# Artificial Intelligence Threat Reporting and Incident Response System

## D8.8 Report on connection with stakeholders

| | |
|---|---|
| **Project Title:** | Artificial Intelligence Threat Reporting and Incident Response System |
| **Project Acronym:** | IRIS |
| **Deliverable Identifier:** | Document number |
| **Deliverable Due Date:** | 31/8/2024 |
| **Deliverable Submission Date:** | 5/9/2024 |
| **Deliverable Version:** | v1.0 |
| **Main author(s) and Organisation:** | Sebastijan Cutura (ECSO) |
| **Work Package:** | WP8 Dissemination, Communication and Exploitation of Results |
| **Task:** | Task 8.5 Community building and liaison with relevant stakeholders |
| **Dissemination Level:** | PU: Public |

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

## Quality Control

| | Name | Organisation | Date |
|---|---|---|---|
| Editor | Sebastijan Cutura | ECSO | 30/08/2024 |
| Peer Review 1 | Lorena Volpini | CEL | 02/09/2024 |
| Peer Review 2 | Sotirios Spantideas | KEMEA | 02/09/2024 |
| Submitted by (Project Coordinator) | Gonçalo Cadete | INOV | 05/09/2024 |

## Contributors

| Organisation |
|---|
| ECSO |

## Document History

| Version | Date | Modification | Partner |
|---|---|---|---|
| v.0.1 | 30/08/2024 | First Version | Sebastijan Cutura (ECSO) |
| v.0.2 | 04/09/2024 | Corrections after the peer review | Sebastijan Cutura (ECSO) |
| v1.0 | 05/09/2024 | Final editing | Gonçalo Cadete (INOV) |

# Legal Disclaimer

# Contents

# List of Figures



# List of Tables

# List of Abbreviations and Acronyms

| Abbreviation/ Acronym | Meaning |
|---|---|
| CISO | Chief Information Security Officer |
| CSIRT | Computer Security Incident Response Team |
| CERT | Computer Emergency Response Team |
| SME | Small and Medium-sized Enterprises |
| AI | Artificial Intelligence |
| KER | Key Exploitable Result |
| SOC | Security Operations Centre |
| DORA | Digital Operational Resilience Act |
| NIS2 | Network and Information Security Directive |
| GDPR | General Data Protection Regulation |
| FEW | Final Exploitation Workshop |

# Executive Summary

Deliverable 8.8 offers a comprehensive summary of Task 8.5, which focused on stakeholder liaison throughout the project's three-year lifespan (M1-M36). The deliverable showcases several key achievements, including a thorough initial identification and categorization of relevant stakeholders, the successful establishment of a Community of Chief Information Security Officers (CISO) with a detailed analysis of its membership structure, and a report on the final exploitation workshop highlighting the outcomes of the engagement efforts. To maintain conciseness and avoid redundancy, this deliverable does not reiterate information on all workshops and conferences attended by consortium partners, as these details have been previously documented in other deliverables namely D8.3, D8.4, D8.5. The report on the IRIS Launch Event is included in D8.3, while additional information on stakeholder engagement and identification can be found in D2.2, D2.6, and D7.5.

# 1 INTRODUCTION

## 1.1 Deliverable purpose

The primary objective of Deliverable 8.8 is to provide a clear and comprehensive account of the engagement with external stakeholders. The document includes all the activities undertaken on linking with relevant stakeholders and engagement during Project activities and events (M1 – M36) that have not yet been reported in the previous deliverables.

## 1.2 Intended readership

This deliverable is public and therefore is mainly addressed to the IRIS Consortium partners, the European Commission (funding authority), as well as other audiences who are interested in learning more about the project. The deliverable will be made available on the IRIS website once approved by the European Commission.

## 1.3 Relationship with other deliverables and tasks

D8.8 "Report on Connection with Stakeholders" is an output of task T8.5 "Community building and liaison with relevant stakeholders" and is closely linked to all tasks within WP8 "Dissemination, Communication and Exploitation of Results". Activities of T8.5 during the 1st and 2nd years of the Project have been reported in D8.3 "Initial report on dissemination, communication, standardisation and exploitation" and D8.4 "Interim report on dissemination, communication, standardisation and exploitation".

# 2 STAKEHOLDER IDENTIFICATION

In the project's inception, the IRIS Consortium undertook a thorough process to identify a wide-ranging list of stakeholders crucial to the project's success. This diverse group encompassed public and private entities, supply and demand-side organisations, large corporations and SMEs, research institutes, and other EU Projects.

This classification was subsequently acknowledged and refined in various project deliverables, particularly those related to the User Requirements, IRIS Reference Architecture, Pilot Use Cases, Dissemination, Communication, Clustering and Exploitation activities.

Each stakeholder category was engaged with a distinct purpose, aligned with the project's objectives. Some stakeholders were involved in testing and validating IRIS tools and solutions, ensuring their effectiveness and relevance. Others were identified as potential clients and beneficiaries of IRIS solutions, forming a key focus for the project's exploitation activities.

This strategic approach to stakeholder engagement ensured that IRIS solutions were not only technically sound but also aligned with market needs and expectations. By involving a diverse range of organisations throughout the project lifecycle, IRIS was able to develop solutions that addressed real-world cybersecurity challenges while also identifying potential avenues for future implementation and adoption.

Some of the main identified stakeholder categories throughout the project lifetime include:

- **National CSIRT/CERT** teams can leverage IRIS to enhance their capabilities in several ways. The platform facilitates improved threat intelligence sharing, enabling more effective online communication and collaboration. It also provides a comprehensive incident management system. These key exploitable results contribute to enhancing the cyber situational awareness, preparedness, detection, and response capabilities of CSIRT/CERT teams. By providing actionable insights for threat mitigation, IRIS empowers these teams to address cybersecurity challenges more effectively. Furthermore, the platform fosters collaboration between various teams and organisations across regional, national, cross-border, and European contexts. This collaborative approach extends to critical infrastructure operators and operators of essential services, creating a more robust and interconnected cybersecurity ecosystem
- **Organizations seeking cybersecurity solutions (end-users)**, whether in the form of products, services, or processes, represent the demand side of the market. These organisations, both large and SMEs, can derive significant benefits from IRIS innovations. By leveraging IRIS, they gain access to services that substantially enhance their cyber resilience. The platform also offers improved incident management capabilities, allowing companies to respond more effectively to

cybersecurity threats. Additionally, IRIS provides these organizations with access to real-time threat intelligence, enabling them to stay ahead of emerging risks and adapt their security strategies accordingly. This comprehensive approach helps businesses strengthen their overall cybersecurity posture in an increasingly complex digital landscape.

- **Organisations that provide cybersecurity products, services, and/or processes**, representing the supply side of the market, can leverage IRIS innovations to enhance their offerings and capabilities. These organisations, both large and SMEs, can utilise IRIS to develop and offer new or improved cybersecurity products and services, expanding their portfolio and market reach. The platform also grants these companies access to real-time threat intelligence, enabling them to stay at the forefront of emerging cybersecurity trends and threats. Furthermore, IRIS allows these providers to enhance the incident response capabilities of their products, making their offerings more robust and attractive to potential clients.
- **Research institutions and universities** can harness IRIS innovations to advance their cybersecurity research efforts. By utilising the platform, these academic and scientific organisations can conduct in-depth studies on cyber threats and emerging trends, gaining valuable insights into the evolving landscape of digital security. This research potential extends particularly to the cutting-edge domains of Internet of Things and AI-driven applications, areas that are increasingly vulnerable to cyber-attacks. Through their work with IRIS, these institutions can play a crucial role in contributing to the development of more effective and sophisticated cybersecurity solutions. This collaborative approach between academia and innovative technology not only enhances the understanding of current and future cyber threats but also fosters the creation of robust defenses against them, ultimately strengthening the overall cybersecurity ecosystem.
- **Public authorities,** particularly those focused on cybersecurity and critical infrastructure operations, can leverage IRIS innovations to enhance their capabilities across several key areas. By implementing IRIS, these organisations can significantly improve their cyber situational awareness, enabling them to better understand and anticipate potential threats. The platform also facilitates faster and more effective incident response, allowing authorities to react swiftly and decisively to cybersecurity challenges. Additionally, IRIS contributes to increased operational efficiency, streamlining processes and resource allocation in cybersecurity management. Perhaps most importantly, the platform provides these authorities with enhanced abilities to collaborate with other stakeholders within the cybersecurity ecosystem. This improved collaboration fosters a more cohesive and coordinated approach to national and international cybersecurity efforts, ultimately strengthening the overall defense against cyber threats.

Throughout the project's duration, the IRIS partners collaboratively focused on engaging key stakeholders. As part of this initiative, we developed and continuously refined a comprehensive contact list featuring representatives from various identified stakeholder categories made available on the IRIS repository. This proactive approach allowed us to

establish and nurture valuable connections within the cybersecurity ecosystem. By the project's conclusion, we had successfully identified and reached out to **45 key individuals**, fostering meaningful relationships that contributed to the project's success.

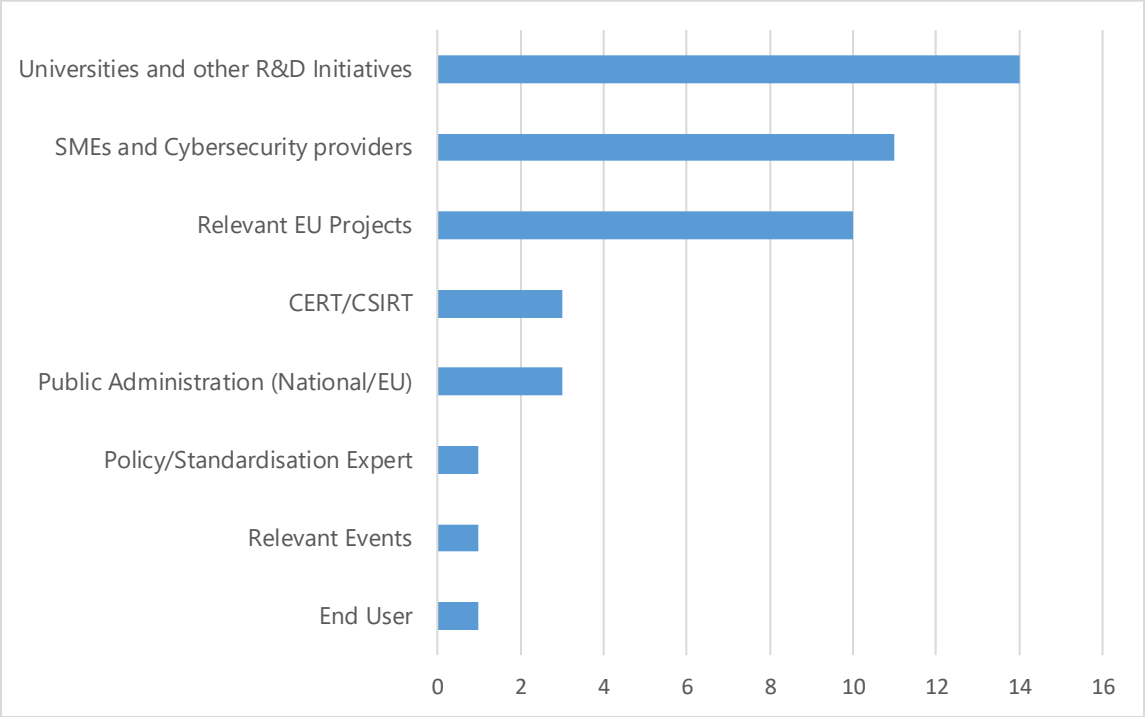


*Figure 1: Number and category of individual contacts of Relevant Stakeholders*

# 3 CISO Community

Throughout the IRIS project's lifecycle, Community of Chief Information Security Officers (CISOs) was established. The CISO Community served as a cornerstone for the IRIS project, fulfilling two major functions. It acted as a catalyst for leveraging project outcomes and provided critical validation for IRIS Solutions. This collaborative engagement ensured that the IRIS solutions remained grounded in real-world cybersecurity needs.

Why are CISOs considered as a crucial target group for the IRIS Project? CISOs are pivotal stakeholders in cybersecurity. They oversee cybersecurity and information security management within their organisations. While not directly involved in day-to-day threat and incident management, CISOs supervise these processes and lead teams of experts. Importantly, they often have the authority to approve major purchases and allocate budgets for security solutions making them ideal targets for exploitation activities as potential buyers of IRIS solutions. As experts in information security, CISOs have a deep understanding of their organisation's security requirements, vulnerabilities, and the threat landscape. This knowledge allows them to recognise the value of effective cybersecurity solutions. Moreover, CISOs are tasked with developing and implementing long-term security strategies. They're likely to be interested in solutions that align with their strategic goals and can demonstrate long-term value. Furthermore, CISOs often work closely with other C-level executives and board members. Their recommendations carry weight and can influence broader organizational decisions about cybersecurity investments. A particular interest can be expected for the European made solutions as they are often responsible for ensuring their organisation complies with various EU data protection and cybersecurity regulations. Finally, CISOs often participate in professional networks and communities. Their opinions and choices can influence peers in other organisations, potentially leading to wider adoption of IRIS solutions.

The CISO Community has grown into a formidable network, now comprising **500 CISOs (or equivalent positions) from 29 European countries.** This makes it one of the largest cross-sector and cross-border community of cybersecurity executives in Europe. A comprehensive list of CISO Community Members including titles and companies represented can be found in the Annex. After the end of the project lifetime, the CISO Community will continue operating as a collaborative forum fostering information exchange that will in turn increase overall level of cybersecurity among the European organisations.

The CISO Community was actively involved in several key project events, including the IRIS Launch Event, Validation Workshop (RISE-SD 2023), three Stakeholder and Industrial Workshops, and the Final Exploitation Workshop. These engagements ensured that the IRIS project remained aligned with the needs and perspectives of top cybersecurity professionals across Europe. CISOs took on prominent roles as speakers in specialised panel discussions at the two major events: IRIS Launch Event and Final Exploitation Workshop.

A significant IRIS awareness raising presentation took place during the 2022 Annual Meeting of the CISO Community, known as the "CISO Meetup," held in Brussels. At this gathering, the IRIS Project was showcased to an audience of over 100 CISOs. The presentation was met with considerable interest, resulting in 14 CISOs deciding to join the project's external stakeholder list. This list was subsequently made accessible on the IRIS Repository, further expanding the project's network of influential cybersecurity professionals. With the active engagement in IRIS Project, CISOs gained insights into challenges and solutions on how to share threat information, how to conduct effective threat response, and how to improve incident reporting to national CERTs/CSIRTs which has become an essential part of the CISO tasks with the recently adopted NIS2 Directive. More details on this engagement can be found in the D8.4.

Overall, creation of a CISO Community fulfilled the goal of creating an active community of potential end-users for collecting feedback to be considered by the project's activities, to support targeted communication of the project's results and to provide an opportunity for the exploitation.

Members of the CISO Community can be considered to hold more potential in commercially exploiting the IRIS results and applying them in daily practice and they are identified as a target group of many IRIS KERs. IRIS business portfolio successfully engaged the CISO Community stakeholders thus generating a hype around the IRIS approach.

In the final stages of the project, we carried out a dissemination and exploitation activity to present the IRIS Project outcomes to the CISO Community. A comprehensive spreadsheet listing was shared and it included all IRIS Key Exploitable Results (KERs), including their type (method, technology, training, pilot scenario), as well as the KER owners, contact persons, and email addresses. Additionally, we distributed brochures detailing the Service Bundles and Components, along with promotional materials available on the IRIS website and YouTube channel including demonstrations of the available tools.

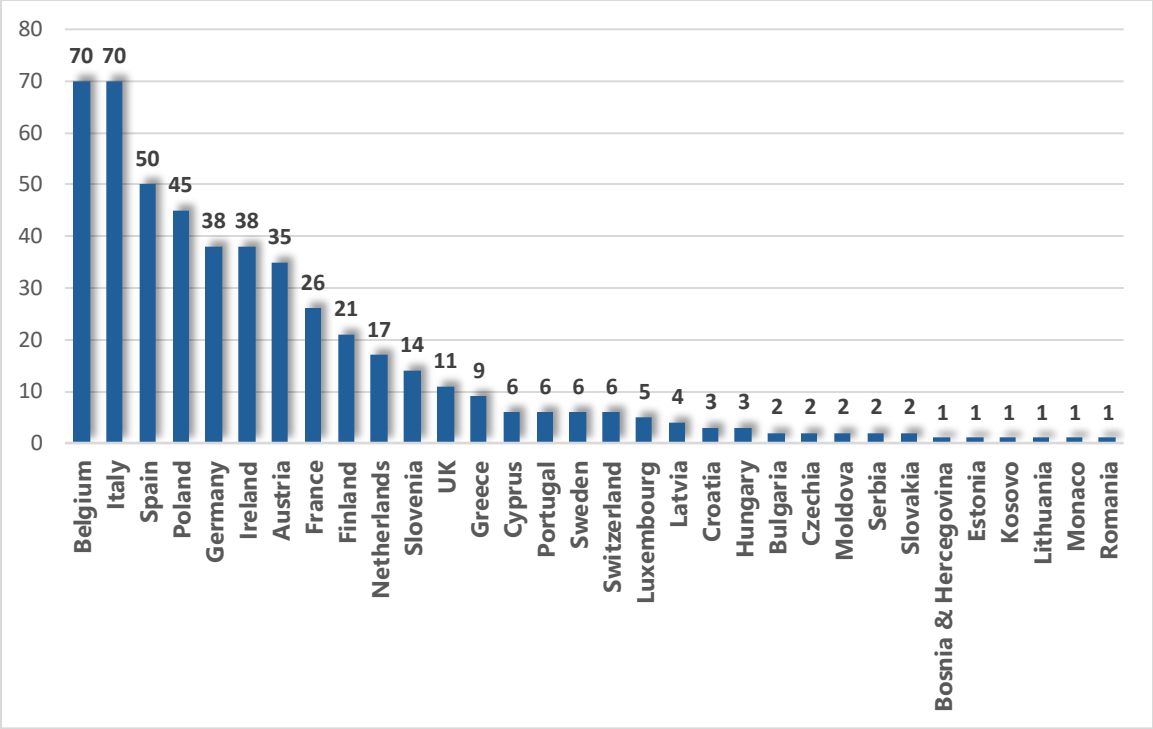


*Figure 2: Country Distribution of CISO Community Members, last updated on 26 August 2024*

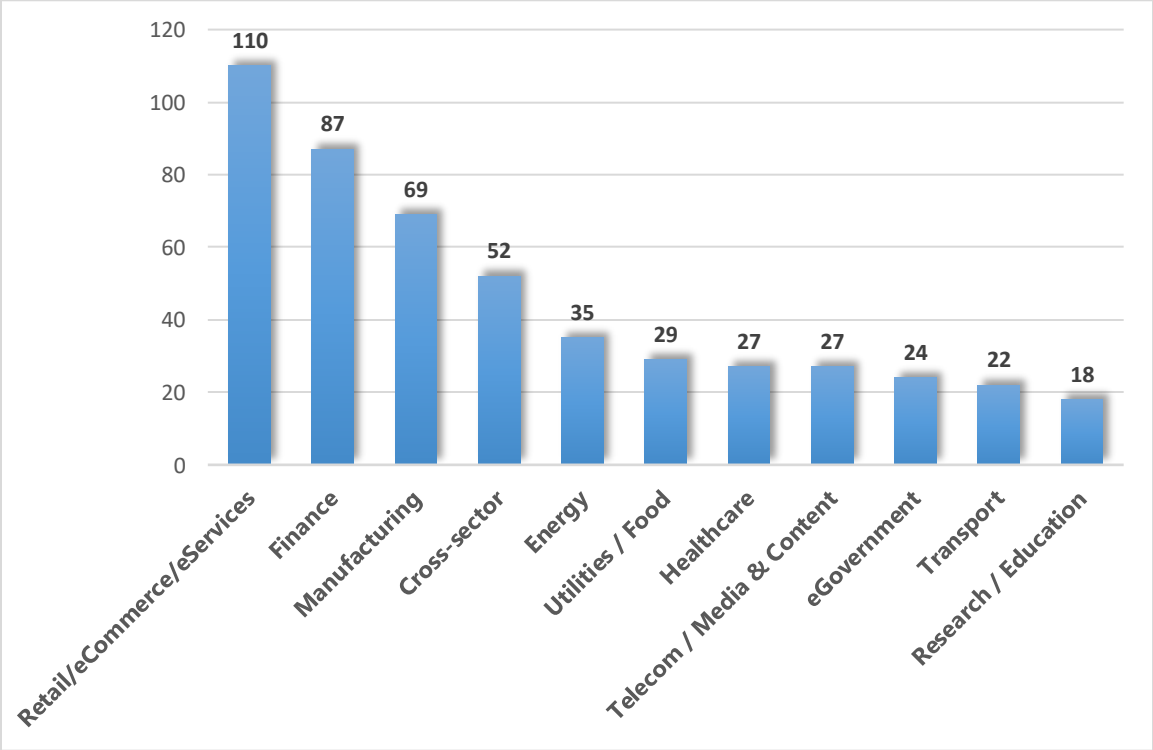


*Figure 3: Sector Distribution of CISO Community Members, last updated on August 26 2024*

# 4 Final Exploitation Workshop

The Final Exploitation Workshop, held on June 20 2024 in Krakow, Poland, as a side event during Cybersec Expo & Forum, one of the largest cybersecurity conferences in the country. To maximise engagement and exploitation opportunities, the Workshop was promoted under the title "Enhancing Cybersecurity through Incident Response and Threat Intelligence." The agenda was carefully crafted to highlight the IRIS Offering, featuring live demonstrations of the platform's functionalities. Detailed elaboration on the exploitation aspects and presentations by IRIS partners are reported in D8.5. As a full-day event, the Workshop also welcomed external high-level experts who led panel discussions and delivered presentations on topics pertinent to the IRIS Project.

External experts were invited to share insights on the topics crucial for the IRIS Project including:

- Incident Reporting
- The Role of SOCs
- Cyber Threat Intelligence Information Sharing

This has effectively helped build-up the narrative for the IRIS partners to showcase solutions that will overcome challenges in the above mentioned domains.

Panel on "Challenges of Incident Reporting" brought together CISOs from large companies and the panel discussion covered a range of critical topics, including the legislative impact of key regulations such as DORA, NIS2, and GDPR. The conversation also delved into the transformative role of AI in cybersecurity and its broader implications. The panelists explored the importance of cultivating a strong company culture, emphasizing the value of people, effective error management, and fostering a culture of learning from mistakes. Additionally, the discussion highlighted the significance of sharing incidents and collaboration across organizations, and how initiatives like IRIS can enhance these efforts.

Panel discussion on the "Crucial Role of Security Operations Centers (SOC)" highlighted the critical role of the SOCs as the central hubs for an organization's cybersecurity efforts. SOCs are tasked with monitoring, detecting, and responding to security incidents in real-time. With the rising complexity and frequency of cyber threats, the demands on SOCs have intensified. SOCs are now tasked with safeguarding hybrid environments, which are increasingly critical to essential services and industrial operations. Panelists concluded that the SOCs will need to further integrate innovative solutions to automate threat detection and response processes. Additionally, the growth of cloud computing and IoT devices will demand that SOCs expand their monitoring capabilities to address a more complex and interconnected threat landscape.

A presentation on the topic "Securing Cyberspace Together: The Imperative of Cross-Border Threat Intelligence Sharing" highlighted that the effective data exchange enhances

the ability to monitor key, essential, and critical environments, which is often a legal requirement. By ensuring interoperability, information sharing strengthens both global and local resilience against anomalies. However, challenges such as the sheer volume of data, differences in data types and purposes, and diverse data sources must be managed. To address these, it is essential to implement technological, physical, organizational, legal, and logical frameworks that support the extraction, preparation, aggregation, transmission, and processing of data. This approach ensures that decision-making processes remain consistent and effective, without negatively impacting system interoperability or communication integrity.

Final presentation "Why is CTI sharing not working?" started by a notion that Cyber Threat Intelligence (CTI) sharing is highly effective when supported by robust frameworks like MISP and OPEN CTI. These modules facilitate seamless exchange of critical threat data, enabling organizations to better anticipate and counteract cyber threats. Additionally, EU regulations such as NIS2 and DORA mandate and encourage CTI sharing, reinforcing the importance of collaboration for improving cybersecurity across sectors. However, CTI sharing also faces significant challenges. A lack of awareness about its benefits, coupled with fears of disclosing sensitive information, can hinder information sharing. There is often resistance from both C-level executives and middle management, who may be reluctant to expose potential vulnerabilities or "shameful" incidents. Moreover, the absence of internal regulations or clear guidelines can further impede the adoption of CTI sharing practices, ultimately weakening the collective defense against cyber threats.

In total **39 participants** were present at the Workshop (in-person only) including high level profiles such as the CEOs of cybersecurity provider companies and CISOs of large companies. In particular, CISO Community was leveraged to attract a large number of CISOs mainly coming from the CISO # Poland Association effectively making the CISO category the largest among the participating individuals.

The following tables capture categories and number of individuals and organisations that attended the IRIS FEW.

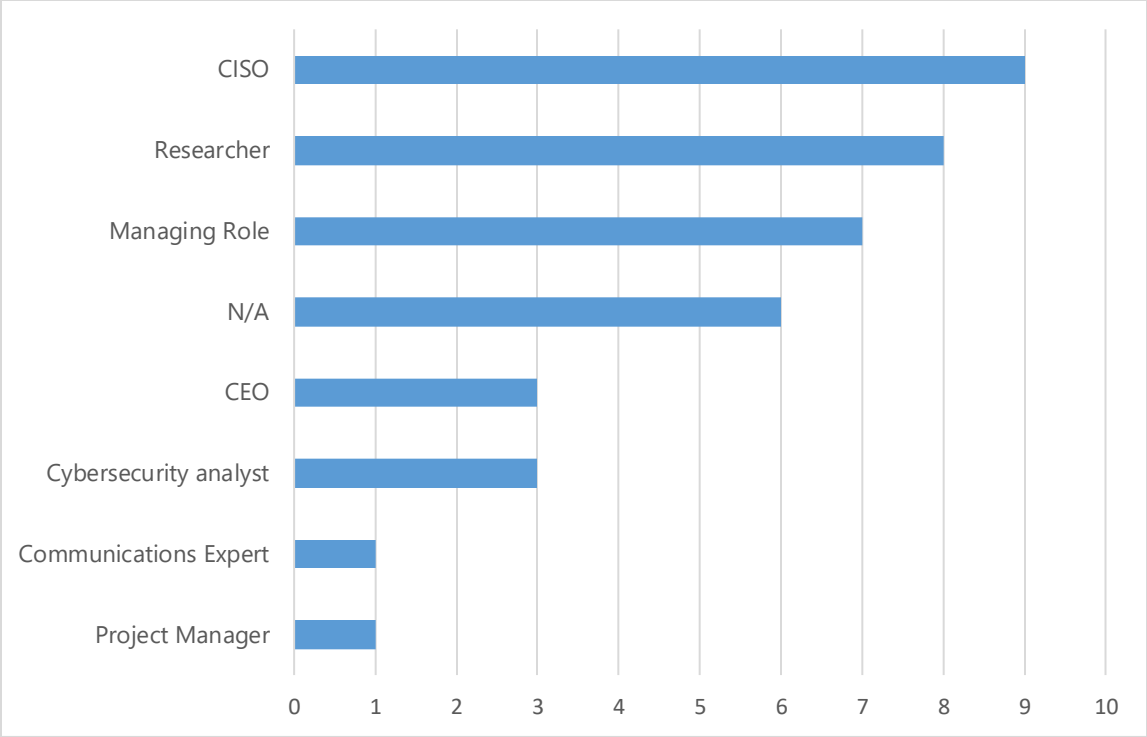


*Figure 4: Number and titles of individual stakeholder participations at the IRIS FEW*

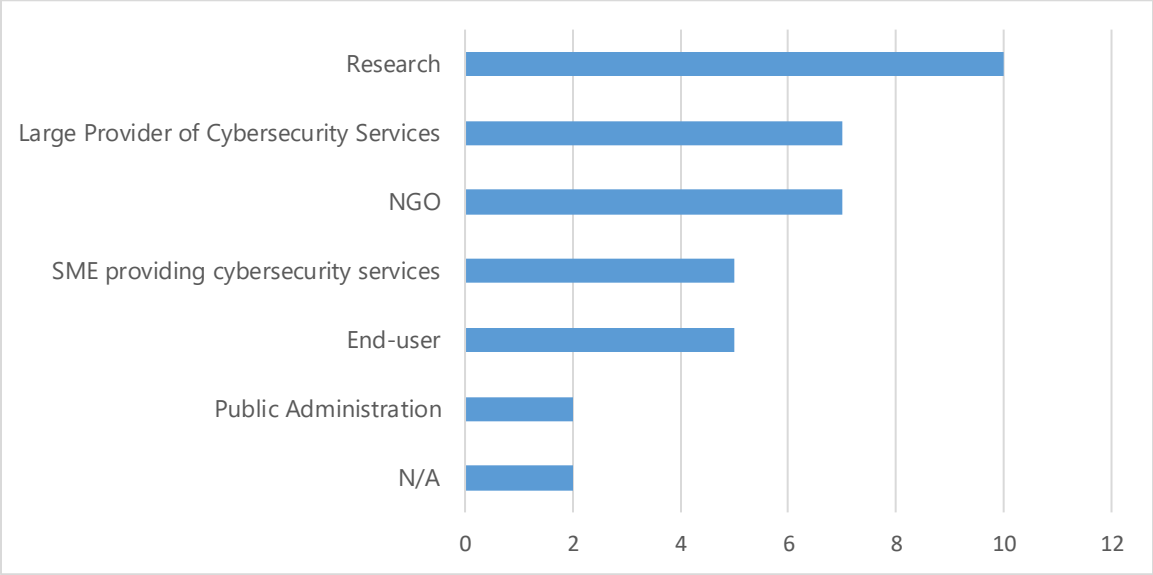


*Figure 5: Category and number of organisations participating at the IRIS FEW*

# 5 CONCLUSIONS

The engagement of external stakeholders throughout the project proved to be a resounding success, playing a pivotal role in shaping and validating the project's outcomes. By strategically involving a diverse array of participants - including CISOs, national CSIRT/CERT teams, industry experts, and representatives from both public and private sectors - the project benefited from a wealth of real-world insights and expertise. This collaborative approach ensured that the developed solutions remained grounded in practical needs while pushing the boundaries of innovation. Stakeholders contributed actively through various channels, including workshops, panel discussions, and direct feedback sessions, which not only enhanced the project's technical outputs but also paved the way for future adoption and implementation of the results. The strong engagement fostered a vibrant ecosystem of cybersecurity professionals, creating lasting networks that extend beyond the project's formal conclusion. Ultimately, this inclusive strategy significantly amplified the project's impact, ensuring its relevance and applicability across diverse cybersecurity landscapes.

# 6 REFERENCES

[1] IRIS consortium, "D2.2 User and Technical Requirements Specification," 2022.
[2] IRIS consortium, "D2.6 IRIS platform and reference architecture," 2023.
[3] IRIS consortium, "D7.5 IRIS pilot evaluation report (Intermediate Report)," 2024.
[4] IRIS consortium, "D8.3 Initial report on dissemination, communication, standardisation and exploitation," 2022.
[5] IRIS consortium, "D8.4 Interim report on dissemination, communication, standardisation and exploitation," 2023.

# 7 ANNEX: CISO COMMUNITY MEMBER'S LIST

*Table 1: CISO Community Member's List, Roles and Organisations*

| ROLES | ORGANISATION |
|---|---|
| Lead Architect Cybersecurity | Siemens |
| VP, Head of Active Threat Monitoring | Standard Chartered Bank |
| Co-founder & Threat Hunter/ Incident Responder | RedTeam.pl |
| Head of ICT &CISO | Ornua |
| CISO | Garnica |
| Senior Programmer & ICT and Business Services | Cork City Council |
| Group CISO | ENGIE |
| CISO | Nital SpA |
| Group CISO | EKCO |
| Global Leader for Ecosystem Security | Schneider Electric |
| CISO | Sisal Group |
| Cybersecurity Director | Barilla Group |
| Information & Cyber Security Analyst | Carel |
| CISO | University of Bologna |
| CISO | Port of Koper |
| IT Director and CISO | Soul-K |
| CSO & CISO | Bachem |
| Group CISO | A2A |
| CSO | Italgas |
| Digital Solutions Leader | Leroy Merlin |
| Director I Corporate Systems | IFCO Systems |
| CISO | Cliniques Universitaires Saint-luc |
| CISO | Emasesa |
| Executive Director, Enterprise Cybersecurity | Aptiv |
| Global CISO | Shell |
| CISO | BNP Paribas Fortis Personal Finance |
| CISO | Secunet |
| Founder and Board Member | Women4Cyber Hungary |
| Global CISO | Transcom |
| CISO | Italgas |
| CSO | Voestalpine |
| CISO | Körber Group |
| CISO | AT & S Austria Technologie & Systemtechnik AG |
| CISO | ELES |
| | |

| ROLES | ORGANISATION |
|---|---|
| CISO | SODO |
| Founder | CISO4U |
| Freelance Security Advisor, previously CISO of Carrefour | Colegio Oficial de Ingenieros de Telecomunicación |
| RSI | Ercros |
| CISO | Fluidra |
| CISO | Zeppelin |
| Global Cyber Security Officer | Intrum |
| Head of Information Security and Privacy | Inter IKEA Group |
| Information Security Risk Officer | Econocom |
| Senior Information Security Officer | NLB |
| Inormation Security Manager | Angelini Industries |
| CISO | Financiera Maderera (Finsa) |
| Group CISO | Mediaset |
| Information Security Advisor | Croatian Pension Insurance Institute (HZMO) |
| Head of Audit, Risk & Compliance | Cablenet Communication Systems |
| CISO | SPLOŠNA BOLNIŠNICA DR. FRANCA DERGANCA NOVA GORICA. |
| CISO | Gameente Assen |
| Head of Department - Business Support Systems & Information Technology | Kosovo Telecom J.S.C. |
| Security Operations Center Manager | Alior Bank S.A. |
| IT Security Officer | University College Cork |
| AVP, Threat & Vulnerability Management | Sun Life |
| CISO | KU Leuven |
| CISO | MPET |
| Ciso as a Service | Fednot |
| Regional Cybersecurity Lead | PepsiCo |
| CISO | Nueva Pescanova Group |
| Director Group Information Security & Enterprise Architecture | Bilfinger |
| ICT Advisory Board Member | Dublin Business School |
| Head of Information Security | Weavr.io |
| CISO | WEngage |
| CISO | Nova KBM |
| Director of Cyber Security | TVH |
| ICT Security Specialist | European Parliament (SECPOL) |
| Business Security Officer for Consumer Solutions | Mastercard |
| CISO | BH Consulting |
| VP Information Security Europe and OT | McKesson |
| CISO | Relex Solutions |
| CISO | P&V Group |

| ROLES | ORGANISATION |
|---|---|
| Cybersecurity Manager | Barilla Group |
| CISO | Swedish Internet Foundation |
| CISO | Sanef |
| Maritime Cybersecurity | CSO Alliance |
| Resilliance Manager | Salzburg AG |
| CISO | WithSecure |
| Head of IT Security | ISMC |
| ISRM | Sandoz |
| CISO | Mondi Group |
| Deputy CISO | Oekb |
| CISO | Lineas |
| CISO | BIPT - Belgian Institute for Post and Telecommunication |
| CISO | Cyta |
| Senior Cybersecurity Consultant | Grant Thornton Cyprus |
| CISO & DPO | Group Motor Oil |
| CISO | Athora Holding |
| CISO | Visma |
| Group CISO | Ineos |
| Senior manager, policy Analysis and International Relations | ECSO |
| CISO | ESET |
| CISO | SPAR Slovenia |
| CISO & DPO | BOSA |
| CISO | Criteria Caixa |
| Head of Cybersecurity | Baselinker |
| Head of Security | Mattermost |
| CISO | Qiagen |
| Cyber security executive | Allianz Group |
| Founder and coordinator of FIN CERT Serbia | Serbian Association of Banks |
| CISO | COREN |
| Senior Security Architect | Veralto |
| Executive Director Information Technology | Intesa Sanpaolo |
| CISO | Institute of Tropical Medicine |
| Senior Cybersecurity Consultant | Soter ICS |
| Group Information Security Manager | DCC plc |
| Group CISO | Energy One |
| CISO | Mediobanca |
| CISO | Nagelmackers |
| CISO | EveryMatrix Ltd |
| CISO | Belgian Nuclear Research Centre |
| CISO | INA Group |

| ROLES | ORGANISATION |
|---|---|
| CISO | Mater Misericordiae University Hospital |
| CISO | MAXAM |
| vCISO,President ISACA Belgium | Approach Belgium |
| CISO | Microsoft |
| Head of IT Infrastructure Department | NLB Banka Sarajevo |
| Associate ICT Director | Novartis |
| CISO | Cassa di Risparmio di Volterra |
| CISO | E&Q Engineering |
| CISO Ireland Representative | Cyber Ireland |
| Group Director of Security, Safety and Incident Management | Atos |
| Co-Founder | CISO Squad |
| CISO | Barceló Hotel Group |
| Executive Director, Cybersecurity and Business Continuity Management | Intesa Sanpaolo |
| Group CISO | Generix Group |
| Head of IT Security | Mondadori |
| CISO | Cabel Industry S.p.A. |
| CISO | Palladium Hotel Group |
| Business CISO | Carrier Commercial Refrigeration |
| CISO | Sofinco España |
| CSO/Head of Corporate Security | Porsche AG |
| Cybersecurity Manager | Roca Group |
| Head of Technology Resielience | Sandoz |
| CISO | Banco Crédito Cooperativo |
| CISO | Ferrero |
| Head of Information and Cyber Security | Gruppo Hera |
| Group CISO Europe | Orange |
| Group CISO | Econocom |
| CISO | Multipharma |
| Cybersecurity VP & CISO EMEA | Schneider Electric |
| IT Governance Specialist | Spitz |
| Security Consulting Consultant | Accenture Italia |
| CISO | EirGrid |
| CISO | Vueling |
| CISO | PCI Pal |
| CISO | Skroutz |
| vCISO, Academic Director | Ataya & Partners, Solvay Brussels School |
| EMEA CISO | Evident Scientific |
| CISO | Tyrolit Group |
| Chief Risk & Security Officer | Sdworx |
| | SCC |

| ROLES | ORGANISATION |
|---|---|
| Infrastructure & Information Security \| In-House Legal Counsel | |
| Cyber Security Manager | Destination Marketing Agency |
| Retired CISO, ex-CISO of Novomatic Italia, Poste Italiane | Retired |
| CISO | Edison |
| CISO | Webuild |
| CIO | FinecoBank |
| Group CISO | Carel |
| Principal Security Architect, Office of the CISO, Google Cloud | Google |
| Head of Cyber Resilience & Strategic Regulatory Relations | AIB |
| Group Senior Director Cybersecurity, European Banking Federation Chairman | Intesa Sanpaolo |
| CISO | Max Mara Fashion Group |
| head of Cybersecurity | Leroy Merlin |
| Deputy CISO | BFF Bank |
| Regional Security Manager for Europe Region | AXA Partners |
| Business Information Security Officer | KBC Group |
| CISO | Bankinter |
| Director, Operatioanl Risk & Cyber Security Control | UBS |
| Cybersecurity Solutions Arhitect | IAPS |
| Information Security Officer | EORTC |
| CISO | MISUMI Europa GmbH |
| CISO | DolomitenBank Osttirol-Westkärnten |
| Principal Cyber Security Officer | Siemens Energy |
| CISO | leTEC |
| Information Security Compliance Manager | Mediahuis IRL |
| CISO | HSBC |
| Senior IT Security Expert | Orange |
| | Untis |
| Information Security Officer, Data Protection Coordinator | |
| ISO | EKCO |
| Co-Founder & Secretary General | Associso |
| CISO | Aluminium Duffel |
| CISO | Bank Ochrony Srodowiska |
| Cybersecurity Manager for South & West Europe | Schneider Electric |
| Information Technology Security Manager | Reig Jofre |

| ROLES | ORGANISATION |
|---|---|
| Head of Corporate Security | Orange Moldova |
| Head of Security & information compliance | ITP Aero |
| VP & CSO | Elisa |
| Partner | EY Poland |
| Cyber Security Consulting | EY Switzerland |
| CISO | BMW Group |
| CISO | Vrije Universiteit Brussels |
| Information Security Officer | McCann FitzGerald |
| CISO | Nordic Invstment Bank |
| CISO | S-Bank Ltd |
| | CISO4U |
| Chief Executive Officer & President | |
| ISO | Vaisala |
| | Tietoevry |
| CISO & CTO | Numata Business IT |
| Head of Cybersecurity | La Salle Campus Barcelona |
| CISO as a Service | Kyndryl |
| CISO | Repsol |
| CISO | Cetelem |
| CISO | University of Malaga |
| CISO | Astra |
| CISO | Quironsalud |
| CISO | Rapid7 |
| CISO | Sopra Steria |
| Information Systems Security Domain Manager | SFR |
| CISO | ENEDIS |
| CISO | European Research Council |
| Global Head of Cyber Security Operations | Intertek |
| CISO | European Investment Bank |
| CISO | Municipality of Hague |
| IT Security Manager | Indra |
| Responsible for Cybersecurity | EMT Madrid |
| CISO | Redbull |
| Jimmy O'Brien | Sligo City Council |
| Group CISO | GLS |
| CISO Team | SNCB - Belgian Railways |
| COO | ECSO |
| CISO | Baden-Württembergische Spielbanken |
| CISO | VDAB |
| CISO | ING Belgium |
| CISO | Tessenderlo Group and Greenyard Group |

| ROLES | ORGANISATION |
|---|---|
| CISO | Siemens |
| CISO | F-Secure |
| Principal Technology Officer of Cybersecurity & Data Analytics | S3 Connected Health |
| CISO | (ISC)² |
| IT Project Manager & IT Industrial Manager | Reig Jofre |
| CISO | Iberdrola |
| CISO | Orange Spain |
| Direc&OT Security R&D Unit | Euracat - echnology Centre of Catalonia |
| CISO | Anticipa Real Estate, Aliseda Inmobiliaria & Testa home |
| CISO | Siemens Energy |
| CISO | Keva |
| CISO | Kesko Group |
| CISO | Infodas |
| Information Security Manager | Hauser |
| CISO | Guardtime |
| Lead Enterprise Security Arhitect | Standard Chartered Bank |
| CISO/Project Security Manager | Hitachi Rail |
| CISO | Monaco Télécom |
| Group Security Officer | ATOS |
| Cybersecurity Officer EMEA, Associate Director Information Security | BD |
| Head of Information Security | AirBaltic |
| CISO | Attentia |
| CISO | Regnology |
| ISO | Lansweeper |
| Cyber Security Manager | PwC Latvija |
| General Manager | 2BeAware |
| CIO/CISO | Rosomak S.A. |
| CISO | CNP Vita Assicura |
| Head of Cyber Security for Europe Cluster | Vodafone |
| CISO | Steelmet |
| CISO | Tuscany Region |
| CISO | Banco BPM |
| CISO | Posti Group Finland |
| CISO | HKI |
| Global CSIRT Manager | Nestle |
| Business Area Security Officer Compressor Technique | Atlas Copco |
| Security Program Director | Logitech |
| Cybersecurity Governance Program Manager | Workday |

| ROLES | ORGANISATION |
|---|---|
| CISO | Marelli |
| Co-founder of Italian CISO Community | Cybersecurity Angels |
| Secretary General | ECSO |
| Head of Information Security and Business Continuity | Celfocus |
| Group CISO | Informa Group |
| ISO | AGH University of Science and Technology |
| Global Head of Attack Surface Management | ING Bank |
| ISO | EPA |
| Group CISO | SHV Energy |
| IT Security Manager | AirBaltic |
| Junior CISO | Schneider Electric |
| DP CISO | Schneider Electric |
| CISO | Arneg |
| Group CISO | Angelini Industries |
| Deputy CISO | Sopra Steria |
| Platform CISO Packaging & Color Management | Veralto |
| CISO | Wiener Stadtwerke Group |
| NASK | OT Security |
| CISO | G2A.COM |
| Cyber Security Manager, North and East Europe | Schneider Electric |
| Head of Information Security and Business Continuity | Open Fiber |
| CISO / Chief Legal Officer | Pronova BKK |
| Head of Information Security | Grupa Azoty Puławy |
| Information Security Officer | Cyprus Agricultural Payments Organisation |
| Group Guidance & Stakeholder Networking (Team of Giorgio Cusma Lorenzo) | Intesa Sanpaolo |
| Cybersecurity operations lead | Latvia State Radio and Television Centre |
| Head of OT Cybersecruity | Grupa Azoty Puławy |
| CISO | PPC Energy |
| Information Security Manager | Finnvera Oyj |
| Deputy CISO | ELES |
| CISO/DPO | Globetech AS |
| CISO | Cork City Council |
| Associate Director - Compliance, Risk & Security Lead | MSD |
| Security Operations | Uniqa |
| CISO | FACC AG |
| | FactorBank |
| Chief Security Officer | |

| ROLES | ORGANISATION |
|---|---|
| CISO | Genua |
| CISO | Alma |
| ISO | Silent Eight |
| CISO | Carrefour |
| Director, Head of Cyber Security | Telecom Italia |
| Manager for Technologies, Innovation and Trusted Supply Chains | ECSO |
| Senior Director of Security & Technology Platforms | Campari Group |
| IT-Compliance Manager and Auditor for the ISO27901 | Econocom |
| CISO | Munchener Hypothekenbank |
| CISO | Dr. August Oetker |
| CISO | Sibelco |
| IT Security & Risk Manager | Felbermayr-Group |
| Senior Security Manager | BT Ireland |
| Global Risk Senior Director | Boston Consulting Group |
| CISO | PWC |
| CISO | Accountor |
| CISO | Gen-energija |
| Security Policy Lead | ENISA |
| CISO | University of Milan |
| Head of CERT | Poste Italiane |
| Cybersecurity Manager | Procter & Gamble |
| CISO | Miller Group |
| Security Officer | Barco |
| Chief Security Risk Officer | Klarna |
| Group CISO | HelleniQ Energy |
| Information Security & Data Protection Officer | Vodafone |
| Head of Sector: Applications and Human Factors | ECSO |
| CISO | Tap |
| VP Group Cybersecurity | Solaris Group |
| CISO/DPO | Itsme |
| Global CISO | Abertis |
| CISO | SPAR ICS |
| ISO | Osram |
| CISO | Erium SAS |
| Group CISO | EDF |
| CISO | Puig |
| IT Risk & Information Security Manager | FCC Servicios Ciudadanos |
| Group CISO | Omilia |

| ROLES | ORGANISATION |
|---|---|
| Cybersecurity Executive, previously acting CISO of Bank of Cyprus | Freelance |
| CISO | Fiorentini |
| CIO | A4 Holding S.p.A |
| Head of Information Security and IT Governance | Esselunga S.p.A. |
| Group CISO | NEXI |
| CISO | Engie Italia |
| CISO & CIO | Elettronica Group |
| Head of Product Cyber Resilience | Leonardo |
| Head of Information Security | ICCREA Banca |
| CISO | Nixu Corporation |
| Cybersecurity Lead | EY |
| Group CSO | ATOS |
| Group CISO | Optum |
| Director of Cyber Operations/CISO | UK Government |
| Head of IT Security and Governance | IPL |
| CISO & CIO | Vitalograph |
| CISO | PGMW |
| Senior Cyber Securit Officer | Skandia Bank |
| COO/CISO | Doccle |
| Group CiSO | Raiffeisen Bank Internaional |
| Head of Detection & Response | Siemens Energy |
| CEO, link with CISOs from Finland | Finnish Information Security Cluster |
| CISO | Volksbank |
| CISO Advisor | Hoxhunt |
| CISO | Ilmarinen |
| CISO | Hartlauer Handelsgesellschaft |
| Information Security Officer | Fednot |
| CISO | Cegeka |
| Vice President, CISO | Deutsche Bank Group |
| ISO | VDK Bank |
| CISO | SHV Energy |
| CISO | ELT Group |
| Executive Director & Head of Red Team Operations & Cybersecurity Testing | Standard Chartered Bank |
| CISO | Polskie Linie Kolejowe |
| CISO | Rossmann |
| Group CISO | Raben Group |
| | |
| SOC Manager | Netia |
| CISO | PayEye |

| ROLES | ORGANISATION |
|---|---|
| CISO | Orange Poland |
| Cyber Resilience Manager | GSK |
| Senior Information Technology Security Officer | Nova Banka |
| Security Technical Lead supporting CISO | Orange Moldova |
| Global Cybersecurity Director & IT Risk \| CISO | Corporación Multi Inversiones |
| Head of Cybersecurity | Macrobond Financial |
| Head of Cybersecurity | Softing Services |
| Head of Security | DWS |
| CISO | TU Dublin |
| CISO | Doka |
| CISO | ING |
| CISO | Signify |
| CISO | Frieslandcampina |
| Enterprise Security Arhitect | Crelan NV |
| Director of the Cybersecurity Department | Alior |
| Director Information Security | Wire |
| CTO | Polpharma |
| Head of Sector: Standardisation, certification and supply chain management | ECSO |
| CISO | S2E |
| Head of the Information Security | Poste Italiane |
| Cyber Threat Intelligence | Rabobank |
| CISO & CRO | Batopin |
| Group CSO | Erste Group Bank AG |
| Global CISO | Iberdrola |
| CISO | Exide Technologies |
| CISO | CHU Brugmann |
| CISO/HEAD of Information and Cybersecurity | Volvo |
| World Wide Cybersecurity Manager | l'Oreal |
| Director, Head of Information Security - Chief Information Security Officer (CISO) | Grant Thornton Luxembourg |
| Cyber Security Professional | Nokia Bell Labs |
| Regional Cybersecurity Manager | Schneider Electric |
| CISO | Deventer Hospital |
| ISO | SPAR ICS |
| Cyber Security Expert | Cedars |
| BISO Europe | PepsiCo |
| Strategy, Policy & Compliance Director | HP Enterprise |
| CISO | BME |
| CISO (former) | Polenergia |

| ROLES | ORGANISATION |
|---|---|
| Chief Security Arhitect ICT/OT | PGE Group |
| Orange Corporate Internal Auditor | Orange |
| Manager: Policy & CISO Network | ECSO |
| CISO | AGBAR |
| CISO | Banco de España |
| CISO | Carbery Group |
| Cyber Security Governance Manager | Schlumberger |
| Global Head of Cyber Security | MSC Cruises |
| CISO | Gruppo Cassa Centrale |
| CISO | Haier Europe |
| Security & Compliance Manager | Gewiss |
| CISO | Inizio Health |
| Regional Chief Security Officer | Mastercard |
| Information Security Manager | PM Group |
| Head of Information Assurance | Österreichische Staatsdruckerei GmbH |
| CISO | Henkel |
| CISO | Palfinger |
| Head of Information Security Operations | Österreichische Staatsdruckerei GmbH |
| CISO | SVD Gmbbh |
| CIO | Tecnalia Research and Innovation |
| Director Risk, Security, Legal, CISO | Christelijke Mutualitet (CM) |
| CISO | Pirelli |
| CISO | Osram |
| Head of IT Infrastructure | Hôpitaux Iris-Sud |
| CISO | Thales |
| Head of IT Infrastructure & Security & Technology | Revantage |
| BISO Europe | PEPSICo |
| CISO | Davinsi Labs |
| CISO | De Lijn |
| Group CISO | Eviden |
| CISO | Zeb Consulting |
| CISO | Metabo |
| Chairman of the Bulgarian Cybersecurity Association, Link to BG CISO | Bulgarian Cybersecurity Organisation |
| Group CISO | Yeswehack |
| CISO | Synthos Group |
| CISO | CHU Brugmann |
| System Security Specialist | Slovenian CERT |
| CISO | Elisa |
| CISO | OP Financial Group |
| Director Of Technology | 8 West Consulting |

| ROLES | ORGANISATION |
|---|---|
| Head of CS Risk Management | Fronius |
| CISO | Agravis Raiffeisen AG |
| CISO | 21 Finance |
| CISO | ARM |
| CISO | Tata Consulting |
| Head of Corporate Information Security / CISO | Jungheinrich AG |
| CISO | Enfuce |
| Product Owner | ECSO |
| OT Senior Cyber Security Analyst | National Grid |
| CISO | UCB |
| COO | Cyber Security Competence and Certification Centre |
| Senior Director of Security and Privacy | Vinted |
| IT Security Manager | Unum Zycie |
| Junior Manager | ECSO |
| CISO | Suncontract |
| CISO | Spyrosoft |
| CISO | Normet Group |
| Head of Cyber & Digital Risk | Advisense |
| Data and Cybersecurity Director (CISO) | GS1 |
| CISO | SPAR Italy |
| CISO | European Defence Agency |
| CISO | Franke Group |
| Lead Arhitect for Global Directory Services | Schneider Electric |
| CISO | Coosto |
| CISO | DCSA |
| Lead Security Officer | BNP Paribas Bank Polska |
| CISO | EVN |
| CISO | Hoerbiger |
| CISO & Compliance Officer | Deutsche Telekom |
| CISO | Dentais |
| Head of Security Architecture | Standard Chartered Bank |
| Head of Group Information Security | Encevo |
| Ex-CISO UBS, Greek Government | Kiberna |
| Regional Information Security Officer | Allianz Partners |
| Head of Security | LearnUpon |
| CISO | European Fund Administration |
| ISO | Register.si |
| Project Assistant | Cyber Ireland |
| CISO | DARS |
| CISO | Zepos & Yannopoulos |

| ROLES | ORGANISATION |
|---|---|
| CISO | Portfolion |
| Head of Information Security Governance | Allianz |
| CISO | Kirchhoff-Ecotec |