eu-LISA Industry Roundtable:

'Looking Ahead. Ensuring Cyber-resilience of EU IT Systems against Emerging Threats'

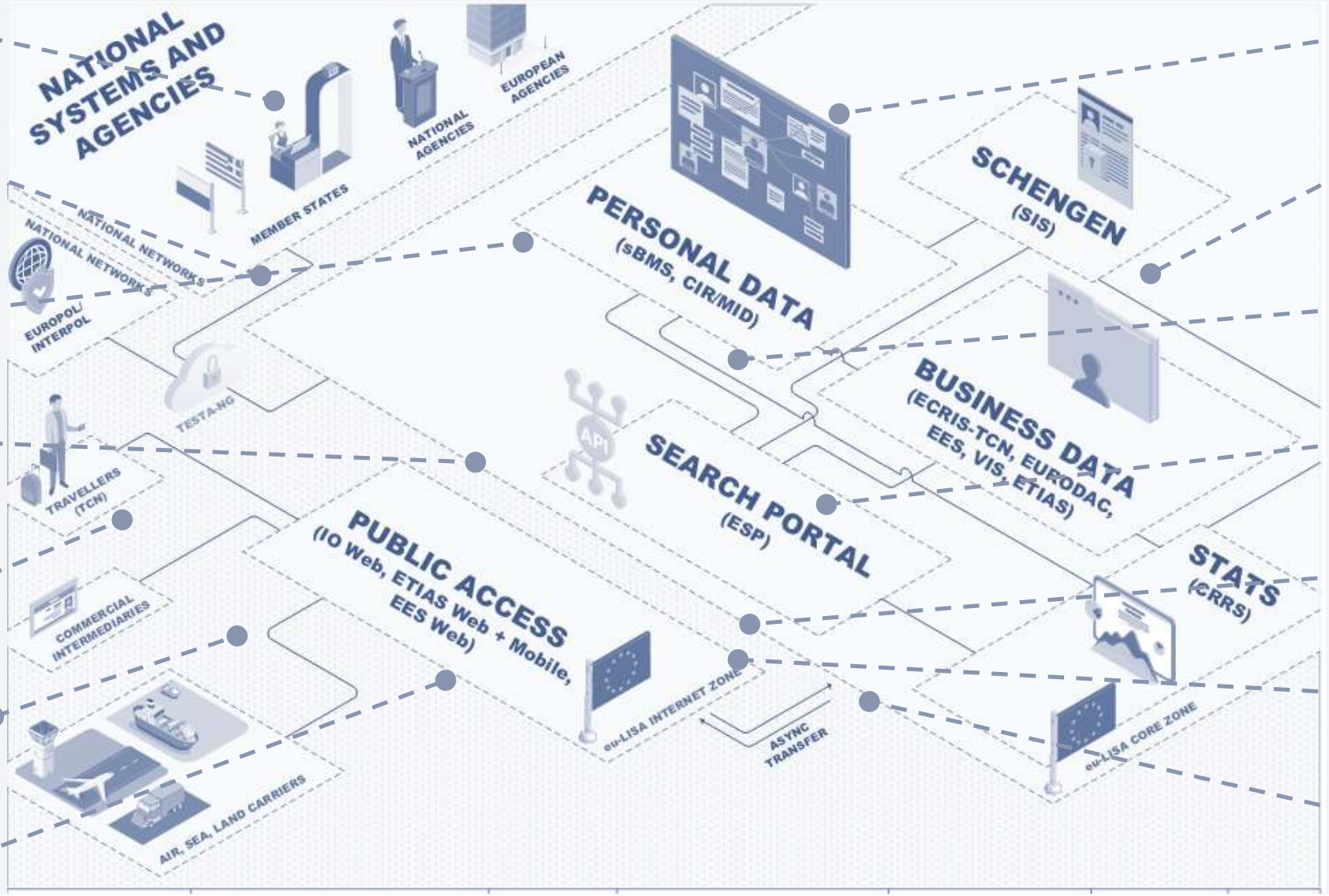
Session II - A. Setting the scene: The Cyber Threat Landscape of eu-LISA Large-Scale IT Systems

Stockholm, 1 June 2023

Dr Luca Zampaglione
Head of Unit Security
Agency Security Officer

Threat Landscape of eu-LISA systems

- Social Engineering
- Extortion
- Data wiping
- Supply chain attacks
- Disinformation
- AI & Deepfakes
- DoS



- Hack and Leak
- Availability
- Data Breach
- Identity Abuse
- Mal/Ransomware
- APT
- Errors & misconfigurations


AEROTRAIL EVO
BTWIN ALLTERRAIN


btwin

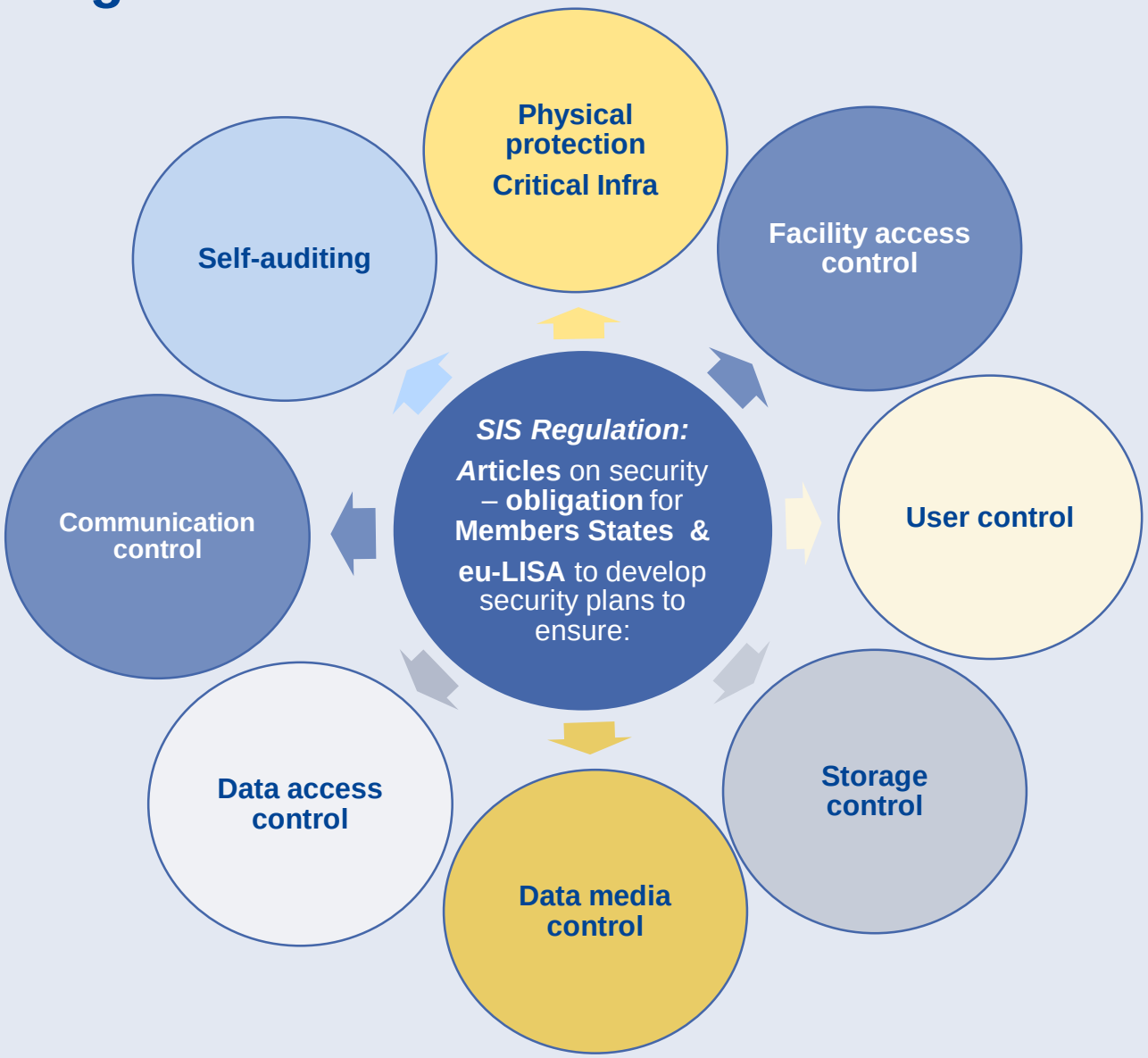
Understanding Cybersecurity in the European Union.

1. The NIS 2 Directive
2. The European Cyber Resilience Act
3. The Digital Operational Resilience Act (DORA)
4. The Critical Entities Resilience Directive (CER)
5. The Digital Services Act (DSA)
6. The Digital Markets Act (DMA)
7. The European Health Data Space (EHDS)
8. The European Chips Act
9. The European Data Act
10. European Data Governance Act (DGA)
11. The Artificial Intelligence Act
12. The European ePrivacy Regulation
13. The European Cyber Defence Policy
14. The Strategic Compass of the European Union
15. The EU Cyber Diplomacy Toolbox
16. The GDPR
17. The Cybersecurity Act (EU 881 / 2019)
18. Cybersecurity services for Radio Equipment Directive (RED)
19. Proposed EU Cyber Solidarity initiative and cyber reserve

Our mandate is our strength

Legal Basis

Our mandate is our strength



Goal

Continuous, Effective & Secure operation of systems

Focus

Confidentiality
Integrity
Availability

Responsibility

Shared responsibility
eu-LISA & Member States

ETIAS Regulation:
Article 60 – Security Incidents

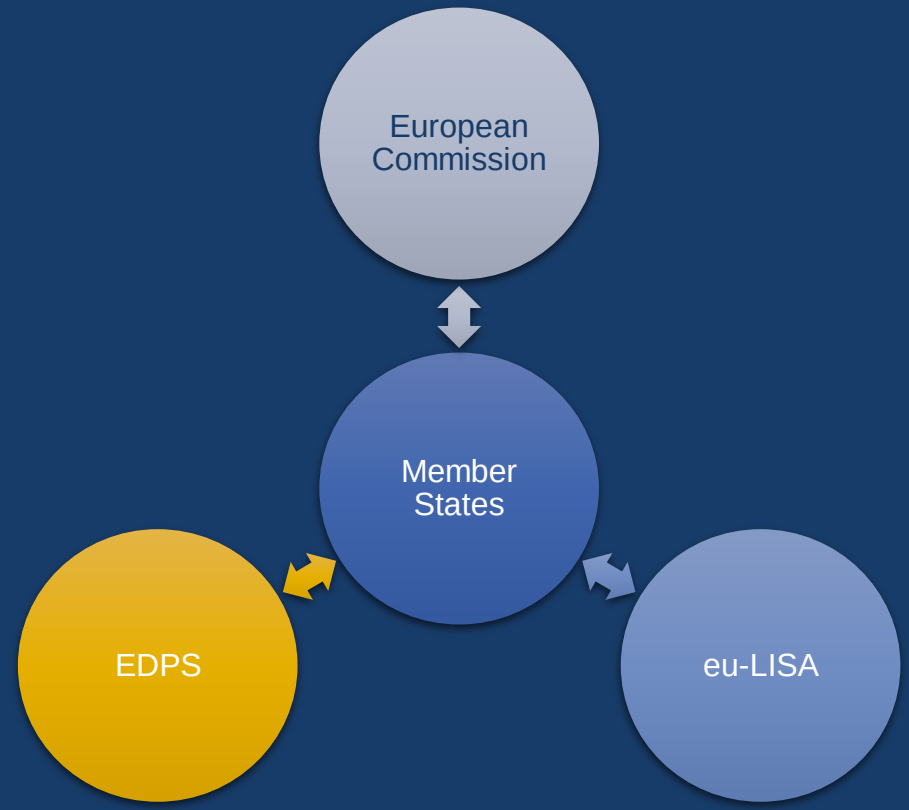
Security incident: *Any event that has or may have an impact on the security of ETIAS and may cause damage or loss to the data stored in ETIAS.*

Compromise of :

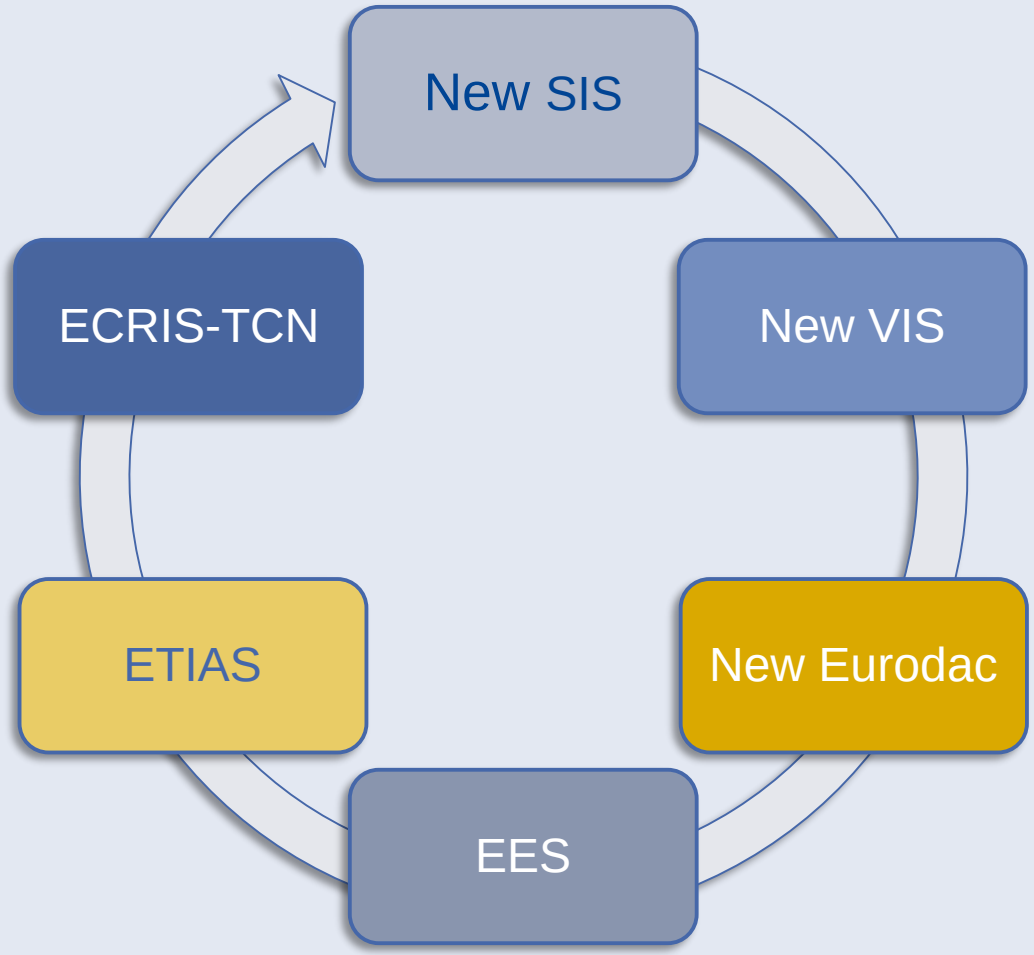
- Confidentiality
- Integrity
- Availability

In case of security incidents:

- The Member States shall notify the Commission, eu-LISA and the EDPS
- Incidents that might affect the operation of the ETIAS should be notified to the Member States



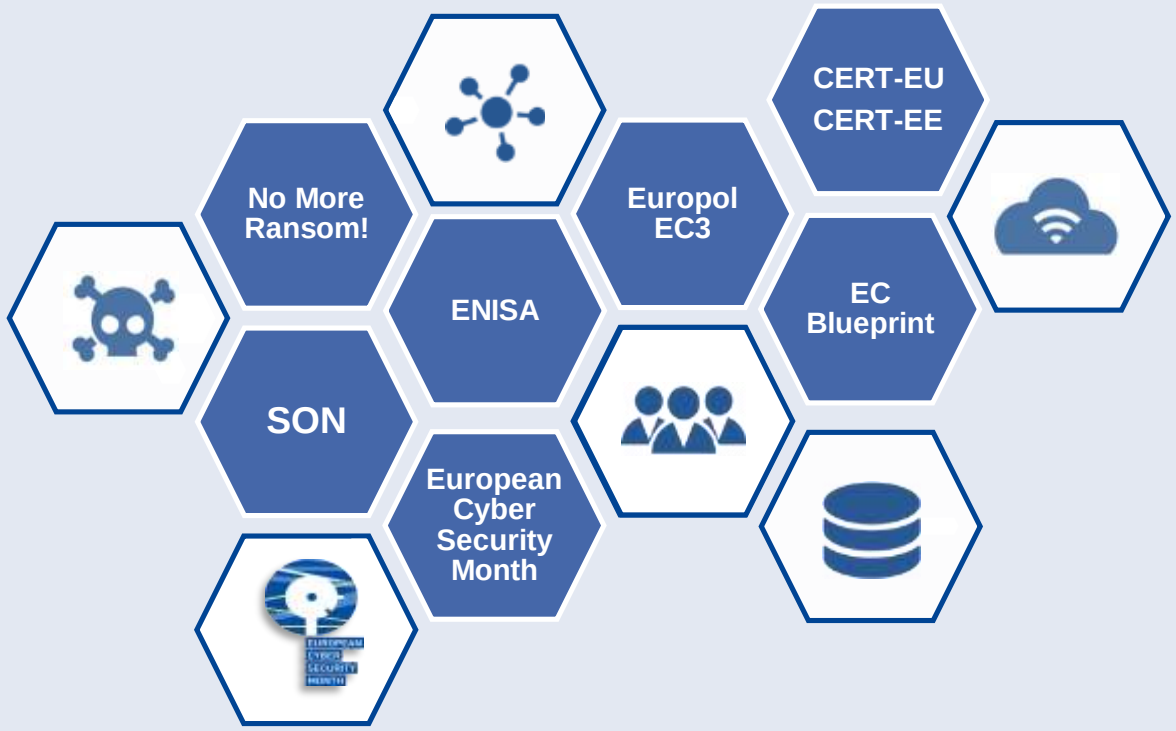
Interoperability - Security Incidents Management



- Implementing Act on the **cooperation** in case of security incidents
- **Cooperation** in case of security incidents 24/7 via:
  - **Cooperation** Group
  - **Cooperation** Platform
  - **Cooperation** Procedure


We never drop the ball
European Commission
eu-LISA
FRONTEX
Security Incident
Europol
EDPS
Member States
Interoperability

Joint Effort for a Cyber-Secure Ecosystem – today and work in progress



- Cooperation through Security Officers Network (SON) with MS, EU Commission and JHA EU Agencies
- Development of the Cooperation Group under IO framework
- Multi-stakeholder coordination (National CERTs and CERT-EU, Security Services, Private Sector)
- Exchanges of best practices (Business Continuity Network)
- Strengthened security through harmonized community security plans
- Build CSIRT capability

Added value

- Strengthened security
- Improved confidence
- Enhanced reliability
- Compliance
- Community code of practice
- Trust

What do we share

- Technical expertise
- Multi-level testing
- Multi-stakeholder project coordination
- Architecture design and development
- Enhanced reliability

Thank you !

eu-LISA
European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice

www.eulisa.europa.eu

facebook.com/agencyeulisa/
twitter.com/EULISA_agency
linkedin.com/company/eu-lisa/
youtube.com/c/euLISAagency