

eu-LISA INDUSTRY ROUNDTABLE:

**LOOKING AHEAD-  
ENSURING  
CYBER-RESILIENCE  
OF EU IT SYSTEMS  
AGAINST EMERGING  
THREATS**

1 AND 2 JUNE 2023 - STOCKHOLM, SWEDEN

# TABLE OF CONTENT

Executive summary	3
<b>Session I</b>	
<b>Setting the scene: Legal Framework and the European context</b>	<b>5</b>
Opening remarks	6
Legislative framework for eu-LISA and the EU large-scale IT systems	7
Recent EU cybersecurity Legislative initiatives	8
<b>Session II</b>	
<b>Setting the scene: The cyber-threat landscape of Large-Scale IT systems</b>	<b>10</b>
The cybersecurity threat landscape for 2023 and beyond: ENISA efforts	11
Latest challenges on cyber-threats and cyber crisis	13
Threat landscape of the eu-LISA large-scale IT Systems	15
<b>Panel discussion</b>	<b>17</b>
<b>Session III</b>	
<b>Technology solutions for the IDENTIFY and PROTECT functions of the cybersecurity framework</b>	<b>21</b>
BAMF: From React to Act	22
Entrust: Post Quantum World & Zero Trust	24
iProov: Identifying, Defending and Protecting Against Emerging Threats to Biometric Face Verification	25
Splunk: Eliminate Your Alert Fatigue – Risk-Based Alerting	27
secunet: SINA SOLID - Secure Dynamic VPN Networking	29
<b>Session IV</b>	
<b>Technology solutions for the DETECT function of the cybersecurity framework</b>	<b>30</b>
CERT-EU: Detection in the cloud	31
NTT DATA: Active Threat Management - a Holistic Approach to Ensure Cyber-Resilience against Emerging Threats	33
SentinelOne: Understanding MITRE ENGAGE Deception for adversary engagement, early breach detection, and improved incident response	35
Deloitte: Managed extended detection and response (MXDR)	37
Dataminr: The value of real-time publicly available information	38
<b>Session V</b>	
<b>Technology Solutions for the RECOVER and RESPOND</b>	<b>39</b>
NCC-SE: The European Initiative to Accelerate Cybersecurity Research and Innovation	40
Palo Alto Networks: Automating the Modern SOC responding and Recovering from Cyber Incidents at Machine Speed	42
Leonardo: Cyber Respond and Recover Approach for Systemic Shock Risk Mitigation	44
Closing remarks	45

# EXECUTIVE SUMMARY

## General context

Network and information systems have developed into a central feature of everyday life with the speedy digital transformation and interconnectedness of society, including in cross-border exchanges. That development has led to an expansion of the cyber threat landscape, bringing about new challenges which require adapted, coordinated and innovative responses in all Member States and EU agencies in the domain of Justice and Home Affairs (JHA).

Given this general context, the key objective of eu-LISA's Industry Roundtable (IR), held in June 2023, was to further strengthen the cybersecurity capabilities of Member States and eu-LISA.

The event focused on presenting and discussing new technology solutions, best practices, and frameworks developed and deployed by industry, Member States and other relevant stakeholders to increase the cyber resilience of IT systems. These solutions were mapped to the five core functions of the Cybersecurity Framework: Identify, Protect, Detect, Respond and Recover.

The IR also provided the opportunity to debate, exchange ideas and share knowledge, based on practical experiences and good practices, with the ultimate goal of guaranteeing the freedom of movement of travellers crossing Schengen borders and mobility within Schengen.

## Changes in eu-LISA's business and effect on its cyber-resilience

Currently eu-LISA finds itself at a turning point, with deep changes being implemented in its business that can have a severe impact on the level of cyber-resilience of the Core Business Systems (CBS) managed by the Agency, if the proper corrective measures are not put in place.

The change in the Agency's business can be summarised in three main areas:

From a **development perspective**: eu-LISA is shifting from being a mainly operational Agency to also an application development Agency, with the new inflow of legislation where it is mandated to develop from scratch a number of applications, including EES, ETIAS, sBMS, ECRIS-TCN or JIT. In addition, the Agency is also managing major upgrades of the CBS currently in production. The development is also shifting to micro-service technologies and private cloud deployments. The Agency needs to guarantee that all these in-house self-developed systems/apps/software do not introduce in the systems new vulnerabilities to cyber-threats.

From an **exposure perspective**: while at the moment the CBS are isolated from the internet, EES and ETIAS will bring new challenges. These systems will be accessed not only from a controlled environment of only public institutions at MS and European level, but also by new clients such as: sea, land and air carriers, by means of a dedicated extranet, and travellers, through new software such as dedicated mobile apps. This new exposure considerably increases the security risk to cyber-threats as well as the appeal of the Agency to potential attackers.

From an **architectural perspective**: the interoperability project will further push the paradigm shift started with the collaboration of EES, VIS and sBMS. Interoperability changes the core architecture of the CBS from silo-based (dedicated HW and SW elements) to systems that share application core elements. This change is even more relevant for the new Internet Zone where the Agency has shared many application components on top of a platform as a service. The Agency needs to make sure that such design does not increase the vulnerability to cyber-threats of its environment.

These changes in the business of eu-LISA account for a new reality both in its internal and external network, of highly granular, highly exposed and highly uncontrolled sets of new potential vulnerable points for cyber-attacks.

## Key messages from the Industry Roundtable

During the one and a half days of the Industry Roundtable, several key messages emerged from the interventions and fruitful discussions held by the different stakeholders:

### Importance of the CBS: Security VS Usability

- The IT systems managed by eu-LISA are essential for the freedom of movement within Schengen, and to ensure security and justice.
- If any of the CBS was compromised by a cyber-attack, the consequences would be very severe: e.g. closing of the external Schengen borders, re-opening of the internal borders...
- As a result, eu-LISA must prioritise the cyber-resilience of the CBS.
- However, cyber-resilience should not come at the cost of the systems being unusable. EU IT Systems have to be protected, but at the same time have to be efficient and usable. A balance between security and usability must be reached.

### The evolution of cyber-threats and cyber-actors

- The **number of attacks** and cyber-threats is rising continuously and very fast.
- The **types of attacks** are changing constantly, with a higher level of sophistication.
- We are seeing an increase in **hybrid threats**, not restricted purely to the cybersecurity domain (e.g. orchestrated disinformation campaigns powered by AI algorithms).
- **Data** is becoming increasingly targeted by attackers (e.g. data breaches, ransomed data).
- **Cyber-actors** are becoming more organised, with better funding and resources. All these aspects have made them more efficient, with a much higher attack potential.

### Solutions and tools that are being applied in this challenging context

It is clear that we are in the middle of a somewhat unbalanced battle: 'attackers need to be successful just once, we need to be successful all the time'. However, even if absolute security does not exist, there are solutions and tools that we can use to protect ourselves in this fast-evolving world of increasing risks:

- Being cyber-resilient starts through **policy**: The EC has made one of its top priorities to ensure cybersecurity within the EU, providing a general regulatory framework through the NIS directive.
- **Communication** is key to face threats effectively. This must include the **sharing of knowledge**. If we detect a vulnerability and we do not share it, our knowledge is of no use for the community.

- **Cooperation** and **collaboration** among all stakeholders, as these new challenges can only be addressed together.
- Communication and cooperation will help to **build trust among stakeholders** and in the systems.
- It is very important to build a **cybersecurity** culture in organisations. Cybersecurity should be an intrinsic part of each organisation's strategy, starting from **top-level management**.
- We need to prepare end users to increase their level of **cyber-awareness: training** and **education** are essential as a first line of defence.
- There is a **lack of human resources** with a high level of skills in cybersecurity. We have to face the challenge of **doing more with less**.
- Therefore, manual defence based solely on human intervention is no longer a viable option. We need to focus on automation in order to dedicate our invaluable human resources to deal with only real high-risk threats, while false alerts are filtered out by machines.
- This can be done through the use of **AI**. AI should not be demonised. AI is a technology that can be used to develop attacks (e.g. disinformation, deepfakes) or to increase cyber-resilience (e.g. automatic detection of threats, identification of new vulnerabilities).
- We also need to be more **proactive** in anticipating new threats, and **not only reactive** to what is already happening.
- Looking to the future, one of the fields that was highlighted during the event and for which we need to be proactive and prepared is the arrival of **quantum computing**. Just like AI, the quantum era will bring new threats, but also new opportunities.
- New approaches to increase cyber-resilience include: **cyber-deception** as a defensive model where fake information is provided to mislead and confuse your adversary; use and analysis of **publicly available information** (e.g. video, text, audio, pictures coming from regular web, deep web, dark web) for the early detection of new threats.

# DAY ONE

## SESSION I

### **SETTING THE SCENE: LEGAL FRAMEWORK AND THE EUROPEAN CONTEX**

Chair:

**Mr Javier Galbally**

Senior Capability Building Officer – R&D, eu-LISA

## OPENING REMARKS



**Ms Agnès Diallo**  
Executive Director, eu-LISA

Ms Diallo, Executive Director of eu-LISA, opened the event with introductory remarks focusing on the changing cybersecurity landscape within which the Agency operates. In particular, she focused on the importance of building systems that help keep Europe open, while ensuring data protection and privacy. In this work, effective collaboration with the wide range of stakeholders, including the EU institutions and agencies, authorities within the Member States as well as industry, is essential to our joint success.

The last few years have brought a number of significant changes, as a result of which cyber resilience has become paramount to our business. First, eu-LISA ('the Agency') has been entrusted with building new systems, including the EES, ETIAS and interoperability, among others. As a result, the Agency has been transformed from an organisation operating systems into an organisation delivering value and services by building new systems. Cybersecurity by design has therefore become central to our work. Second, with the introduction of the new systems, we are serving new end users, which will soon include third-country nationals crossing Schengen borders, as well as carriers providing transportation services to those travellers. This increases system vulnerability and therefore increases the importance of cyber resilience.

With the changing external environment, in particular caused by the war in Ukraine, we've also been facing a growing number of cyber incidents, which increased almost twofold in the first few months following the breakout of the war. Therefore, cybersecurity threats are very real for the Agency and its stakeholder community.

Ms Diallo continued her introductory remarks outlining some of the key points on the dynamics of cybersecurity threats. For example, the number of DDoS attacks has grown significantly in recent years. Considering the importance of data, the number of attacks attempting to capture data has also increased. For example, in an attack on the FBI, more than 5 million fingerprint sets have been stolen from its data bases in a single breach. Similarly, the likes of Uber and Twitter have seen millions of their customers affected by data security breaches.

As cyber threats evolve, so do the actors perpetrating these offences. Increasingly often, we see state-sponsored activists as well as established criminal organisations involved in cyber warfare and cybercrime. Of course, we are also very active in developing new solutions to address these challenges, and this event is one of the tools through which we can collaborate towards the common goal of improving our resilience against cyber threats.

## LEGISLATIVE FRAMEWORK FOR EU-LISA AND THE EU LARGE-SCALE IT SYSTEMS



**Mr Marc Sulon**

Head of Unit, EC,  
DG HOME Unit B.3  
– Digital Schengen

In his speech Mr Sulon focused on the policy and legal framework within which the Agency and its systems operate, and what cyber resilience means in this context. Although cybersecurity may appear secondary, it is in fact at the core of the relevant legislation, considering the importance of ensuring the continuous operation of large-scale IT systems managed by eu-LISA.

Marc Sulon opened his presentation with an overview of the legal acts upon which the Agency operates. He further emphasised the importance of data protection, as well as physical protection, as explicitly defined in the eu-LISA regulation. The regulation also defines the means through which the Agency operates, in particular the fact that the Agency operates on two sites: in Strasbourg and in St. Johann im Pongau in Austria. This may introduce some limitations on the operations of the Agency, including cyber resilience.

This approach is part of the legacy that eu-LISA has taken over with the Schengen Information System, which was set up in 1995 and has been operating in an isolated environment, as specified in the relevant regulation. The regulations covering the work of the Agency and its systems also clearly define the requirements for disaster recovery and business continuity planning.

With the new systems, in particular the EES, we are opening the systems to a number of new access points, including a mobile app, as well as connectivity to a wide range of other systems and end points. The regulation therefore imposes a number of requirements and obligations on the Agency as well as Member State authorities. The regulation also imposes a range of obligations on data protection, as well as an obligation for a fall-back solution, which Member States need to implement locally in case of unavailability of the EES at border-crossing points. Each BCP should be capable to continue business even if the system is not available, implementing a local solution to collect data and upload it to the central system at a later time. The reason is that we need to ensure continuous operation of the systems to ensure that EU borders remain open and under control.

ETIAS is very similar in terms of provisions for implementation. However, ETIAS is opening the door to the internet. ETIAS changes the situation and introduces additional constraints. One of the challenges specific to ETIAS is the maintenance of the watch list, which will contain very sensitive data, perhaps even more sensitive than the information contained in the Schengen Information System. We need to implement the system in a way that ensures the protection of personal data, while at the same time allowing for fuzzy searches. As is well known, fuzzy searches on an encrypted data base are technically very challenging, unless we are ready to run the risk of decrypting the data.

Interoperability introduces other challenges related to the interconnection of the systems, as it introduces the possibility to spread malware across them. Therefore, we need to ensure that this doesn't happen and the systems are separated with regard to security. To address these challenges, the interoperability framework requires the setting up of a platform that will facilitate collaboration in the resolution of security incidents, considering that this is a major risk.

In closing, Mr Sulon emphasised that the availability of information systems was paramount. If the compensatory measures, such as the Schengen Information System or the Visa Information System, were to become unavailable, border controls would need to be reintroduced because the information available to one Member State would not be available to others, thus creating different risk levels across the EU. The same would apply to the EES. System availability, and the fact that the data provided by one Member State is accepted by other Member States, creates a certain level of trust, which forms the basis for the free movement of people in the Schengen Area. Therefore, by ensuring that the systems are protected and available, eu-LISA enables the functioning of the Schengen area.

## RECENT EU CYBERSECURITY LEGISLATIVE INITIATIVES



**Ms Boryana Hristova-Ilieva**  
Legal Officer EC,  
DG CNECT Unit H.2 –  
Cybersecurity and Digital  
Privacy Policy

Ms Hristova-Ilieva opened her presentation with an overview of the impact that security incidents have on the economy. For example, the average cost of a data breach for an individual business was EUR 3.5 million already in 2018; on average, every 11 seconds one organisation is hit by a ransomware attack; the aggregate cost of security incidents affecting businesses in Germany amounted to EUR 220 billion in 2020. We also witness a growth in attacks targeting vulnerabilities in supply chains and in software.

Ms Hristova-Ilieva continued her presentation with an overview of the development of the legislative framework in the area of cybersecurity. The foundations for the current horizontal cybersecurity framework were laid by the NIS 1 directive, which entered into force in 2016 after protracted negotiations. At the time, the opinion of the Member States was that cybersecurity is within the scope of national security and therefore needs to be dealt with at national level.

The NIS 1 directive was followed by the Cybersecurity Act, which entered into force in 2019, which gave ENISA a permanent mandate as a cybersecurity agency. In the middle of the COVID pandemic, the Commission adopted the ambitious EU Cybersecurity Strategy, which included the proposal for a NIS 2 directive, the proposal for a DORA regulation focusing on the financial sector, also the proposed Critical Entities Resilience directive focusing on critical infrastructure. This was followed by the entry into force of the Cybersecurity Competence Centre and Network Regulation in 2021, and a proposal for a Cyber Resilience Act in 2022. Finally, in early 2023, the NIS2 directive entered into force, followed by the proposal for a Cyber Solidarity Act and the Communication on the Cyber Skills Academy in April 2023.

Ms Hristova-Ilieva then explained the main challenges of the NIS1 directive as follows:

- Not all sectors that may be considered critical were in scope.

- Inconsistencies and gaps due to the NIS scope being de facto defined by the Member States.
- Diverging security requirements across Member States.
- Diverging incident notification requirements.
- Ineffective supervision and limited enforcement.
- Voluntary and ad hoc cooperation and information sharing between Member States.

To address these shortcomings, the NIS2 directive was proposed, building on the foundation established by NIS1, including the three main pillars:

- **Member States' capabilities:** national authorities and strategies on cybersecurity; coordinated vulnerability disclosure frameworks; crisis management frameworks.
- **Risk management and reporting:** expanded scope, size, threshold; accountability of top management for non-compliance; streamlined cybersecurity risk management measures for entities, including supply chain security; streamlined incident reporting requirements.
- **Cooperation and information exchange:** CyCLONe; CVD and European vulnerability database; peer reviews; biennial ENISA cybersecurity report.

In terms of scope, NIS2 has significantly expanded, covering all medium and large enterprises, as well as a broader set of sectors. Similarly, the requirements to be imposed by authorities in the Member States will be harmonised across the EU with the help of the NIS2 directive (e.g. measures to protect supply chains). Furthermore, NIS2 introduced top-management accountability for compliance with the requirements. As next steps, Member States will transpose the directive into national legislation by October 2024 and the Commission will adopt two implementing acts on security measures and thresholds that need to be met for reporting on significant incidents, also by October 2024.



One of the areas that remains uncovered by the existing legislation is the security of supply chains for both hardware and software. To bridge this gap, the Commission proposed the Cyber Resilience Act, the main aim of which is to reduce the number of vulnerabilities in the products sold on the EU market (including hardware and software).

This would require any products with digital components that are placed on the EU market to comply with certain cybersecurity requirements, which are technology-neutral and risk-based. It is then up to the manufacturer to assess which of the requirements apply to the particular product and how they can meet the objective set in the requirement. To facilitate compliance with these requirements, the Commission has already started work on the development of harmonised standards. The conformity assessment will be performed either by the manufacturer or by third-party service providers.

Both software and hardware are within the scope of the CRA; however, non-commercial products are not covered by the CRA, and this includes non-commercial open source software, as well as cloud and software as a service solutions, which will be covered by the NIS2 directive.

Similarly, certain products, such as cars, medical devices, etc. will be excluded by default from the scope of the regulation. Finally, conformity requirements will be defined separately for each class of products: default category, which requires self-assessment; critical class I, which requires application of a standard or assessment by a third party; critical class II, which requires assessment by a third party; highly critical, which requires mandatory EU certification.

Ms Hristova-Ilieva closed her presentation by outlining the timeline for the Cyber Resilience Act, which was adopted by the Commission in September 2022. The proposal is now going through the co-decision procedure, where the European Parliament is preparing its position.

Also, the Council is working on the general approach, however it is not clear whether a general approach will be agreed upon before the end of the Swedish presidency. The expectation is that the agreement between the Parliament and the Council will be reached before the European Parliament elections in 2024.

## Three main pillars of NIS 2 Directive

### MEMBER STATE CAPABILITIES



National authorities  
National strategies  
**Coordinated Vulnerability Disclosure (CVD) frameworks**  
**Crisis management frameworks**

### RISK MANAGEMENT & REPORTING



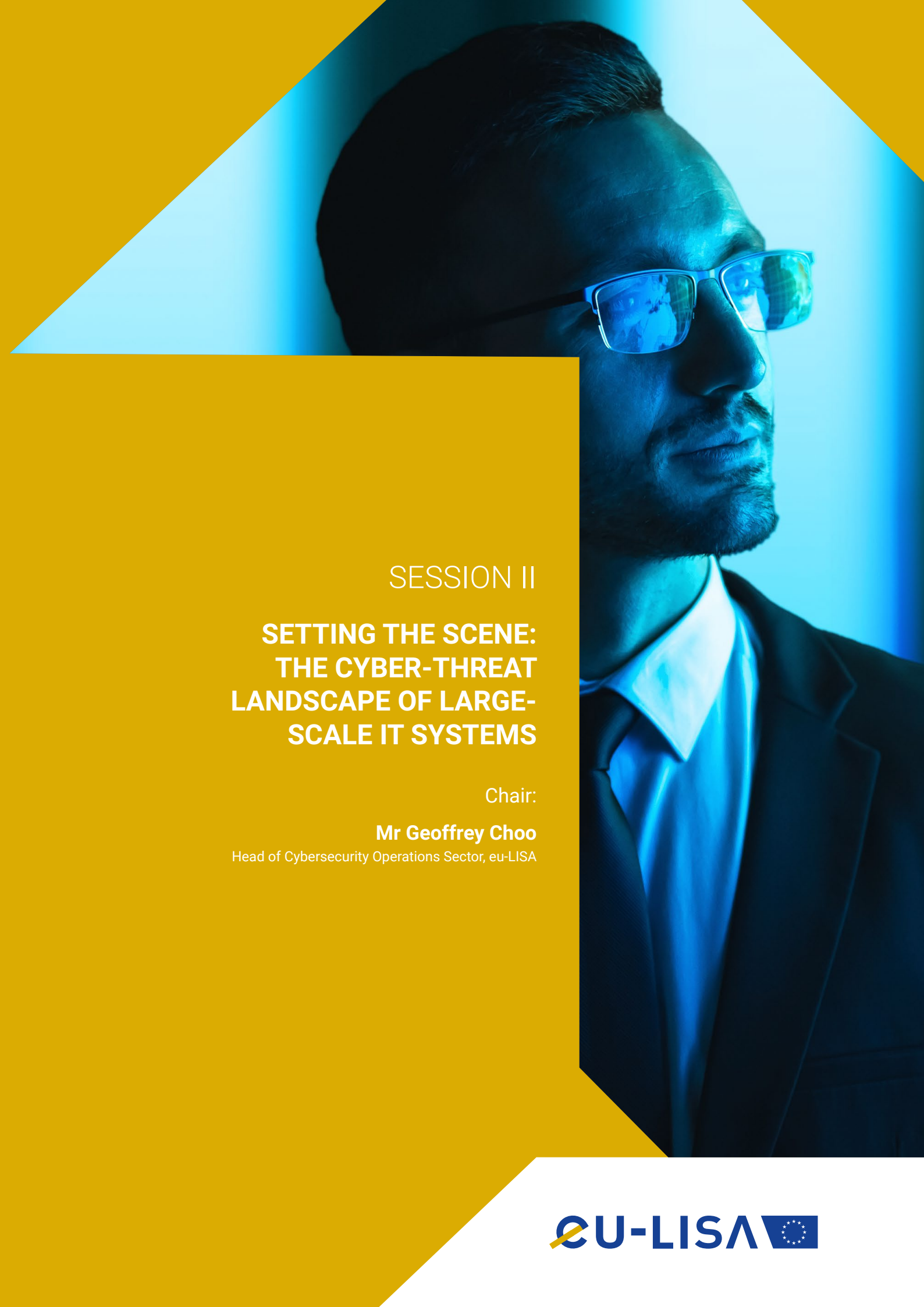
**expanded scope, size threshold**  
**Accountability of top management for non-compliance**  
Streamlined cybersecurity risk management measures for entities, including **supply chain security**  
Streamlined incident reporting requirements

### COOPERATION AND INFO EXCHANGE



Cooperation Group  
CSIRTs network  
**CyCLONE**  
**CVD and European vulnerability database**  
Peer-reviews  
**Biennial ENISA cybersecurity report**





SESSION II

**SETTING THE SCENE:  
THE CYBER-THREAT  
LANDSCAPE OF LARGE-  
SCALE IT SYSTEMS**

Chair:

**Mr Geoffrey Choo**

Head of Cybersecurity Operations Sector, eu-LISA

## THE CYBERSECURITY THREAT LANDSCAPE FOR 2023 AND BEYOND: ENISA EFFORTS



**Mr Apostolos Malatras**

Team leader Knowledge and Information, ENISA

Session II of the Industry Roundtable was opened by Mr Apostolos Malatras, leader of the team responsible for the yearly report on the cybersecurity landscape published by ENISA (European Union Agency for Cybersecurity).

The 'Cybersecurity Landscape report' is currently in its 10th edition. The report identifies the top threats over the past year, major trends observed with respect to threats, threat actor and attack techniques, and presents an impact and motivation analysis. It also provides relevant mitigation measures. Mr Malatras pointed out that 'it is a way to reflect on the past to prepare for the future'.

In particular, the highlights of the 2022 report, as explained by Mr Malatras, are:

**Impact of geopolitics** on the cybersecurity threat landscape, especially as a result of the invasion of Ukraine by Russia:

- Significant increases in hacktivist activity.
- Cyber actors conducting operations in concert with kinetic military action.
- The mobilisation of aid by nation-state groups.
- Disinformation is a tool in cyberwarfare.

**Threat actors** are increasing their capabilities:

- 0-day exploits.
- Continuous 'retirements' and the rebranding of ransomware groups is being used to avoid law enforcement and sanction.
- Hacker-as-a-service business model gaining traction, growing since 2021.
- Threat groups have an increased interest and exhibit an increasing capability in supply chain attacks and attacks against Managed Services Providers (MSPs).

Regarding specific **existing types of threats**, the most important ones observed during 2022 were attacks against data (i.e., data breaches, data leaks) and Distributed Denial of Service (DDoS):

- Significant rise in attacks against availability, particularly DDoS. DDoS attacks are getting larger and more complex, moving towards mobile networks and the Internet of Things and are being used in the context of cyber-warfare.
- Data breaches are increasing year on year. The central role of data in our society produced a sharp increase in the amount of data collected and in the importance of proper data analysis. The price we pay for such importance is a continuous and unstoppable increase in data breaches.
- Phishing is once again the most common vector for initial access. Advances in the sophistication of phishing, user fatigue and targeted, context-based phishing have led to this rise.
- Extortion techniques are further evolving with the popular use of leak sites.

Novel, **emerging threats** are marking the threat landscape with high impact:

- The Pegasus case triggered media coverage and governmental action, which also then was reflected in other cases concerning surveillance and the targeting of civil society.
- Machine Learning (ML) models are at the core of modern distributed systems and are increasingly becoming the target of attacks.
- AI-enabled disinformation and deepfakes. The proliferation of bots modelling personas can easily disrupt the 'notice-and-comment' rulemaking process, as well as the interaction of the community, by flooding government agencies with fake comments.

**Sectors most affected** by the evolving threat landscape:

- The most targeted sector is public administration and government bodies, which accounted for 25% of the observed number of cyber incidents. This is clearly a cause for concern for EU agencies such as eu-LISA.

Based on the above information, Mr Malatras summed up the key findings of the 2022 landscape as follows:

**Threats**





- Cyber-attacks are continuously increasing and becoming more complex and sophisticated.
- Cyber actors carrying out the attacks are becoming more organised, better funded, more coordinated and, in consequence, more efficient. Therefore, the risk level is rising.

**Countermeasures**

- Good practices and coordinated actions by all affected stakeholders are essential to reach a common high level of cybersecurity.
- Information and knowledge sharing among all stakeholders is at the very core of the fight against cyber-threats. It helps potential victims, researchers, industry and cybersecurity authorities such as ENISA to find solutions to new threats.

To wrap up his presentation, Mr Malatras pointed out that, over the 10 years in which the annual Threat Landscape Report has been produced, ENISA has been playing catch-up with cyber-criminals. Even if the report is highly useful in detecting new trends, it is still a reaction tool. ENISA has decided to add to their strategy a pro-action dimension and from next year they will use foresight tools to produce a new report on emerging and future cybersecurity threats up to 2030, in order to be ready for what is about to happen, before it happens. We need, Mr Malatras said, to be more active in the prevention, and not only on the cure.

**ENISA THREAT LANDSCAPE 2022 - HIGHLIGHTS**

-  Impact of geopolitics on the cybersecurity threat landscape
-  Threat actors increasing their capabilities
-  Ransomware and attacks against availability rank the highest during the reporting period
-  Novel, hybrid and emerging threats are marking the threat landscape with high impact

## LATEST CHALLENGES ON CYBER-THREATS AND CYBER CRISIS



**Mr Emmanuel Kessler**  
Head of Prevention and  
Outreach, Europol's  
Cybercrime Centre EC3

In the second presentation of session II, Mr Emmanuel Kessler from Europol EC3 discussed how the threat landscape is used in order to fight cybercrime from an operational point of view, and he gave an overview of the tools used by Law Enforcement Agencies, and in particular Europol, to bring the cyber-war to the real world in order to arrest and prosecute the criminals.

In particular, Europol operates on the basis of some permanent capabilities within the agency:

- Europol has a 24/7 operational centre that, in addition to other areas, covers cybersecurity.
- Europol runs the EC3 cyber intelligence as a means to investigate new cases after these are reported to the operational centre.
- Finally, Europol has the EC3 operational unit that acts based on the information provided by the intelligence team.

All these response teams in the agency coordinate with multiple stakeholders involved in the fight against cybercrime:

- It hosts and facilitates the efforts of the 'Joint Cybercrime Action Taskforce (J-CAT)' which includes Law Enforcement Agencies from EU Member States as well as third countries such as Australia or the US.
- EC3 also collaborates closely with other EU agencies, EU entities and strategic international partners, such as the European Commission, ENISA, the European Defence Agency, CEPOL, CERT-EU, the EU Cybercrime Taskforce, INTERPOL and NATO.
- Finally, Europol liaises continuously with the private sector, especially in the areas of internet security, financial services and communication providers.

All the previous capabilities and the coordination and collaboration with all relevant partners, Mr Kessler explained, allows in the end for EC3 to bring into life and efficiently operate the Law Enforcement Emergency response Protocol consisting of seven steps:

- STEP 1. Early detection and identification of a major cyber-attack.
- STEP 2. Threat classification of the attack.
- STEP 3. Emergency response and coordination centre.
- STEP 4. Early warning notification.
- STEP 5. Law enforcement operational action plan.
- STEP 6. Investigation and multi-layered analysis.
- STEP 7. Emergency response protocol closure.

As a way to showcase the full operational process and the intricacy of the fight against cybercrime from a law enforcement perspective, Mr Kessler went on to present some successful cases led by Europol:

**GoldDust – An emblematic example of cooperation.** As a result of the GoldDust operation, on 4 November 2021, the Romanian authorities arrested two individuals suspected of cyber-attacks deploying the Sodinokibi/Revil ransomware. The suspects were allegedly responsible for 5 000 infections, which pocketed in total EUR 500 000 in ransom payments. Operation GoldDust involved 17 different countries, Europol, Eurojust and INTERPOL. The arrests followed the joint international law enforcement efforts of identification, wiretapping and seizure of some of the infrastructure used by the criminals.

**VPNLab.net – Disrupting criminal capacities.** In 2022, again as the result of the joint coordinated effort of multiple law enforcement authorities, the VPNLab.net domain was seized and closed, following multiple serious criminal acts such as ransomware deployment. LEAs took custody of the 15 servers that hosted the domain, making it unusable.

**Operation tourniquet – Closing of RaidForums.** The operation was coordinated by Europol to support independent investigations of the US, UK, Sweden, Portugal and Romania. As a result, a full criminal ecosystem as well as an illegal marketplace were shut down, with the forum’s administrator and two accomplices being arrested. The hacking forum, which counted over 500 000 users, was considered one of the largest in the world. The forum sold access to database leaks belonging to a number of US corporations. The leaked information included credit cards, bank account numbers, user names, passwords...

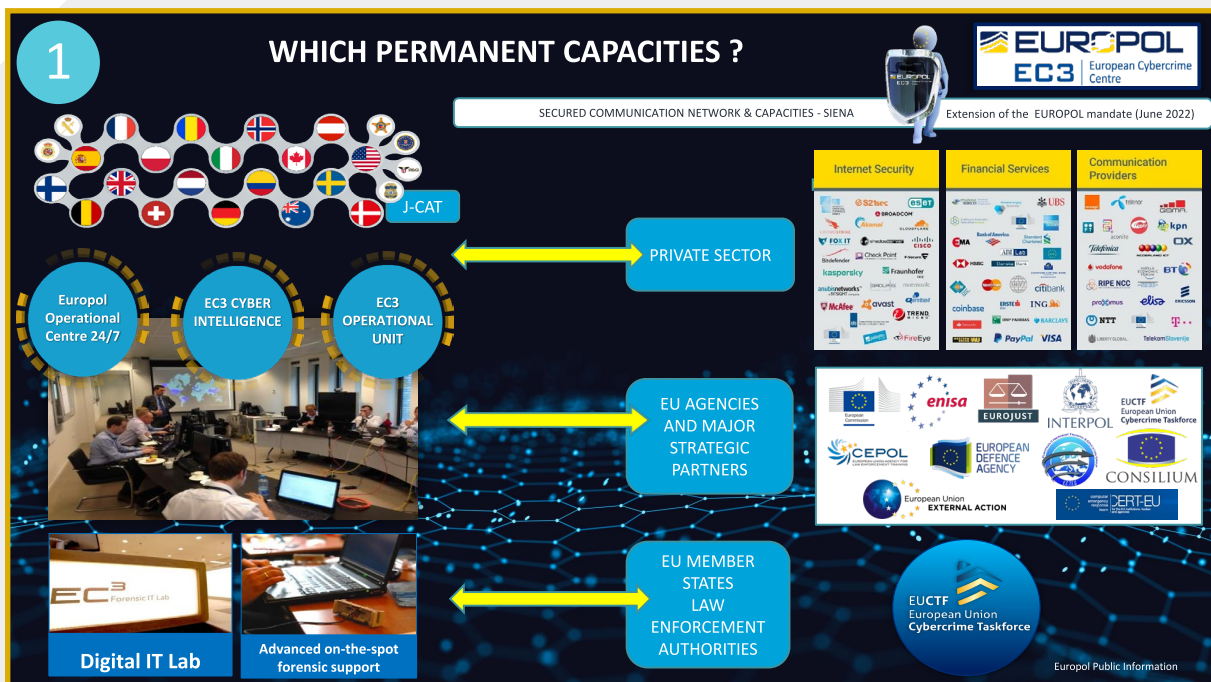
**HIVE Ransomware:** In the attack, criminals used the HIVE ransomware to copy data and then encrypt the files. Afterwards, they would ask for a ransom to both decrypt the files and to not publish the stolen data on the HIVE Leak Site. The ransomware was used to target businesses and critical infrastructure sectors, including government facilities, manufacturing, information technology and healthcare. The operation to dismantle the criminal network was led by Germany, the Netherlands and the US, involving authorities from 13 countries. In particular Europol EC3 provided support in information exchange, analytical support in cryptocurrency, malware, decryption and forensics.

As a result of the operation, around EUR 120 million were saved thanks to mitigation efforts, as the decryption keys were shared free of charge to the corporations affected by the ransomware attack.

After the successful operations showing the complexity of bringing cyber-attackers and cyber actors to justice, Mr Kessler explained what, in his view, were the next challenges for LEAs in the field of fighting cybercrime:

- The use of AI by attackers, which is difficult to detect or deter.
- The anonymity of criminals, which makes it in some cases almost impossible to track them down.
- The tracing of payments and communications.
- Cross-border jurisdiction in cybercrimes.

To face all these challenges, Mr Kessler concluded, there was only one possible way forward for all stakeholders involved in the fight against cybercrime, as demonstrated by the successful operations given in his presentation: **more cooperation, more collaboration, more knowledge sharing, more communication.**



## THREAT LANDSCAPE OF THE EU-LISA LARGE-SCALE IT SYSTEMS



**Mr Luca Zampaglione**  
Head of Security Unit,  
eu-LISA

To close Session II, Mr Luca Zampaglione, Head of Security Unit at eu-LISA, explained how the general threat landscape, which was introduced by ENISA at the beginning of the session, specifically applied to the Large-Scale IT systems managed by the Agency.

Mr Zampaglione also built upon the messages given by Mr Marc Sulon to open Session I, where the representative of DG HOME clearly explained the very serious consequences that would derive from any of eu-LISA's systems being compromised by a cyber-attack. In particular, should that be the case, the Schengen external border would have to be closed and, potentially, also the internal borders would need to be reopened.

Mr Zampaglione began by presenting the different changes that are currently being finalised by eu-LISA and that will eventually result in a turning point for the Agency. All these changes in the core business of the Agency will increase the threats to which the systems are exposed. The changes, Mr Zampaglione explained, can be summarised in three main areas:

**From a development perspective:** eu-LISA is shifting from being a mainly operational agency to being also an application development agency, with the new inflow of legislation where we are mandated to develop from scratch a relevant number of applications including EES, ETIAS, sBMS, ECRIS-TCN, JIT with more to come... In addition, we are managing major upgrades of the Central Business Systems currently in production. The development is also shifting to micro services technologies, DEVOPS pipelines and private cloud deployments. We have to make sure that all these in-house self-developed systems/apps/software do not introduce in the systems new vulnerabilities to cyber-threats, and that they are adequately secure by design.

**From an exposure perspective:** while at the moment our systems are isolated from the internet, EES and ETIAS will bring new challenges.

Our systems will be accessed not only from a controlled environment of only public institutions at MS and European level, but also by new clients such as:

- Sea, land and air carriers, by means of a dedicated extranet.
- Travellers, through new software such as dedicated mobile apps.

This new exposure considerably increases the security risk to cyber-threats as well as our appeal to potential attackers.

**From an architectural perspective:** the interoperability project will further push the paradigm shift started with the collaboration of EES, VIS and sBMS. Interoperability changes the core architecture of our systems from silo-based (dedicated HW and SW elements) to systems that share application core elements like front-end query ESP (European Search Portal) and core data bases like the CIR (Common Identity Repository) or the MID (Multiple Identity Detector). This push is even more relevant for the new Internet Zone, where we have shared many application components on top of a platform as a service. We have to make sure that such design does not increase the vulnerability to cyber-threats of our environment and that we take specific containment measures.

Mr Zampaglione explained how all these changes in the business of eu-LISA accounted for a new reality both in the internal and external network of the Agency, of highly granular, highly exposed and highly uncontrolled sets of new potential vulnerable points for cyber-attacks. Therefore, the Agency needed to put in place the necessary safeguards to properly address the new threat landscape.

However, Mr Zampaglione continued, the protection of the systems could not be at the expense of their usability. It was of little value to have unbreakable and unhackable systems if they could not be used. **A balance between security and efficiency had to be reached.**

To do so, Mr Zampaglione emphasised the need to rely on the Agency’ mandate. In particular, based on the regulations of each of the systems, the Agency, through the security team, develops security plans to ensure physical protection of critical infrastructure, facility access control, user control, data storage control, data access control, communication control and also self-auditing.

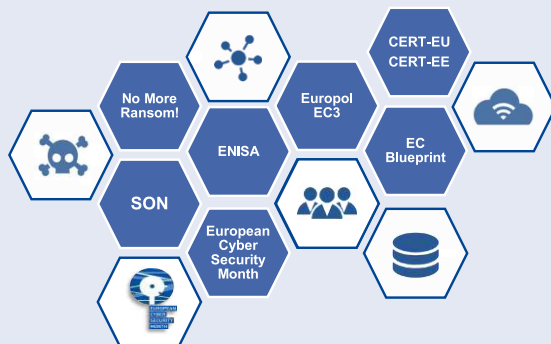
The goal of these plans is to ensure the continuous, effective and secure operation of the systems. To do so, the focus must be placed on the confidentiality, integrity and availability of data. All this can only be achieved through the shared responsibility of eu-LISA and of the other stakeholders connected to the systems, especially the Member States.

Finally, Mr Zampaglione stressed the key message to reach the common goal of increasing the cyber resiliency of the Large-Scale IT systems: **COOPERATION** between eu-LISA, the European Commission, ENISA, Europol, the European Data Protection Supervisor (EDPS) and, above all, the Member States through their different border management and Law Enforcement Agencies.

To make this cooperation a reality, eu-LISA works on different levels:

- Cooperation through the Security Officers Network with MS, EU Commission and agencies operating in the Justice and Home Affairs domain.
- Development of a security cooperation group under the interoperability framework.
- Multi-stakeholder coordination: National Centres for Computer Emergency Response Teams (CERTs) and CERT-EU, security services and the private sector.
- Exchanges of best practices.
- Strengthening of security through harmonised community security plans.
- Building a Computer Security Incident Response Team (CSIRT).

### 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





## PANEL DISCUSSION

Chair:

**Mr Geoffrey Choo**

Head of Cybersecurity  
Operations Sector, eu-LISA

Panellists:

**Mr Marc Sulon**

EC DG HOME

**Ms Boryana Hristova-Ilieva**

EC DG CNECT

**Mr Apostolos Malatras**

ENISA

**Mr Emmanuel Kessler**

Europol

**Mr Luca Zampaglione**

eu-LISA

## PANEL DISCUSSION

**Mr Marc Sulon (EC DG HOME) | Ms Boryana Hristova-Ilieva (EC DG CNECT)**

**Mr Apostolos Malatras (ENISA) | Mr Emmanuel Kessler (Europol) | Mr Luca Zampaglione (eu-LISA)**

The first topic of the panel discussion focused on the protection of personal data and what can be done from the legislative perspective to encourage industry to provide better privacy-enhancing solutions for our systems, including data anonymisation, homomorphic encryption, in order to further reduce the impact of potential data breaches.

Mr Sulon responded that defining specific requirements on the implementation of data protection legislation was not the responsibility of DG HOME. 'What we are interested in are solutions that enable data to be accessed without the need to expose data. We need to ensure that the data we have is used as much as possible within the legal constraints, but at the same time the data is protected from possible data breaches. In that sense, the possibility to work on encrypted data without decrypting is essential to reduce the risk.'

The second question focused on the implications of the NIS2 directive and the Cyber Resilience Act for the systems operated by eu-LISA. In her response, Ms Hristova-Ilieva explained that the purpose of the NIS2 directive is to increase the overall cyber resiliency of the networks and information systems involved in critical services, whereas the CRA focuses on ensuring that the whole supply chain for components or software placed

on the market meet certain criteria, and therefore ensure the cyber resiliency of the EU, including public-sector organisations. Similarly, the Cyber Resilience Act would be to the benefit of all users who use solutions with digital components, which means that end users, SMEs and public administrations will all benefit from the higher level of assurance introduced by the CRA. She emphasised that the specific measures will be based on the cybersecurity standards that are already in use at Member State level.

The discussion then focused on the main cybersecurity threats that ENISA, Europol and eu-LISA foresee in the coming years. Mr Apostolos Malatras (ENISA) began by stating that the chance of being wrong when trying to predict what will happen in the future is very high. 'What is important to note is the increasing sophistication of all types of attacks. Another important aspect is the security of supply chains, in particular due to the potential detrimental impact of attacks on supply chains, considering that the software systems that are being built are increasingly becoming component-based. Therefore, if one of the components is compromised, it may affect a large number of users. This is something that is often being exploited by adversaries, because with just one successful hit, they can affect a large number of entities, as we have seen in the case of SolarWinds, for example.'



The third major challenge is the change in the nature of the attacks. Whereas previously, the attacks were mainly IT-focused, these days, we are increasingly facing hybrid threats, including disinformation and so on. These are more challenging as we are often not prepared to effectively deal with those, considering that they require a skill set different from what a typical cybersecurity engineer possesses. This requires a paradigm shift with regard to how we are dealing with these challenges, and therefore requires much closer collaboration and information sharing among the entities involved across different domains, including IT, law enforcement, cybersecurity, diplomacy, etc.'

Mr Kessler (Europol) added that attacks focusing on capturing data will become increasingly important. Ransomware and malware attacks will remain a major concern as well. Furthermore, crime as a service has become far more professional; cybercriminals have become much more professional and organised.

Mr Zampaglione (eu-LISA) focused on disinformation as one of the key threats today and in future. From eu-LISA's perspective, criminal organisations already today widely deploy disinformation to defraud individuals seeking information about travel to the EU, by way of creating websites mimicking official websites for the EES or ETIAS, even though the systems are not yet in operation. Another important aspect is the possibility of misconfiguration in the software that we operate. This is especially important with custom-made software, where misconfiguration leading to vulnerability can be done by mistake and in good faith. Hence, particular care is needed when performing penetration testing.

Mr Sulon added that one of the areas that constitute a potential threat is the end user, in particular access control to the systems. This is a major challenge, considering that some systems have or will have a very large number of end users. For example, today the SIS is used by several hundreds of thousands of persons in Europe, which poses a challenge, as the system contains large amounts of highly sensitive information.

The panel then moved on to discussing the different practices that can help in dealing with these threats. Mr Malatras acknowledged the importance of focusing on the end user as a vulnerability; however, he also challenged the panel, asking whether we, as security professionals, have done enough to ensure that the systems that we develop and operate are developed in a way that users of those systems don't fall victims as easily.

For example, phishing emails have been around for over 20 years, however, we still have very few effective solutions protecting the end users by blocking malicious URLs, etc. One of the challenges is that the systems we operate have different requirements and risk levels, therefore, we can't have a one-size-fits-all solution.

We need to have targeted approaches depending on the criticality of systems and risk levels from both technical as well as regulatory perspectives. What we can do is achieve a certain level of harmonisation with regards to standards we apply, reporting requirements, etc. which would allow us to build a certain level of cyber resiliency. And both the NIS2 and the CRA contribute to building this solid foundation of cyber resilience.

Another important aspect is information sharing between authorities, in particular with regard to cybersecurity incidents and how those are being addressed. Sharing such information may be very helpful in prevention and response by other authorities.

Finally, it is essential to ensure that legislation focusing on cybersecurity and cyber resilience is harmonised in terms of requirements, to avoid duplication and full coherence, as well as trust among the authorities involved.

One of the questions from the audience focused on the importance of penetration testing, cybersecurity audits, and other technical measures, which were not addressed by the panel. Mr Malatras clarified that the reason these were not explicitly mentioned is that these measures, such as cybersecurity audits, reliance on trusted providers of software and hardware, etc. are a baseline from which to start.

Another question focused on what could be changed in the legislative framework to further enhance cybersecurity, if it were possible. Mr Sulon explained that regular revision of the applicable legislation is a standard process in the Commission, which takes place every five years on average. Furthermore, the regulations covering the Agency and the systems are rather general in terms of how the risks are defined, thus ensuring that the legislation doesn't need to be revised every time there is a new trend in a threat landscape, for example.

What needs to be ensured in the future is that regulations are technology-neutral as much as possible to make sure that the systems can be built and updated in line with the development of technologies. Mr Zampaglione seconded the statement of Mr Sulon, explaining that the regulatory framework should only set the necessary requirements, but not define the technologies or approaches these requirements must be met with.

The last question from the audience focused on the aspect of the skills shortage in the area of cybersecurity and its effect on the ability of the EU to deal with the rise in cyber threats. Mr Malatras explained that the skills shortage is being observed across the EU. Vice-President Schinas and his cabinet are actively working on promoting the skills agenda, as part of which the European Cybersecurity Skills Academy has recently been launched, which is an initiative focused on addressing the shortage of cyber skills in Europe.

The initiative includes awareness raising, training, cyber competencies, etc. With the continuous digitalisation and proliferation of automation, AI, etc., the need for cybersecurity skills will continue to increase, hence the need to continue growing the number of professionals skilled in cybersecurity. Mr Kessler agreed that growing the number of people skilled in cybersecurity is essential. He emphasised that development of cybersecurity skills is essential across the board and at different levels, starting from basic skills that are necessary for investigating cybercrime, to the more sophisticated skills necessary for analysing crypto-currency transactions and for decryption.

The final part of the panel discussion focused on Chat-GPT and the associated threats and opportunities in this area. Mr Kessler emphasised that AI will revolutionise law enforcement. Therefore, in order to keep up with the criminals, the use of automation and AI is essential. For example, in dealing with the EncroChat and Sky ECC cases - apps used for encrypted communication - where Europol had to process around 500 million messages. It is simply not feasible to process such an amount of data without the use of automation and machine learning tools.

Mr Zampaglione emphasised the fact that with the increasing use of AI, including in the development of software that we use, may lead to the loss of skills and knowledge that is necessary to understand the code in which the software is written, thus undermining our ability to identify vulnerability in the software and fix those issues. Therefore, especially in case of mission-critical systems, it is essential to resist the tendency to rely on AI.

Mr Sulon emphasised that AI is a tool and as with any tool, the outcome depends on the application. It can be used by criminals for criminal intent, but it can also be used by us to protect our systems from criminals. It is therefore important to focus on the application of the technology, instead of simply branding it as something either good or bad.



# DAY TWO

SESSION III

## TECHNOLOGY SOLUTIONS FOR THE IDENTIFY AND PROTECT FUNCTIONS OF THE CYBERSECURITY FRAMEWORK

Chair:

**Ms Eleni Antoniou**

Head of Information and Assurance Sector, eu-LISA



## BAMF: FROM REACT TO ACT



**Mr Kausik Munsu**

Chief Technology Officer,  
German Federal Office for  
Migration and Refugees,  
BAMF

Mr Munsu opened his presentation with an overview of activities performed by the German Federal Office for Migration and Refugees (BAMF), which has over 8 300 employees, including around 900 internal and external IT staff supporting approximately 150 IT products.

One of the key challenges for the IT department in BAMF is the volatility of workload, specifically connected to immigration crises, such as the one that took place in 2015-17 and since the beginning of the war in Ukraine.

Mr Munsu continued the presentation with an outline of the development of IT security in Germany, which started in 1950 with the creation of a Central Department for Encryption, a branch of the German Intelligence Service. BSI, the German Federal Office for Information Security, was created in 1991 to focus specifically on information security due to the increasing reliance on information technologies in the public sector and beyond. In addition to the BSI, each Federal Ministry and Agency have their own cybersecurity department.

Currently, Mr Munsu continued, the Cybersecurity Architecture of Germany is a complex network of domestic and international agents (an overview is available here: <https://www.stiftung-nv.de/en/publication/germanys-cybersecurity-architecture>).

Focusing on asylum processes, Mr Munsu emphasised that the process is integrated with the EU large-scale IT systems, such as the Visa Information System, the Schengen Information System and Eurodac. In future, these processes will be connected to other systems, and will consume and provide a growing number of digital services.

Effective operation of this network requires a certain level of trust, which can be achieved with the help of a strong cybersecurity strategy and framework. BAMF started its focused work on cybersecurity in 2005 with the introduction of web services.

To ensure security, BAMF had to develop a secure gateway, as well as solutions of strong authentication and federated identity management with delegated administration of identities, which was accomplished in 2006. However, the biggest challenge came between 2014-2016, when more than a million refugees entering Germany had to be processed. This required scaling vertically in terms of servers, storage and network, as well as horizontally, in terms of the services provided, including the provision of mobile registration workstations.

After the crisis was over, in 2018 BAMF introduced a digital transformation strategy, with the objective of building a modern, flexible and agile agency, capable of responding to these kinds of challenges. This digital transformation involved the adoption of cloud-based or cloud-native architecture, microservices-oriented continuous deployment, as well as a cybersecurity framework enabling digital trust.

The most recent challenge that BAMF has faced is that, with the entry into force of the NIS2 directive, BAMF is considered critical infrastructure, which puts additional emphasis on cybersecurity.

To respond to this, BAMF has developed a comprehensive multi-layer security framework Igloo for Security. At the centre of the Igloo are assets, which are protected by different isolation layers (eight layers covering all aspects, ranging from data protection, to network protection, to device and development protection).

In the beginning most of the focus was on protection of infrastructure; however, with time BAMF realised that protecting applications is as important. One outcome of this was the introduction of secure coding practices, as well as code scanning tools (static and dynamic code analysis), as well as the use of memory-safe programming languages.

Another important element in ensuring data protection was the implementation of separate read and write accesses, as well as token exchange, which enabled secure implementation of micro-services. To ensure this, BAMF has implemented service mesh and cascade calls.

The other important aspects of the cybersecurity framework are attribute-based access and self-sovereign identity. This new approach to identity management is more suitable than the more traditional roles-based approach, as it is impossible to track the huge number of roles possible in the micro-services architecture.

Next layer in the protection framework is the development protection layer. BAMF relies on a large number of external contractors, software libraries and code in the development of systems.

To deal with some of the challenges, BAMF has introduced an internal artefact repository, where external artefacts and code are tested before being launched in the operation environment. Developers use external resources only from this repository, where those have already been pre-cleared.

In closing, Mr Munsu emphasised that it is not possible to buy security or build an absolutely secure system or organisation. Security is a continuous process.

## Conclusion



- You can't buy Security
- You can't reach an absolute secure state in an organization
- You can't build fully secure systems
- Security has to be seen as a *continuous process*

- The *information* is there, the *methods* are there, the *tools* are there; and most importantly: The *people* are there
- 5 Dimensions need to be combined in the right context: *Information, Awareness, Organization, Process, and Technology*

If we stop or slow down in keeping up with continuous developments, we will give up advance *act instead of react*

## ENTRUST: POST QUANTUM WORLD & ZERO TRUST



**Mr Mamdouh Al-Gendy**  
Sr. Technical Sales  
Consultant, Entrust

Mr Al-Gendy opened his presentation with an overview of the recent achievements in the area of quantum computing, which allows certain mathematical problems to be solved significantly faster than with traditional binary computing. He emphasised that, although consumer-grade quantum computers may appear as something unattainable in the near future, there are indications to the contrary, in particular with companies based in China claiming to aim at putting on the market consumer-grade quantum computers priced at USD 5 000 in just a couple of years. This poses a fundamental challenge to our approach to cybersecurity.

Today, breaking encryption of the industry standard public key encryption system is impractical with the computational resources available to hackers.

With quantum computing, traditional cryptography becomes irrelevant, as the time required to break current state of the art cryptography will be measured in minutes.

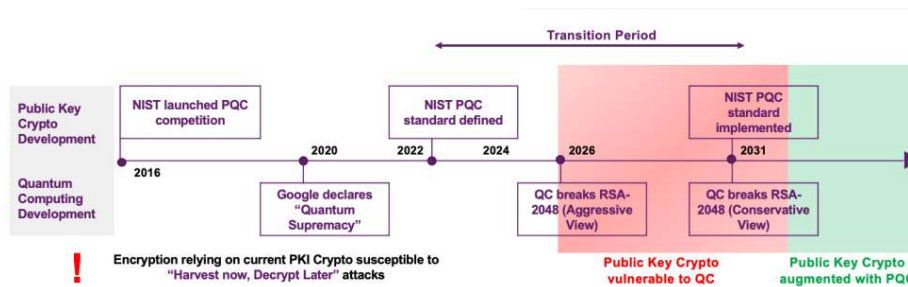
At the moment, among the rest of the world, the US is leading in terms of preparedness to post-quantum cryptography, specifically with the development of standards and technologies. He continued his presentation with an overview of a market survey on preparedness to post-quantum threats, where more than half of companies (including both medium and large enterprises) indicated that they are either not aware or have not started preparations for post-quantum threats.

To face these new threats, companies and public sector organisations need to start preparing now, starting with assessing the current use of cryptography, as well as the potential future needs and the resulting demand for specific competencies and capabilities.

In closing, Mr Al-Gendy suggested that preparedness for post-quantum cryptography in the future will be similar to compliance with cybersecurity requirements today, namely that it will require an assessment of compliance, etc.

### QUANTUM THREAT AND EXPECTED TIMELINE

- › Quantum computers will be able to break current public key encryption
- › Accurate crypto inventory & mitigation strategies are required
- › Long term data needs to be protected not then, but now
- › Failure to migrate leaves applications and data at risk of compromise.





## iPROOV: IDENTIFYING, DEFENDING AND PROTECTING AGAINST EMERGING THREATS TO BIOMETRIC FACE VERIFICATION



**Ms Gemma Bird**  
Head of Biometric  
Platform, iProov

Ms Bird opened her presentation by explaining that the threat of synthetic imagery was acute and not something that would materialise in the distant future - synthetic imagery is already being used to attack production systems that use biometrics for authentication. She then presented the user experience in using remote authentication solutions when applying for a bank account or interacting with public services.

First, an identity document is scanned using a camera or NFC reader. Then, the picture stored in the chip or on the photo-page of the document is compared with a live image captured using a smartphone camera. In order to ensure liveness detection and protection against injection attacks, a unique sequence of light is used to illuminate the user's face when capturing the live image. The captured information is then sent to the iProov service for analysis.

Ms Bird then explained the differences between presentation attacks and injection attacks. Whereas presentation attacks have limited scalability and are well-known and therefore solutions and standards already exist, injection attacks are much more challenging, as those can be automated and therefore scaled indefinitely. Detection of injection attacks can be done by analysing metadata or imagery-based testing.

However, there are no standards at the moment on the detection of digital injection attacks, which makes it difficult to compare the performance of different biometric systems against this type of attacks.

iProov provides services to millions of users, and they spot digital injection attacks aimed at their system used for biometric authentication in the hundreds per week. The main concern is the rapid evolution of digital injection attacks, which are now made possible by widely available tools, which can be used without any expert knowledge, which leads to a significant growth in these kinds of attacks.

In addition to such off-the-shelf tools, criminals are also developing custom tools that are pushing the boundaries or detection capabilities.

Ms Bird continued her presentation by outlining a few approaches to address this challenge. The first approach is based on the use of metadata, which sometimes allows analysts to detect whether an injection has occurred on the basis of the information that comes from the devices.

This information, however, can be forged. Another approach is based on the analysis of imagery, aimed at determining whether the imagery comes from a bona fide user. This cannot be perfectly forged, for example by making sure that the data gathered is hard to synthesise (e.g. random flashes of coloured light or specific movement patterns).

iProov uses a combination of metadata-based algorithms with imagery-based algorithms to enhance the security of their detection system. As the data processing takes place in the cloud, iProov has a comprehensive overview of the attacks taking place across multiple platforms and geographies.

This, in turn, enables it to witness the evolution in the attacks and tools used by criminals. As a result, it is possible to learn, adapt and re-train the algorithms to ensure that they are effective in identifying new types of attacks.

The questions from the audience focused on a number of aspects pertaining to the solution presented by iProov. The first question was on the lighting conditions within which the solution had been tested. Ms Bird confirmed that the solution had been tested and validated in a variety of lighting conditions.

The second question focused on the quality of the image originating from a document used for comparison against the live image. Ms Bird explained that iProov is working with partners providing solutions for document capture using either NFC or a smartphone camera.

The solution provided by the partners help ensure that the authenticity of the document is also verified.

Another question focused on specific use cases in which the solution provided by iProov is being used. Ms Bird explained that the solution has been used for a number of years with live customers, which include such use cases as online customer onboarding in the banking sector.

In case of Rabobank, the solution is used to validate identity when transferring from a child account to an adult account when a client reaches the age of majority, which previously required driving to a bank branch.

Another use case in the banking sector is higher level of identity verification for higher-level transactions. The solution is also used in the public sector in the US, for example in the context of tax reporting. Anything that can be considered as a high-risk transaction can be considered a good use case for this solution.

## SPLUNK: ELIMINATE YOUR ALERT FATIGUE – RISK-BASED ALERTING



**Mr Johan Bjerke**  
Principal Security  
Strategist, Splunk

The presentation focused on the security operations centre (SOC) and the solution to reduce alert fatigue using a risk-based approach.

The problem that the contemporary SOC faces is a very large number of alerts that are being put into a queue, leading to long resolution times.

Many organisations have around 10 000 alerts per day in a queue. It is not feasible for human analysts to process such number of alerts; as a result, SOC analysts are overworked and a significant proportion of the alerts are abandoned (those with lower levels of risk).

Mr Bjerke suggested that what needs to be changed is the detection methodology, which has for a long time been based on a certain detection logic, which identifies logs and pushes those to be further analysed by human analysts.

This has been happening for some 30 years at least. The attack surface of organisations today is so big that this kind of detection approach does not work.

Therefore, what is needed is a risk-based approach to alerting. This is something that has been used in financial institutions, which analyse risks connected to transactions.

This same approach can be applied in the cybersecurity context, by assigning specific risk values to particular actions and by assigning those scores to a particular device, component or application.

As a next step, an additional detection logic is applied that is time-bound, for example, assessing risk allocation to particular entities during a period of one hour.

If a certain entity has been assigned with a risk score exceeding a certain pre-set threshold, an alert is created, which is then entered into a queue for further assessment by human analysts.

Deploying such an approach leads to drops of up to 80% in security alerts and of up to 30% in false positives.

Mr Bjerke then provided a number of examples showcasing how the adoption of a risk-based approach led to a significant reduction in event abandonment rates due to the significantly lower number of alerts (daily notable events reduced by 10x).

The overall outcome was an 80% reduction in alerts, a doubling of alert fidelity, and a 90% reduction in the time needed for investigation.

To support clients in adopting risk-based approaches in alerting, Splunk has published a book entitled *The Essential Guide to Risk-Based Alerting*.

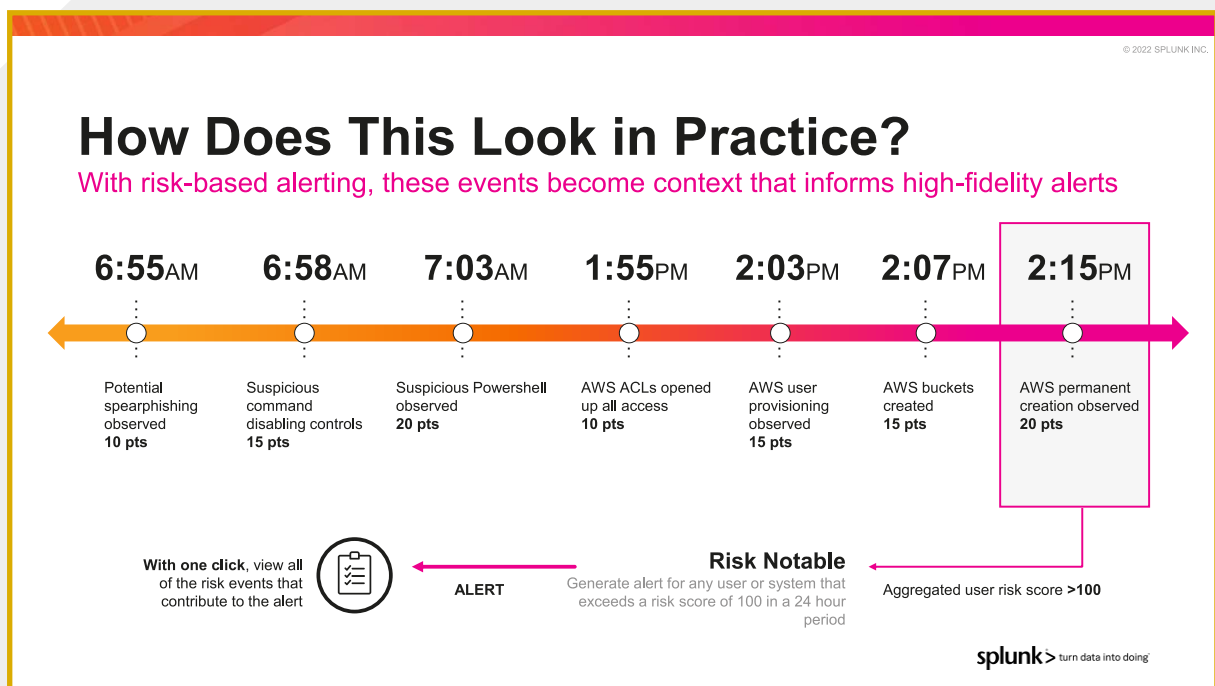
A question from the audience focused on the issue of risk subjectivity and the fact that teams dealing with alerts may tend to over-exaggerate the risks. How did Splunk deal with this? Mr Bjerke responded that Splunk essentially provided a platform with a number of components, some of which indeed included standardised risk settings for different events.

Although everything was pre-configured out of the box, everything could be adjusted according to the requirements of a particular environment or user.

Another question from the audience focused on the importance of sharing information about risks among authorities using such risk-based approaches.

Were there communities around risk-based alerting? Mr Bjerke responded that there was in fact a public forum for risk-based alerting SOCs, which was run by a company called Outpost Security.

Splunk also published a lot of open-source material, including the detection library with risk indicators.



## SECUNET: SINA SOLID - SECURE DYNAMIC VPN NETWORKING



**Mr Ronald Westerlaken**  
Sales Director EU  
Organisation &  
Institutions, secunet

Mr Westerlaken presented a solution developed in collaboration between Secunet and the University of Ilmenau, which addresses the challenges associated with configuring large VPN networks, which, in the traditional set up have challenges with scalability, result in high administrative effort and are increasingly prone to errors.

In a traditional VPN, the failure of a single node has severe repercussions for the entire network. The main objectives for the development of a flexible solution were: self-configuration, support for nested networks and private IP address ranges, scalability and agility, protection of confidentiality, integrity and authentication, as well as resilience to DDoS attacks.

On the basis of these requirements, secunet developed the SOLID concept, which stands for Secure OverLay for IPsec Discovery, which dynamically auto-configures IPsec-based security associations in the VPN overlay network.

SOLID provides the following benefits: reduction of operating expenses; eliminates the need for load balancers; automatically takes over ongoing connections in the event of failure in <10 seconds; provides real-time monitoring of the SOLID devices, supporting automatic detection and response.

One of the key benefits of SINA SOLID is that it is dynamically scalable with limited need for manual set up.

Following the initial pre-configuration, the gateways participating in the network will automatically re-arrange themselves within the network, thus significantly reducing the need for manual set up, which would normally be very high in a traditional network.

In addition to the standard premise-to-premise connection, SINA SOLID also enables client-to-premise and client-to-client connections, which allows direct connections between the clients even if the central network has failed.

A question from the audience focused on the possibility of a similar solution to be deployed in the post-quantum context. Mr Westerlaken explained that this particular solution was developed together with the German BSI in compliance with the requirements for the EU SECRET level of communication security.

In the future, secunet will also be working on bringing similar solutions to less restrictive communication environments, where solutions focusing on post-quantum cryptography can also be implemented.



SESSION IV

**TECHNOLOGY  
SOLUTIONS FOR THE  
DETECT FUNCTION OF  
THE CYBERSECURITY  
FRAMEWORK**

Chair:

**Mr Aleksandrs Cepilovs**

Capability Building Officer – R&D, eu-LISA

## CERT-EU: DETECTION IN THE CLOUD



**Mr James Barr**  
Cloud Engineer, CERT-EU

Session IV of the Industry Roundtable was opened by Mr James Barr, computer engineer at CERT-EU, who addressed one of the main challenges faced currently by many organisations: the transition to the cloud and ensuring cyber resilience in this new reality through efficient detection.

He started his presentation by explaining how 'smart logging' of the commands in the system, and the correct visualisation of such logs, is essential to be able to use the data and to detect anomalies.

Rather than simply logging the raw data, Mr Barr explained, great gains can be obtained from: visualisation tools such as dashboards and pre-processing of the raw data to log only metrics of that data that can be interpreted.

To showcase these principles, he gave a practical example of the improvements achieved through this strategy from a human analyst perspective, in a simple client/server system operating before the cloud.

He then went on to explain the main difference between that old, simple system, with the current 'cloud era'. The modern cloud environment is characterised not only by the number of devices interconnected but also by the diversity of these devices.

In order to be able to monitor this very complex and intricate network, analysts still use similar principles to the ones explained in the initial simple example: dashboards and visualisation tools; a full logging infrastructure to cope with the huge amount of data produced by the environment.

While the principles remain similar, visualisation and logging of processed data, new questions arise, primarily: what data to include in the logging and visualisation, since now the amount of actions available is too large for humans to monitor.

To help in this task, there are automation tools on the market that are able to analyse all the different inputs from the system and detect potential threats in order to report them to the analysts.

From a hands-on perspective, Mr Barr explained how the main problem with these tools is the cumbersome manual configuration of the software, setting the detection rules that should be applied among the thousands of them existing for systems in the cloud.

Another difficulty that Mr Barr has encountered in the cloud is the very large number of query languages that exist and which are almost impossible to learn and master fully.

Those languages are essential to set detection rules and respond, to create threat-hunting rules, to create alerts in your system, to create metrics that you want to visualise and also for pattern matching.

In essence, it is important to select tools that have integrated simple query languages that are easy to learn, and which the tool then automatically translates to communicate with the different modules and systems within the network.

To sum up the information provided so far in his presentation, Mr Barr said that, from his large experience in the field, the cloud environment not only brings consistency, overwhelming richness and possibilities in the use of systems, but it also brings constant evolution and is still lacking in automation, especially in the configuration of those systems, including the cyber-threat detection tools.

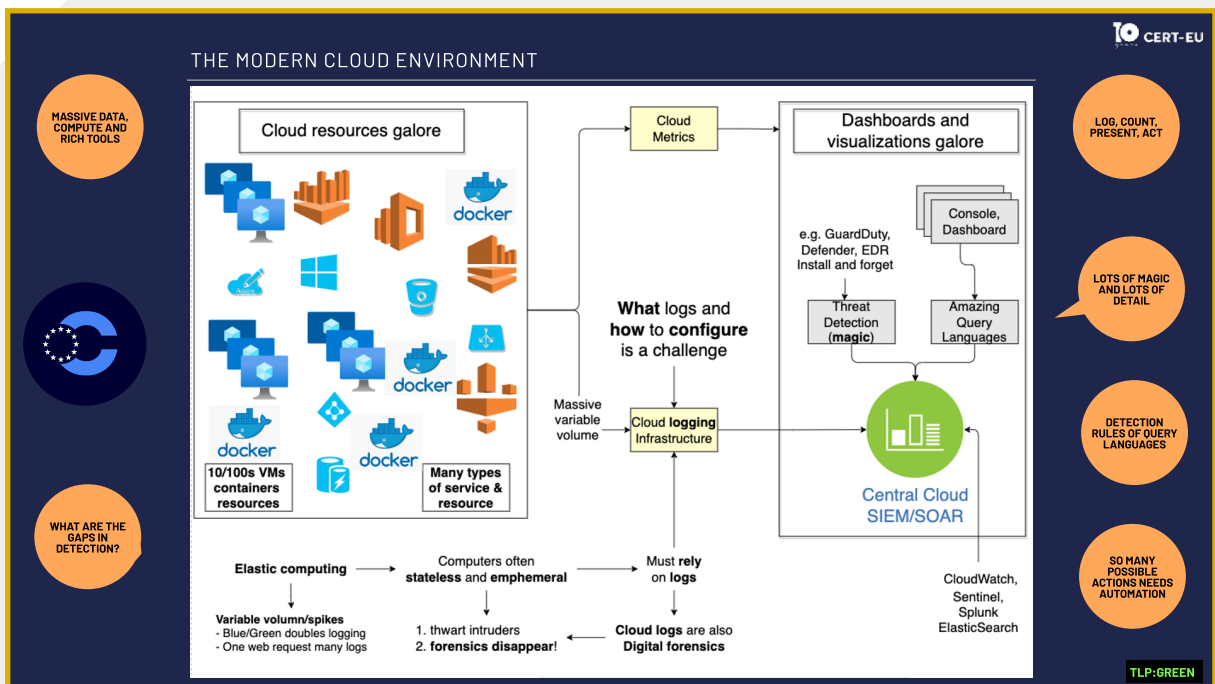
Another important point raised by Mr Barr was the cost in terms of efficiency and potential security threats of the multiple software and resources that are created and 'abandoned' in the systems, such as proofs of concept, unused features, legacy software, old versions...

In the cloud it is very easy to query the resources available, so a key message is to remove any of the resources that are no longer needed in order to keep the overall environment 'tidy'.

Regarding security, the cloud also brings some advantages with respect to the previous environments.

In particular, in his experience Mr Barr has found that development languages for the cloud are more open and therefore the software engineer can integrate quite seamlessly the security assessment within his development process.

To conclude his presentation, Mr Barr gave a clear message: 'I am sure that many people are very aware of what and how to detect cyber threats and how to respond. However, I feel much work still needs to be done to package it all up, automatically, seamlessly and efficiently.'





## NTT DATA: ACTIVE THREAT MANAGEMENT - A HOLISTIC APPROACH TO ENSURE CYBER-RESILIENCE AGAINST EMERGING THREATS



**Mr Panagiotis Iliopoulos**  
Senior Manager,  
NTT DATA

After the opening presentation by the European institution CERT-EU, session IV featured 4 presentations by industry, the first of them provided by Mr Panagiotis Iliopoulos from NTT DATA.

After a brief presentation on the cybersecurity department within NTT DATA, Mr Iliopoulos started the technical part of his presentation by pointing out some of the existing key challenges in the cybersecurity field that most corporations/institutions face from a management perspective:

- Convergence of virtual, physical and digital corporate environments.
- Digital transformation, automation and transition to the cloud.
- Adoption of the hybrid working model (in person and telework).
- Implementation of the growing regulatory framework.

In the view of Mr Iliopoulos, while in many corporations the level of awareness regarding cybersecurity threats has certainly increased over the last years, there was still a lack of effectiveness in the way the four key challenges mentioned above are being managed, especially in terms of information security, budget allocation and onboarding of new paradigms such as the Zero Trust philosophy.

From a general point of view, the inefficacy of most strategies implemented in cybersecurity threat management, according to Mr Iliopoulos, was that they were focused on a single investment at one point in time, and not on a continuous adaptation to the evolving threat landscape.

To solve these inefficiencies, the speaker presented a new approach based on 'holistic active threat management'.

The proposed framework is built on two main pillars:

- Active definition and continuous update of the threat profile of the organisation.
- Active detection of new cybersecurity threats, and not only reaction against known threats.

In practice, these two pillars are achieved through a number of key activities that should be embedded in the core business of any organisation:

- Continuous self-scouting to identify areas of improvement.
- Interaction with core cybersecurity processes.
- Testing of the detection processes via pen testing and red teaming.
- Compliance with best practices, internal policies and regulations and standards.
- Clear definition within the organisation of roles and responsibilities.

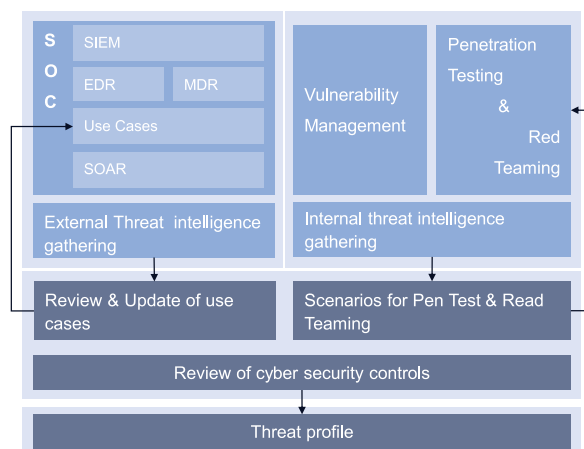
According to Mr Iliopoulos, this proposed framework of active threat management is the way in which organisations should move forward in order to face the new challenges in cybersecurity, especially the new hybrid threats, which can be defined as a mixture of coercive and subversive activities, conventional and unconventional methods, that are used in a coordinated manner by state or non-state actors to achieve specific objectives (e.g. disinformation, alternative facts, defamation, social engineering...).

### Active Threat Management Components

#### Holistic active threat management approach

Continuous process to manage cyber security related threats that is comprised by two sub processes:

- Active definition and continuous update the threat profile of the organization
- Active detection of cyber security threats



## UNDERSTANDING MITRE ENGAGE DECEPTION FOR ADVERSARY ENGAGEMENT, EARLY BREACH DETECTION, AND IMPROVED INCIDENT RESPONSE



**Mr Wouter Marien**  
Account Director,  
SentinelOne

The second industry address of the session was delivered by SentinelOne. Mr Wouter Marien presented a new approach for protection against cyber threats based on deception.

The speaker started engaging with the audience with some famous successful examples of deceptive strategies used in the past during war, such as the Trojan Horse, as illustrated by a quote by Mr Winston Churchill during the second World War: 'in wartime, truth is so precious that she should always be attended by a bodyguard of lies'.

Based on this principle, MITRE's Centre for Technology & National Security in the US, has published a new protection approach against cyberattackers consisting of using part of their own weapons against them.

According to SentinelOne, the new paradigm for cyber resilience allows an organisation to improve in key areas such as:

- Find and manage adversaries.
- Learning adversary techniques to better inform the defence teams.
- Find insider threats.
- Have a better, faster more efficient incident response.

All this can be achieved through the 'judicious use of networks, pocket litter, and honeypots can waste the adversary's time and resources, expose their pedigree, and create false knowledge on their part.

Deception can also add randomness and unpredictability to an architecture, network traffic, service, or mission activity, making an adversary's understanding of the environment more challenging and, at best, inaccurate'.

To clearly define and explain their strategy and the different concrete actions that can be undertaken to apply it, MITRE has released a publicly available guide called ENGAGE, cataloging measures that organisations should take to actively engage with and counter intruders on their networks.

In particular, the objective of adversary engagement is to learn how our adversaries attack us, what tools they use, what they will do after they establish a point of entry to our systems, and, in summary, insights into what they are seeking. Adversary engagement can be achieved through two main actions that should be used together with strategic planning and analysis:

- Cyber denial, which prevents or impairs the adversary's operations.
- Cyber deception, which reveals deceptive facts to mislead and confuse the adversary.

Mr Marien finalised his very interesting presentation by explaining the ten key iterative steps that go into applying the ENGAGE framework:

**PREPARE**

- **STEP 1.** Assess knowledge of your adversaries and your organisation.
- **STEP 2.** Determine your operational objective.
- **STEP 3.** Determine how you want your adversary to react.
- **STEP 4.** Determine what you want your adversary to perceive.
- **STEP 5.** Determine channels to engage with your adversary.
- **STEP 6.** Determine the success and gating criteria.

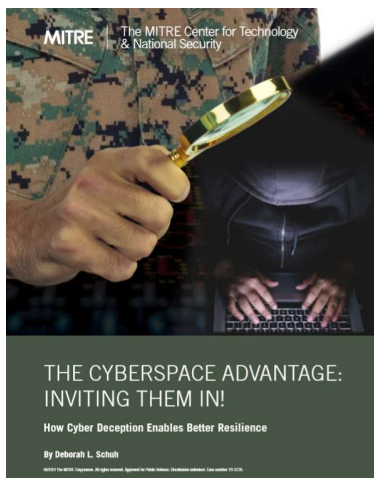
**OPERATE**

- **STEP 7.** Execute your operation.

**UNDERSTAND**

- **STEP 8.** Turn raw data into actionable intelligence.
- **STEP 9.** Feedback intelligence.
- **STEP 10.** Analyse successes and failures to inform future actions.

**MITRE – Center for Technology & National Security**



**The Value of Cyber Deception**

1. Finding and managing adversaries.
2. Learning adversary techniques to better inform defense
3. Finding insider threats
4. Better incident response
5. Deceiving the adversary

*“Judicious use of networks, pocket litter, and honeytokens can waste the adversary’s time and resources, expose their pedigree, and create false knowledge on their part. Deception can also add randomness and unpredictability to an architecture, network traffic, service, or mission activity, making an adversary’s understanding of the environment more challenging and at best inaccurate”*

## DELOITTE: MANAGED EXTENDED DETECTION AND RESPONSE (MXDR)



**Mr Yousef Khasawinah**  
Cyber-Security Manager,  
Deloitte

Mr Yousef Khasawinah, from Deloitte, presented the company's solution to manage detection and response, MXDR.

To start his presentation, Mr Khasawinah gave an overview of current challenges in the cybersecurity arena from three main perspectives:

### Business challenges

- The sensitivity of information processed by organisations, and especially by EU Institutions, Bodies and Agencies (EUIBAs).
- The number and sophistication of cyberattacks to organisations, especially in the public sector as was explained in ENISA's intervention, is rapidly increasing.
- Migration to the cloud.
- The new reality of 'work from everywhere' and 'remote everything'.

### Resource challenges

- Difficulty in recruiting, retaining and training cybersecurity talent.
- Shortage of skilled engineers.
- Limited knowledge of geo-specific compliance issues.
- Service redundancies from mismatched technologies.

### Technology challenges

- Complex and expanding IT, OT, IoT, and vendor solution landscapes.
- Security blind spots in connectivity in migrating to the cloud.
- Adapting to new technologies, consolidating & modernising legacy systems.
- Increasing speed and sophistication of cyberattacks.

To face all these challenges, Mr Khasawinah proposed the MXDR tool, composed of three different layers working together:

- EDR: Endpoint detection and response.
- XDR: Extended detection and response, which adds to EDR capabilities not only endpoints but also different components of the IT ecosystem.
- MDR: Managed detection and response, which adds a layer of data analysis to XDR.

In a nutshell, the MXDR tool integrates technology developed by other companies to provide a single solution with modules that address areas such as cyber threat intelligence, identity management or cloud security.

## DATAMINR: THE VALUE OF REAL-TIME PUBLICLY AVAILABLE INFORMATION



**Mr Gus Hodson**  
Key Account Director,  
Dataminr

Dataminr presented a very innovative and totally different approach to the challenge of early detection of cyber threats.

The speaker, Mr Gus Hodson, explained the value of using publicly available data to identify new threats. To set the context, the speaker gave some very illustrative figures on the amount of publicly available data currently available worldwide and how this continues to grow exponentially.

In just one minute on the internet, Mr Hodson said, there are 350 000 tweets posted, 500 hours of video uploaded to Youtube, or 243 000 photos published on Facebook. This is an immense amount of data that, if properly analysed, can be of great value to detect new threats to an organisation.

The challenge, Mr Hodson explained, remains how to analyse, in real time, that amount of data, to properly filter those that are of the most value. Among the big difficulties that are posed by this examination process are:

- Speed: effectively managing in real time huge databases is not an easy task.
- Heterogeneity of the data that can come in the form of text, pictures, audio, video...
- Heterogeneity of sources and source redundancy, including the standard web, the deep web and the dark web.
- Heterogeneity of languages.
- Detection and inclusion of deleted data.

To solve these problems, Mr Hodson continued, the only possibility is the use of automation through AI models. Many of these models have been integrated in a solution developed by Dataminr, capable of integrating new data sources in real time and of producing results tailored to the objectives of a given organisation, so as to:

- Receive early warnings of novel digital threats.
- Stay up to date on cybersecurity threats as they develop over time and inform the defensive strategy team with alerts on tactics, techniques and procedures and indicators of compromise associated to threat actors.
- Obtain alerts on insecure configurations known to be targeted by hackers.

To showcase the efficiency of the tool, Mr Hodson presented some success stories in which the Dataminr solution had been able to detect threats and events early, such as: attacks related to the war in Ukraine, an attack by an anonymous Sudan hacking group on Sweden's medical infrastructure, a cyberattack on a UK water company, a cyberattack targeting Italian Ministries and Institutions, or a cyberattack that suspended the State administration operations in the province of Carinthia in Austria.



SESSION V

**TECHNOLOGY  
SOLUTIONS FOR  
THE RECOVER AND  
RESPOND FUNCTIONS  
OF THE CYBERSECURITY  
FRAMEWORK**

Chair:

**Mr Aleksandrs Cepilovs**  
Capability Building Officer - R&D, eu-LISA

## THE EUROPEAN INITIATIVE TO ACCELERATE CYBERSECURITY RESEARCH AND INNOVATION



**Mr Christoffer Karsberg**  
Coordinator NCC-SE,  
ECCC-NCC

Session V of the Industry Roundtable was opened with a keynote by the Swedish National Coordination.

Centre for Cybersecurity Research and Innovation, delivered by Mr Christoffer Karsberg. The Swedish National Coordination Centre is the Swedish representation within the Network of National Coordination Centres (NCCs), which is the national counterpart of the European Cybersecurity Competence Centre (ECCC).

The ECCC's mission is to increase Europe's cybersecurity capacities and competitiveness, and to build a strong cybersecurity Community.

In order to strengthen cybersecurity capacity in the EU, the Commission has proposed different methods. From the policy perspective, the Cyber Resilience Act and other policy initiatives put demands on Member States, Agencies and providers.

To address these requirements, capacity building is stimulated through dedicated funding on cybersecurity initiatives. The ultimate aim is to increase the competitiveness of European stakeholders in the cybersecurity domain.

The European Cybersecurity Competence Centre is an EU agency, located in Bucharest. Its head office was inaugurated on 9 May 2023. The agency is currently building up, both in terms of staff and operations.

The first activities include the promotion of cybersecurity capacity building by managing funds. The ECCC is designing the programmes and calls, follows up on them, and promotes capacity building by gathering stakeholders.

The network of coordination centres is the counterpart at Member State level, i.e. there is a dedicated representation in each Member State.

Their mission is similar to that of the ECCC, but at national level. This also includes the assessment of applications to join the European Cybersecurity Competence Community.

This community comprises a large network of stakeholders, including research institutions, companies, public entities, NGOs, standardisation organisations and ENISA.

The activities of the Swedish representation within the Network of National Coordination Centres (NCC-SE) include providing support to the ECCC in its mission, to provide and highlight national priorities in the cybersecurity domain and to promote the EU funding initiatives.

This also includes providing guidance regarding EU calls and financial support to Subject Matter Experts. Furthermore, the Swedish National Coordination Centre coordinates the Swedish stakeholders within the competence community. NCC-SE cooperates with the Swedish research institute cybernode.

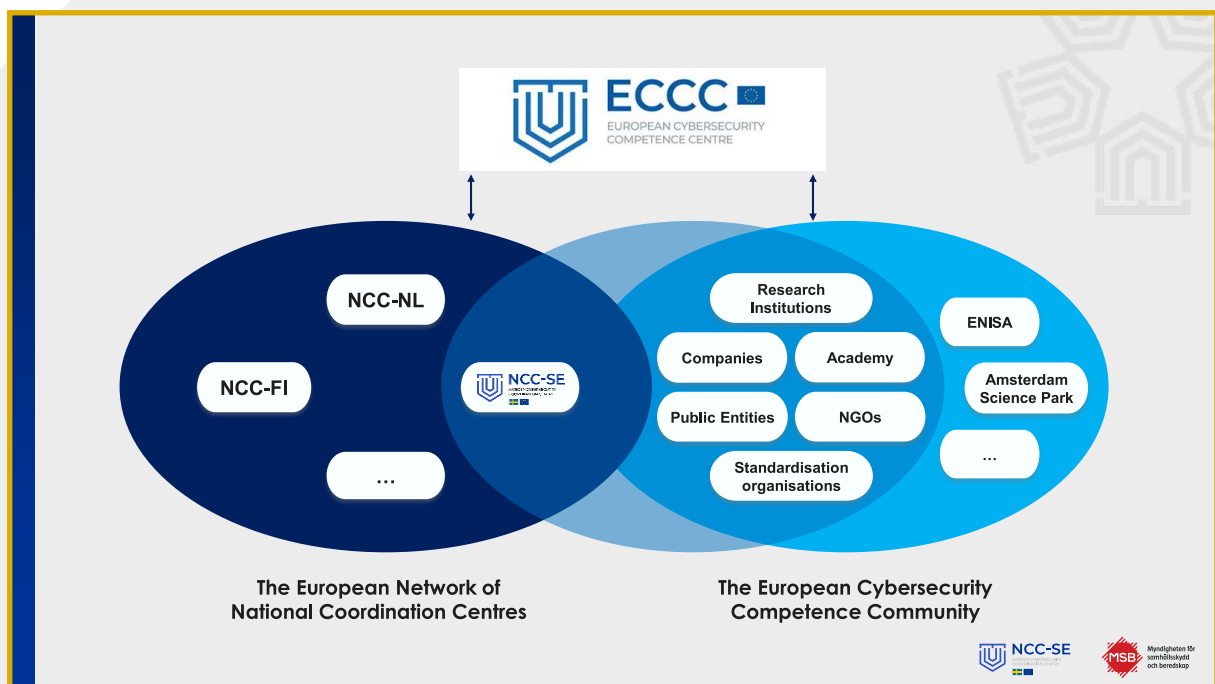


In 2023, the portfolio of NCC-SE consists of several activities. When it comes to the ECCCC and NCC-Network, NCC-SE cooperates with several EU working groups and takes part in the deployment of a platform for the European Community.

Further, the NCC-SE participates in conferences throughout the year. Finally, various activities with cybernode take place, e.g. newsletters, meetings and webinars.

The ECCCC provides, among other tasks, cybersecurity related financial support through Horizon Europe and DIGITAL Europe. As for Horizon Europe, this corresponds to Cluster 3 (Civil Security for Society Research).

In 2023, three calls are being launched: Secure Computing Continuum, Privacy-preserving and identity management technologies and security of robust AI systems. Regarding the DIGITAL Europe Cybersecurity Implementation Programme, the calls include coordination between the cybersecurity civilian defence spheres, standardisation in the area of cybersecurity and support for implementation of EU legislation on cybersecurity strategies.



## PALO ALTO NETWORKS: AUTOMATING THE MODERN SOC RESPONDING AND RECOVERING FROM CYBER INCIDENTS AT MACHINE SPEED



**Mr Eirik Valderhaug**  
Senior Principal Systems  
Engineering Specialist,  
Palo Alto Networks

Mr Eirik Valderhaug, Senior Principal Systems Engineering Specialist from Palo Alto Networks, provided a presentation on the automation of a modern Security Operations Centre (SOC).

A SOC is needed in any larger organisation in order to address the alerts that have been received by the different cybersecurity related tools.

Mr Valderhaug summed up the challenges when assessing the alerts as follows:

### **Too much info, too many silos, not enough insight.**

The number of alerts and quantity of data is so extensive that humans are overwhelmed: An average organisation receives 11 000 alerts per day and therefore requires 4 days to investigate an incident. The time until discovery of an incident is on average over 200 days.

In the last years, critical entities of the IT architecture have been redesigned: Network structures were evolved towards Zero Trust approaches, infrastructure was migrated to the cloud and endpoint security was improved through threat intelligence and data analytics.

In contrast, Mr Valderhaug pointed out that the design of SOCs had not changed. The security incident and events management concept of SOCs was still the same as in times with much less data to be evaluated.

The organisational structure of today's SOCs is mostly human-centred with an analyst as the foundation dealing with all of the alerts. Besides the large amount of data to deal with, humans are limited to evaluating human-readable sources.

Mr Valderhaug expressed the need for a change in this approach, with the human being at the top of the organisational pyramid, only evaluating the very difficult tasks. Most of the alerts needed to be handled by analytics, detection, investigation and response algorithms.

Instead of assessing the alerts separately, intelligence data analytics tools collect all the data from various sources, and machine learning algorithms create an overview.

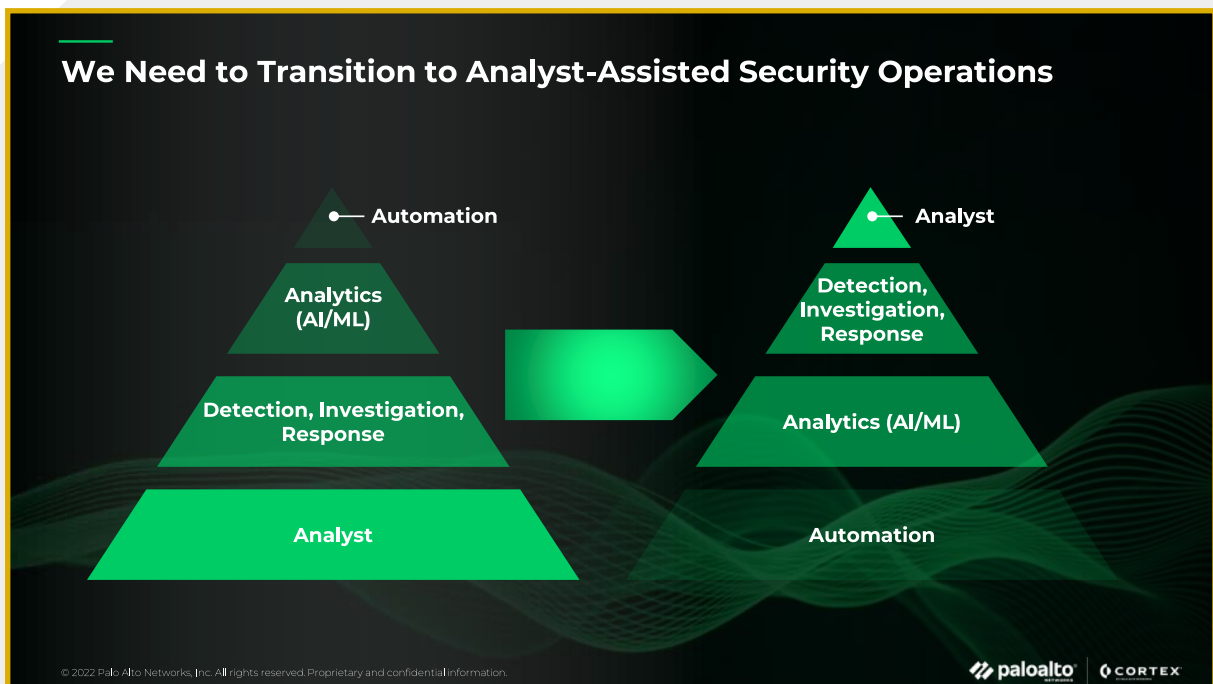
Following the automation first approach, the majority of events can then be handled without human intervention, leaving only a small fraction of the alerts for the analyst.

Mr Valderhaug introduced the XSIAM solution developed by Palo Alto Networks and shared some insights on the operation of the automated SOC in Palo Alto's own enterprise: 36 billion events are registered every day.

On average, 133 alerts are identified, which are then categorised into incidents automatically, of which 125 can be resolved automatically using analytics algorithms, leaving only 8 for a human analyst.

The mean time to detect an alert is 10 seconds, while the response time to high-priority incidents is less than one minute.

Finally, Mr Valderhaug addressed the topic of security operations for cloud-based systems. SOCs needed to cover data from cloud vendors as well, with the aim of having only one integrated SOC with a single user interface for the whole organisation.



## LEONARDO: CYBER RESPOND AND RECOVER APPROACH FOR SYSTEMIC SHOCK RISK MITIGATION



**Mr Aldo Sebastiani**  
SVP Cyber-Security &  
Digital Center, Leonardo

Mr Aldo Sebastiani, Senior Vice President Cybersecurity & Digital Center at Leonardo, explained the concept of the systemic shock risk mitigation.

Mr Sebastiani started his presentation with a focus on business survival. Current IT architectures represent interconnected ecosystems with a high level of complexity and interdependencies. Few hubs arise, where a problem in a critical node creates an uncontrolled chain reaction that implies a systemic shock.

There are several amplifying factors that increase the risk of these kinds of systemic shocks. In scale-free networks and homogeneous networks, vulnerabilities within a single component or library can have dramatic effects, as they cannot be contained due to their large spread throughout the ecosystem.

A high propagation speed and inefficient response, as well as an inefficient classification of the criticality of data imply further weaknesses.

However, the risks can be mitigated by implementing relevant regulations at the policy level and zero trust architectures at the technical level. A proper risk-based survival approach defines appropriate means to respond to threats and to recover from successful attacks.

Mr Sebastiani explained the approach of crisis and recovery vault. The key concept is to make organisations resilient by ensuring the availability of essential services in minimal configuration and access to mission-critical data. Business survival is not about recovering the full business operation immediately, but about ensuring a level of system functionality that allows business continuity.

Mr Sebastiani underlined the need for a risk-based approach to prevent systemic shocks using several numbers: 62% of attacks have led to data encryption. This becomes even more critical, as 50% of these ransomware attacks comprise the backup functionality of data as well. This leads to an average of 21 days of downtime after a successful attack. Privacy and confidentiality are affected as well.

Lessons learned from previous incidents include the need to protect data in use and to design applications in such a way that mission-critical services can run in minimal configuration. It is essential to analyse which data are critical in order to mitigate the risk of systemic shocks.

## CLOSING REMARKS



**Mr Luca Tagliaretti**  
Deputy Executive Director,  
eu-LISA

Mr Tagliaretti closed the event by highlighting that the Industry Roundtable is a unique forum where multiple stakeholders have shared their thoughts and experiences to achieve the goal of cyber-resiliency for the systems managed by eu-LISA: Member States, the European Commission, EU agencies and industry.

Almost 100 participants attended in person and around 160 joined online.

Mr Tagliaretti outlined the main takeaways from the Industry Roundtable as follows: the number of attacks as well as the continuous development of technologies that can facilitate threats are rising fast and steadily.

Not only the number, but also the types of attacks are changing constantly, with a higher level of sophistication. Disinformation powered by AI algorithms is becoming a very common tool of destabilisation. Cyber-actors are becoming more organised, better funded and with better resources. All these points have made them more efficient and with a much higher attack potential.

During the Industry Roundtable, responses on the threat landscape were discussed. Firstly, the EC has made one of its top priorities to ensure cybersecurity within the EU, having established several policies on the subject.

A second element represents building and improving skills in the area of cybersecurity in order to be able to address the emerging threats. The third element is the investment in technology, both by agencies and by funding innovative projects. Finally, cooperation and collaboration among all stakeholders was vital, as the new challenges could only be addressed together.

Mr Tagliaretti concluded with the following message: If you want to go fast, go alone. If you want to go far, go together. eu-LISA has decided to go far, and the Industry Roundtable is one piece in the puzzle of building a cybersecurity response at the European level.

Mr Tagliaretti thanked all contributors to the event: the members of eu-LISA and all the speakers and participants in person and online, who made the event a success through their contributions.

Finally, he provided information about the next Industry Roundtable 'Digitalisation of Justice', to be held in the autumn in Spain and called on the participants to attend this event.

**ISBN:** 978-92-95227-66-8

**ISSN:** 2600-2728

**doi:**10.2857/405899

Photography by **Pax Engström**

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

**2023**

[eulisaroundtable.eu](https://eulisaroundtable.eu)