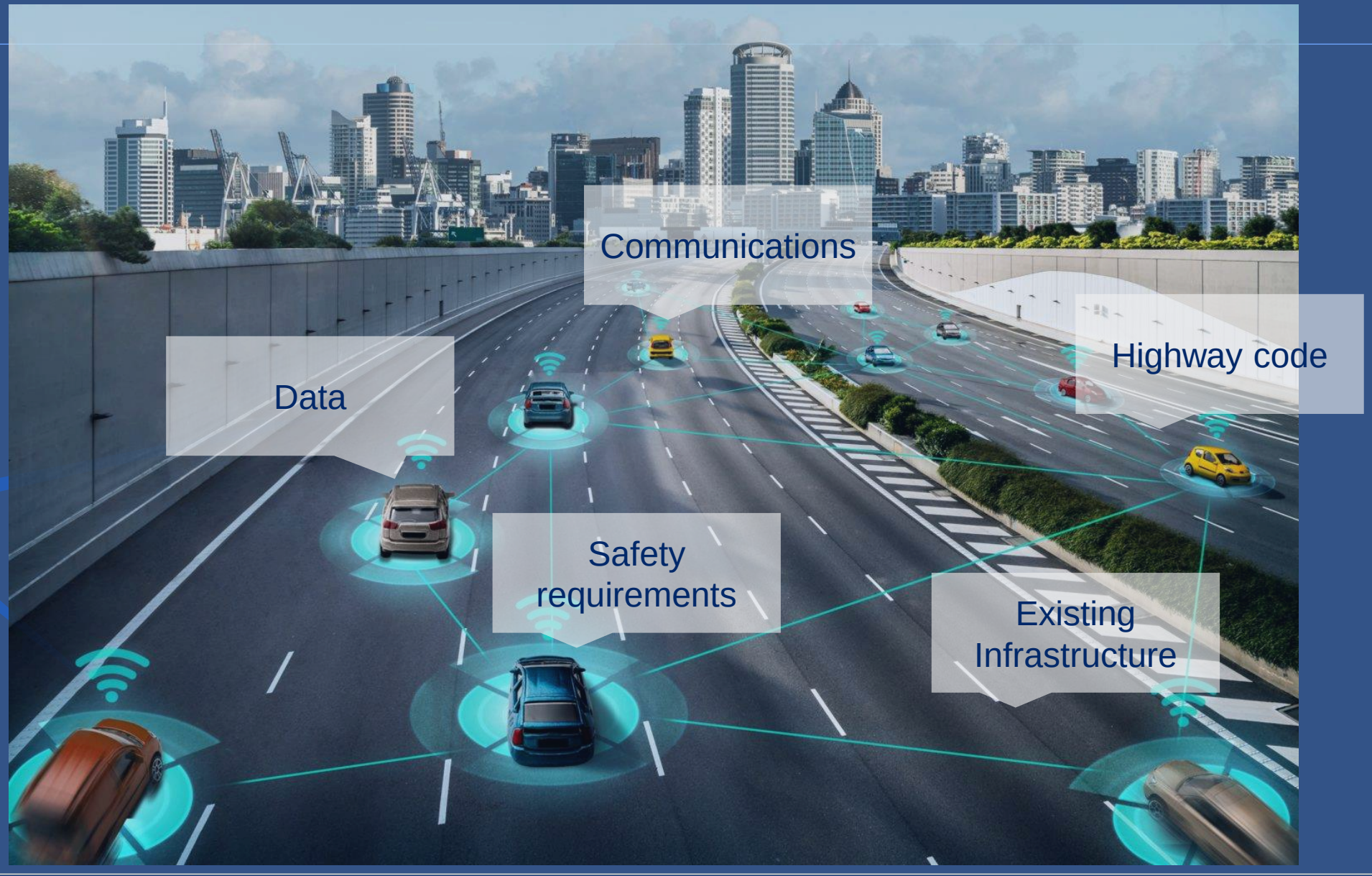


Emerging technologies | Speed of adoption

Time for 100 millions person to adopt technology



New technologies | Balance between Risk & Agility



Merci
Thank you
Danke
Dank je wel

eurostar

Session 3 - Cybersecurity in transport design, supply chains and emerging technologies

The Cyber Fusion Center of the Future

Erik Van Buggenhout
Head of Managed Security Services
NVISO Security

Building the Cyber Fusion Center of the Future

TRANSPORT CYBERSECURITY CONFERENCE

Erik Van Buggenhout

Head of Managed Security Services

nviso

Building for success

How to build a highly functioning Fusion Center

Common SOC issues

Expensive

Alert Fatigue

Skill Shortage

Ever-Expanding Landscape

Critical Success Factors

Threat-Centric

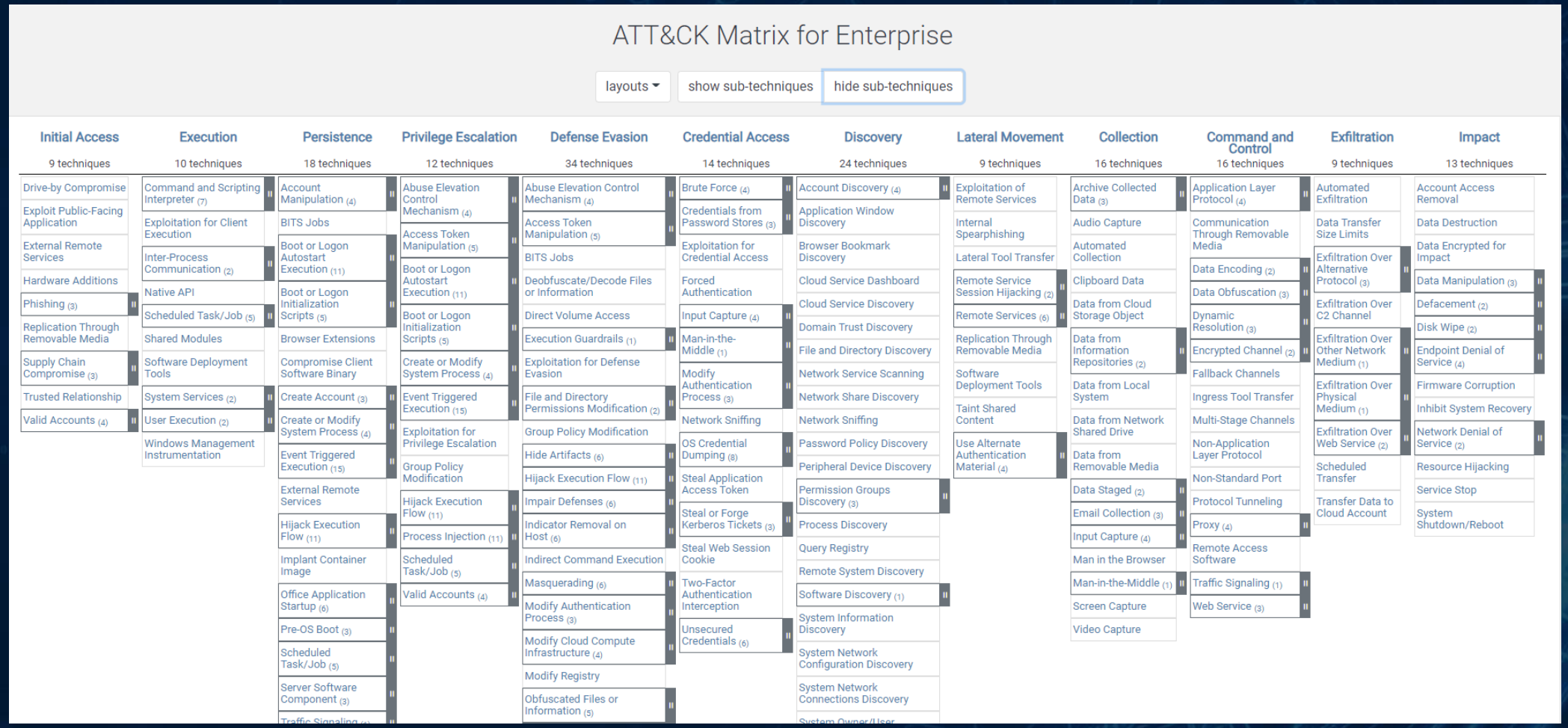
Purple Focus

SOAR-Centric

Automation-First

Threat-Centric

Leveraging MITRE ATT&CK for a threat-centric approach



Purple Focus

Combining Red and Blue skills

The Cyber Fusion Center should be **a purple ambassador** and make sure red thinks a bit more blue, while blue should think a bit more red:

Red Team with a "touch of blue"

- **Understand prevention, detection, and response** techniques
- **Understand complexities** and limitations of target organization and tailor recommendations
- **Present known TTPs** to Blue Team (highlight "quick wins") and innovate Red Team approach continuously

Blue Team with a "touch of red"

- Understand and follow up on known adversary TTPs
- **Test individual TTPs continuously** and improve where possible
- Track and report on **coverage of TTPs** (e.g., ATT&CK framework)

Purple Focus

Combining Red and Blue skills

So… No more yearly red teams? There's room for both:

Organize **periodic Red Team exercises** **to assess** the actual state of security in the organization. Offer feedback only after the exercise ends, as the exercise is typically meant to be stealthy (realistic adversary emulation)…

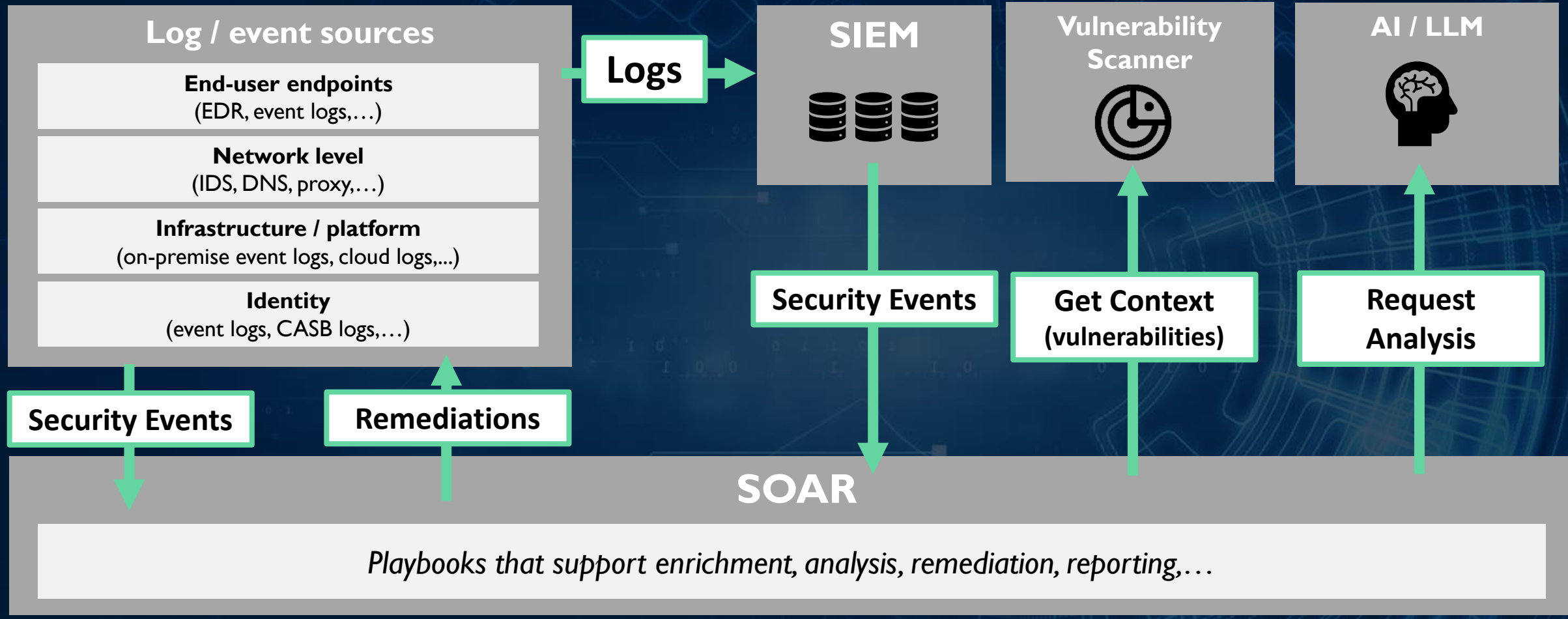
VALUE: Periodic assessment of organization resilience

Perform **continuous Purple Teaming** to improve the state of security in the organization. Blue Team members simulate focused attack techniques as part of their operations to immediately test effectiveness of detection and prevention controls.

VALUE: Continuous improvement of organization resilience

SOAR-Centric

A SOAR-Centric architecture

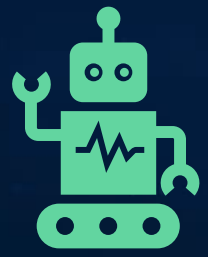


The **SOAR platform becomes the "central brain"** of the Fusion Center (instead of the SIEM). All security technologies should be connected to the SOAR (both for detection, contextualisation, handling, reporting and remediation)

Automation

Marriage between automation and human effort

"Geographically improbable log-on for user Erik Van Buggenhout"



Enrich: Add privileges of user Erik Van Buggenhout to security event

Enrich: Add insights & reputation of source IP address to security event

Enrich: Add whether or not MFA was used in authentication to security event

Enrich: Add historic locations used by Erik Van Buggenhout to security event

Enrich: Add security risk score for user Erik Van Buggenhout to security event

Enrich: Add info on workstation security alerts for Erik Van Buggenhout's workstation to security event

Enrich: …

Decide: Confirm whether, based on the above enrichments, a false positive can be confirmed

Remediate: When confirmed true positive (and allow-listed for remediation), execute remediation

Present: When unsure, present enriched security event to analyst for further follow-up