Cyber Europe 2024

After Action Report

Powered by ENISA

November 2024

About the document

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: enisa.europa.eu.

CONTACT

For contacting the authors, please use exercises@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

EDITORS

Radu Arcus, Nikolaos Christoforatos, Fanouris Fanourakis, Gema Fernández, Christian Van Heurck, Alexandros Zacharis

CONTRIBUTORS

Rory Aston James, Claire Charlier, Laura De Vos, Carolina Simioni

ACKNOWLEDGEMENTS

Cyber Europe Planners, ENISA Operational Cooperation Unit, Distribution System Operators Entity, European Network of Transmission System Operators for Electricity

DISTRIBUTION

This document is **TLP:CLEAR**, according to the Traffic Light Protocol (TLP) latest version[1]. Therefore, its distribution is limited to Cyber Europe Planners, and Cyber Europe 2024 participating organisations.

[1] TLP version 2.0 is the current version of TLP standardised by FIRST

LEGAL NOTICE

Print	ISBN 978-92-9204-680-4	DOI 10.2824/3428659	TP-01-24-004-EN-C
PDF	ISBN 978-92-9204-679-8	DOI 10.2824/2285347	TP-01-24-004-EN-N

Table of contents

01

PART 01:

EXERCISE OVERVIEW

Introduction

Cyber Europe is a series of European Union-level cyber incident and crisis management exercises organised by the European Union Agency for Cybersecurity (ENISA)[2], intended for both the public and private sector across the European Union and European Free Trade Association (EFTA) Member States. These exercises simulate the escalation of large-scale cybersecurity incidents into cybersecurity crises. They provide opportunities to analyse sophisticated technical cybersecurity incidents and assess participants' ability to manage complex scenarios.

Cyber Europe 2024, which focused on the energy sector, took place from 19 to 20 June in a hybrid format; it was coordinated from the Exercise Control Centre in Athens, Greece, where the organising team and most national Planners were based. (Local) Planners were involved with preparing, designing, and organising their teams' participation, determining objectives, scenarios, and logistics. During the cybersecurity exercise, they were responsible for coordinating participant involvement, ensuring the exercise runs smoothly, and monitoring the progress of the exercise at the organisational level. They assisted the Players with any questions they had about the scenario.

The local Planners, along with the Players, participated online. Players were the individuals or entities actively involved in exercise. They contributed to Cyber Europe 2024 by executing assigned tasks, making decisions, and responding to simulated events or incidents. Recognising the energy sector's critical importance to the EU's economic growth and development, and its status as a prime target for cyberattacks, this year's exercise scenario was carefully designed to help stakeholders - including companies and industry leaders - prepare for, and proactively address, evolving cybersecurity threats.

In general, the purpose of Cyber Europe 2024 was to ensure the adequacy and improve processes/ standard operating procedures (SOPs), internal cooperation, relationships within the teams of Planners and Players, clear internal communication channels, the capacity to deal with cybersecurity crises and improve the public relations response during cybersecurity crises. Additionally, Cyber Europe 2024 also focused on raising awareness at the corporate level about the importance of cybersecurity preparedness and the value of investing in cybersecurity.

The following sectors were taking part in the cybersecurity exercise with each their own purpose and different aims.

[2] A glossary of terms used in this document is provided in page 34.

Energy sector

The specific sectorial entities targeted were Electricity Transmission and Distribution System Operators and Gas Storage Operators. Cyber Europe 2024 concentrated on ensuring compliance with relevant national legislation, particularly concerning reporting obligations. It aimed to enhance the adequacy and effectiveness of dedicated structures for managing cybersecurity crises at the national level, as well as to improve the contributions of energy sector entities and networks at the EU level concerning awareness and readiness during a cybersecurity crisis. Another key aim of Cyber Europe 2024 was to strengthen the effectiveness of communication channels with relevant supply chain actors during a cybersecurity crisis, ensuring that the information exchanged is complete, high-quality, and timely. These aims are also applicable for EU level sectorial networks.

Digital Infrastructure and Public Administration sector

The specific sectorial entities targeted were Data Centre Service Providers (Digital Infrastructure) and National Energy Regulators (Public Administration). One of the aims was to improve the response of indirectly affected sectors during cybersecurity crises impacting the energy sector. Another aim focused on advancing national progress in implementing Network and Information Systems Directive (NIS2)[3] provisions related to incident reporting for Public Administration.

EU level cybersecurity networks

Cyber Europe 2024 also had specific aims for the Computer Security Incident Response Team (CSIRT) Network and the European Cyber Crisis Liaison Organisation Network (EU-CyCLONe). These included ensuring the adequacy of EU-level operational cooperation and escalation mechanisms during cybersecurity crises and ensuring the existence, adequacy, effectiveness, and speed of communication channels and SOPs between CNW (CSIRTs Network), and EU-CyCLONe. An additional aim was to assess the completeness, quality, and timeliness of information exchange.

EU institutions, bodies, and agencies

Cyber Europe 2024 also had the aim for ENISA Operational Cooperation Unit, CERT-EU and EC3 (European Cyber Crime Centre) to ensure the adequacy and improve their internal processes/SOPs and ensure the adequacy, effectiveness and rapidness of the communication channels and SOPs between EUIBAs and EU level networks.

[3] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) available at Directive - 2022/2555 - EN - EUR-Lex (europa.eu)

Methodology

This After-Action Report was created to present the results of Cyber Europe 2024 based on the predefined Evaluation Framework and methodology. This evaluation framework was developed by ENISA, derived from the Network and Information Security Directive (NIS2), and will be published at a later stage. The report contains expectations and feedback from participants, including both Players and Planners, which will be further explained in this chapter.

The data collection for Cyber Europe 2024 was conducted through various methods before, during, and after the cybersecurity exercise to ensure a comprehensive evaluation of the participants' performance and the effectiveness of the systems and processes in place. This multi-stage approach allowed for a thorough analysis of different aspects of the exercise.

Before Cyber Europe 2024

Data was primarily gathered through surveys designed to capture the participants' expectations and Players' self-assessed confidence levels. These pre-exercise surveys provided baseline information that helped the evaluators understand the initial conditions and expectations of the Planners and Players.

During Cyber Europe 2024

A more dynamic and real-time approach to data collection was employed during the exercise. Observers and feedback collectors with evaluation responsibilities gathered data through direct observations, 1-on-1 interviews, and social listening. This approach allowed for immediate documentation of events and participant responses as they unfolded. The use of hotwash sessions, which are immediate debriefing meetings held at the end of the exercise to gather participants' feedback and discuss what worked well and what did not, further facilitated the collection of feedback from Planners, facilitating the timely recording of issues and successes.

After Cyber Europe 2024

The day after the exercise, the focus shifted to reflective and analytical data collection methods. Feedback surveys were distributed to participants to assess whether the exercise met their expectations, while post-exercise self-assessment surveys allowed Players to

evaluate their own performance. These post-event surveys were important to compare the outcomes with pre-exercise expectations.

The combination of these methods has provided a comprehensive view of the exercise's effectiveness and highlighted opportunities for enhancement in future iterations. By analysing both immediate feedback and long-term reflections, ENISA was able to draw comprehensive conclusions and identify potential areas for improvement.

It is more crucial than ever to act on these suggested improvements in a timely manner to enhance effectiveness and achieve a tangible impact. To ensure the implemented changes meet the intended and desired effect, relevant parts of the scenario could be replayed and assessed for their effectiveness.

Scenario

The general purpose of the exercise scenario was to assess how well European stakeholders are prepared to handle a complex and ongoing cyberattack. For instance, due to the growing pressure of incidents together with the number and intensity of these incidents, the scenario aimed to test the sector's ability to keep operations running, protect vital infrastructure, and respond effectively to various threats that could have serious economic and social impacts. Additionally, the scenario emphasised the importance of situational awareness, aiming to enhance participants' ability to perceive, understand, and anticipate the potential impacts of cyber threats in real-time. By doing so, the scenario aimed to improve participants' understanding of the strategic impact of cyber-attacks in the energy sector, as such attacks could be used for broader geopolitical goals.

By challenging the Players to handle a complex crisis in a realistic environment, the exercise aimed to provide important insights into where improvements are needed to strengthen the sector's overall cyber resilience.

The exercise scenario was designed to create a realistic and challenging setting to test the EU's cyber resilience, especially in the energy sector. Different types of threat actors were included to simulate the complexity and variety of real-world cyber threats. The scenario was made more realistic by adding various simulated roles, such as government spokespersons, journalists, and network operations teams, which the Players were required to interact with during the exercise. The Players, representing key stakeholders in the energy sector, such as Electricity Transmission and Distribution System Operators, Gas Storage Operators, Data Centre Service Providers and National Energy Regulators were expected to respond to the events as they unfolded. Their responsibilities were to manage the crisis, reduce the impact of the cyber-attacks, and ensure the continued operation of essential energy infrastructure.

The results and key findings from the scenario, including the performance of both Planners and Players, will be further elaborated in Part 2.

02

PART 02:

KEY INSIGHTS

Players' insights

The analysis presented in this section results from data obtained from **at least 64%** of the Players involved in this exercise.

Cyber Europe 2024 was a success, with around 5,000 estimated participants engaging throughout the two days of the exercise. The high level of participation did not only exceed the expectations, but it also demonstrated the widespread interest and enthusiasm for the exercise.

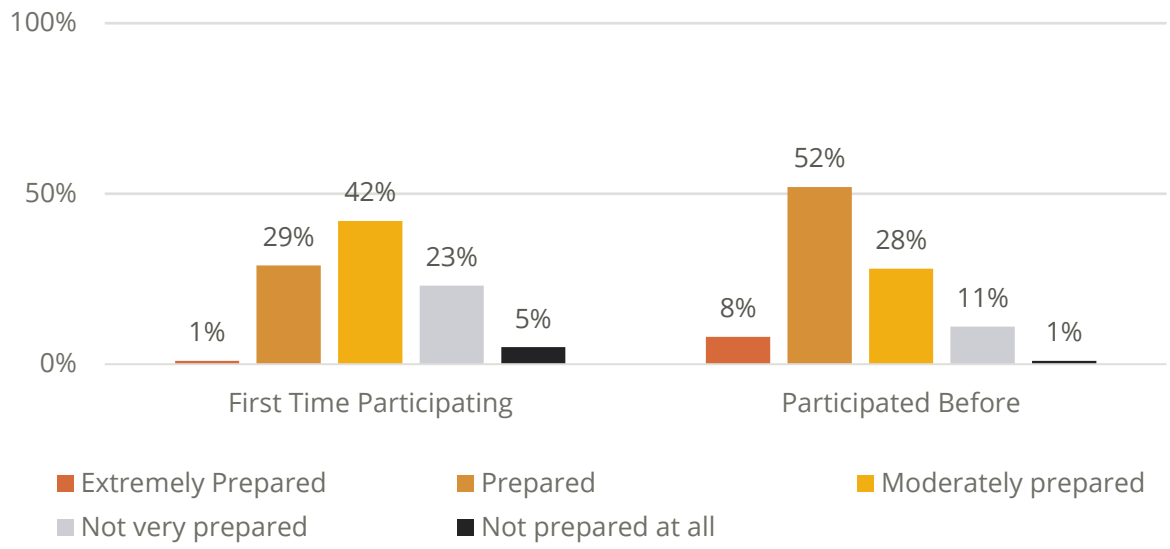
General perception

The exercise was well-received by Players, who widely regarded it as beneficial for testing their cybersecurity capabilities and procedures. Cyber Europe 2024 provided a valuable platform for identifying gaps in their current systems and ways of working, thereby highlighting areas for improvement.

Preparedness

As shown in the graph below, Players who participated in previous editions of Cyber Europe felt more *prepared to play* the exercise compared to newcomers, with only a minority feeling extremely prepared, indicating a need for enhanced readiness for the exercise overall. The feedback from Players, based on ex-post questions, also revealed a gap between perceived and actual preparedness, especially among new Players.

Graph 1: Cyber Europe Players' Participation Readiness



Challenges

It was expected that one of the difficulties would be linked to unclear roles and insufficient preparation, which were indeed the primary challenges faced during the exercise, suggesting a need for better pre-exercise training and clearer role definitions.
Despite the challenges faced, most Players expressed satisfaction with their experience. They appreciated the exercise's substantial contribution to enhancing cybersecurity readiness. This sentiment was validated by 92% of Players who felt that Cyber Europe 2024 significantly improved their cybersecurity readiness, underscoring the exercise's effectiveness.

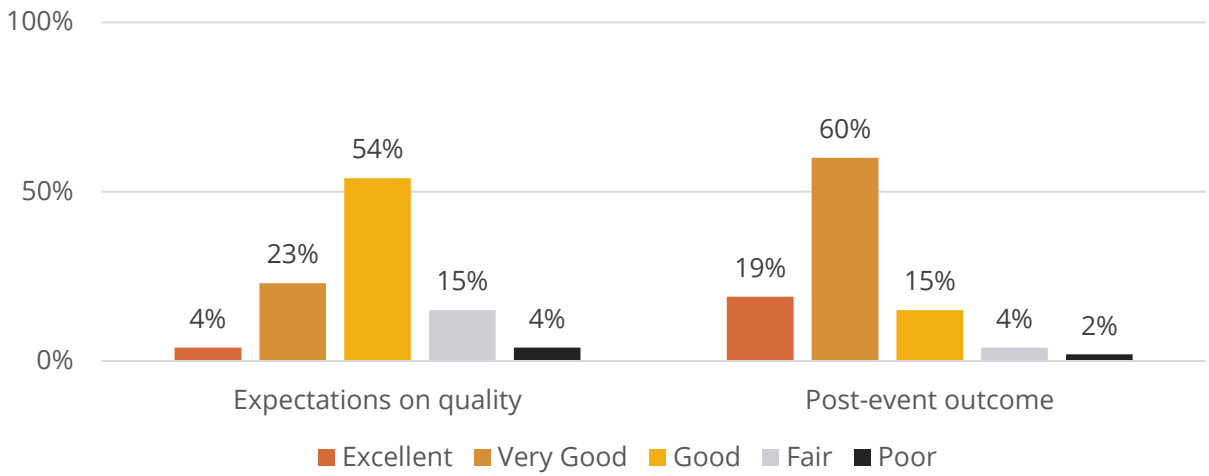
While some teams managed the injects with minimal guidance from Planners, others required additional support to navigate them effectively. This highlights the necessity of providing comprehensive support and guidance throughout the exercise, ensuring that all Players can fully benefit and know what they have to do. It is also important to acknowledge that the complexity of the tools can pose challenges for Players who may not have the same level of familiarity as the Planners. This situation highlights the need for a diverse skill set within team members to tackle complex scenarios effectively.

It is crucial to recognise the critical role that communication and information sharing play in building situational awareness and driving a successful response. This aspect cannot be emphasised enough.

Satisfaction levels

Post-event satisfaction levels were high and aligned well with initial expectations, demonstrating that the exercise met its purpose of being beneficial and educational.
Data highlighted in the graph below shows Cyber Europe 2024's success in meeting initial expectations with post-event outcomes. The high satisfaction rates underscore the exercise's significant value.

Graph 2: Expectations on quality of Cyber Europe 2024 compared with Feedback of Post-event outcome by Players



Collaboration and information sharing

The level of collaboration and information sharing varied significantly among Players. Some teams demonstrated excellent teamwork and were ready to share information, while others were less inclined to collaborate. Promoting a culture of sharing is essential in these types of exercises to enhance overall effectiveness.

Planners' insights

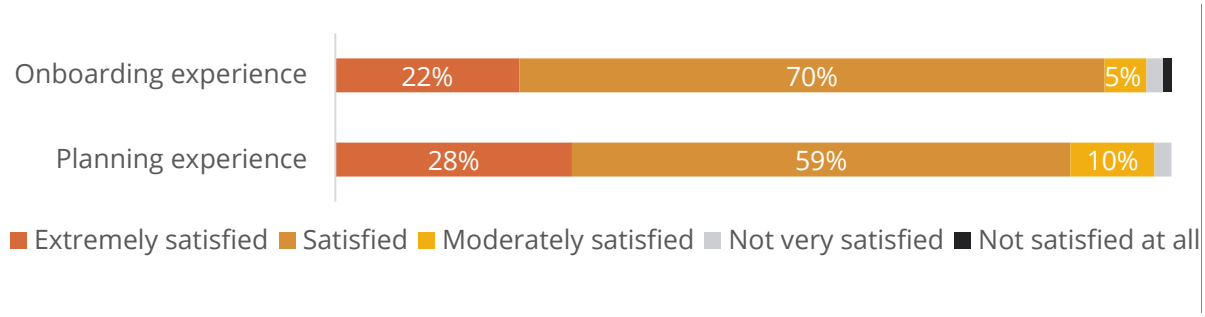
General perception

Planners expressed their satisfaction with the exercise. They appreciated the opportunity to test their national cybersecurity capabilities and procedures in a controlled environment.

Onboarding and planning experience

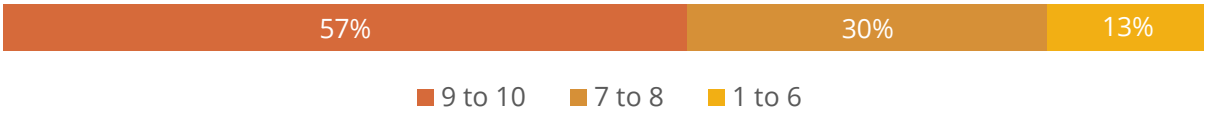
The overall satisfaction with onboarding and planning was high, as shown in the graph below, with extreme satisfaction particularly noticeable among National Cybersecurity Authority (NCSA) Planners. The fact that Planners received an Ambassadors Kit containing ready-to-use material to support the process of engaging playing organisations has potentially contributed to this positive trend.

Graph 3: Level of Planners' satisfaction with the onboarding and planning experience after Cyber Europe 2024



The likelihood of recommending participating in Cyber Europe as a Planner remained high, with over 50% indicating a likelihood of 9 or 10 on a scale of 1 to 10, reflecting the exercise's perceived value and effectiveness.

Graph 4: Likelihood of Planners to Recommend Participating in Cyber Europe



Teams' preparedness

While Planners were confident about their teams' preparedness, feedback from Players revealed varied readiness levels, highlighting a small gap between Planners' expectations and Players' actual preparedness. This indicates that Planners should have a better understanding of their Players' preparedness in the future.

Planners' Exercise Guide

This guide contains all the essential information and instructions required to successfully execute the exercise. It includes detailed technical information and serves as a guide to assist Planners on how to better help Players. The guide was considered comprehensive, providing all the necessary information and details that helped in the execution of the exercise. Planners perceived it as a "one-stop shop" for technical credentials, troubleshooting, and Player assistance. This guide allowed Planners to identify areas for improvement in their current ways of working. Despite some minor technical issues and variations in collaboration levels, the exercise was seen as a valuable learning opportunity.

Findings and observations

Policy observations

The findings and observations are based on the impressions collected by the observers and feedback collectors during Cyber Europe 2024.

Operators effectively reported incidents to national authorities and CSIRTs, facilitating smooth cooperation. However, there was no evidence of information exchange at the regional or EU level with their peer energy operators.

A gas storage incident between two Member States highlighted deficiencies in cross-border incident reporting. The NIS1 provisions were not fulfilled unless the receiving CSIRT or NCSA considered cross-border impacts. There was no clear evidence that inquiries about cross-border impacts were performed when receiving incident notifications. However, some CSIRTs mentioned which other Member States had been affected but there is no evidence on how they did this assessment. This shows that the methods were lacking transparency.

Cybersecurity authorities faced challenges in assessing the energy-related aspects of crises, and the sectorial coordination between them and operators within each Member State was insufficient for multi-state incidents. Overall, cybersecurity authorities struggled to assess energy-related crises, underscoring the need for regional analysis of multi-state incidents.

Vertical legislations provided guidance on how to assess cross-border impact for specific sectors. For example, the Network Code for Cybersecurity[4] provides a clear procedure involving CyCLONe authorities for electricity incidents, which will support the regional and European cooperation.

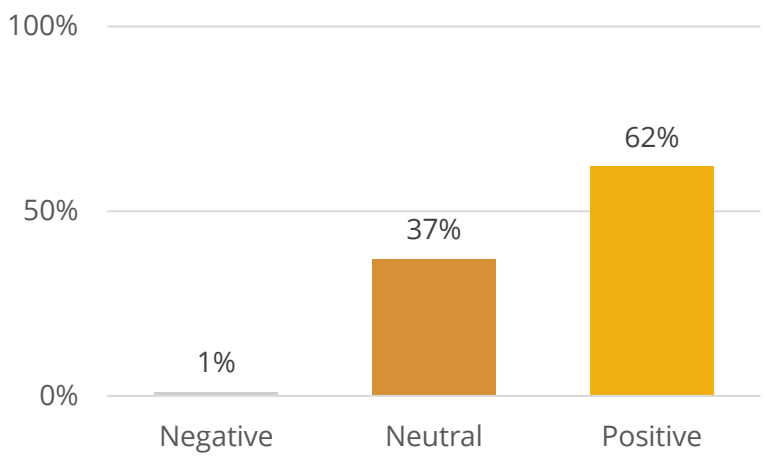
There was no procedure for activating measures in the event of a cross-border gas incident.

[4] 20241103_Regulation_(EU)_2019-943.pdf (eepublicdownloads.blob.core.windows.net)

Social Listening Analysis

During Cyber Europe 2024, a social media analysis[5] was held to present the total number of interactions. The event garnered significant attention on social media platforms and the campaign reached a potential audience of 2 million users, indicating the extensive spread and visibility of the event across various platforms.

Graph 6: Sentiment analysis from Cyber Europe 2024



The strong enthusiasm was driven by keywords such as "developments," "invaluable,", “success”, and "cyber resilience." Neutral sentiment was linked to terms like "analyse" and "coordination."

The analysis showed that X was the dominant social media platform, making up 84% of the activity. LinkedIn had the most engagement with 1,700 likes and 125 shares, and peak activity occurred right after the opening ceremony on the first day and at the end of the second day.

Several Players shared their certificates of participation on LinkedIn and Twitter. Due to privacy settings on LinkedIn, it was not possible to determine the exact number of Players who shared their Cyber Europe 2024 participation certificates. Many profiles were private, suggesting that the actual number of shares was likely higher than what could be observed. However, it is known that approximately 1,000 individuals downloaded their certificates.

In conclusion, the social media campaign for Cyber Europe 2024 was highly effective in engaging a wide audience, driven by key event moments. The campaign successfully highlighted emerging themes in cybersecurity, and the sentiment analysis indicated an overall positive reception and enthusiasm for Cyber Europe 2024.

[5] The tool Talkwalker was used to gather data on social media reach and engagement

03

PART 03:

LESSONS IDENTIFIED AND RECOMMENDATIONS FOR IMPROVEMENT

Lessons identified

from data collected before, during and after Cyber Europe 2024

It is important to emphasise that the below list of lessons identified is not exhaustive as ENISA does not have a view on additional findings. Each sector, Member State, and other entities involved, gathered unique findings related to their specific internal processes and procedures.

All target deadlines for the lessons identified in the following table are dependent on budget and resource availability.

Lesson identified	Owners for mitigation	Target deadline
1. Also involve local Planners in the evaluation process	ENISA and MS Planners	Before the next exercise
2. Provide feedback to Players	ENISA and MS Planners	Next exercise
3. Allow for broad representation	MS Planners	Before summer 2026
4. Communicate and promote the possibility to tailor the exercise scenario (for national contexts)	ENISA and MS Planners	Before summer 2026
5. Offer a dashboard for tracking inject delivery and results	ENISA	Before summer 2026

1. Also involve local Planners in the evaluation process

Integrating local Planners into the evaluation process is needed to capture the nuances and specific challenges faced at the local level. This involvement ensures that the feedback and lessons identified are more comprehensive and contextually relevant and will also contribute to improving the understanding of preparedness of their Players.

Recommendations for improvement:

- Involve local Planners from the start of the evaluation process, ensuring they have a clear understanding of the objectives and evaluation criteria. Their early engagement will provide valuable insights into local conditions and constraints.

- Integrate insights and feedback from local Planners into the final evaluation report. Highlighting their contributions will emphasise the importance of local context in the overall assessment and help identify areas for improvement.

2. Provide feedback to Players

The importance of feedback emerged as a crucial lesson from the exercise, particularly in the context of the high-pressure environment created for participants. While multiple Players expressed a desire for real-time feedback on their performance while handling the technical artifacts, the aim of Cyber Europe 2024 was to simulate a stressful scenario where they had to juggle multiple tasks simultaneously. Given this focus, immediate feedback was not a core component of the exercise. However, the necessity of post-exercise feedback was clear, as it plays an important role in internal evaluation and process improvement.

Recommendations for improvement:

- Conduct post-event meetings and detailed walkthroughs of challenges encountered during the exercise. These sessions should be designed to review what went well and what did not, enabling Players to learn from experiences and improve future performance.

3. Allow for broad representation

Feedback indicated that involving only certain departments limited the robustness of task management and decision-making processes. A more diverse representation can enhance the comprehensiveness and effectiveness of crisis management.

Recommendations for improvement:

- Include representatives from diverse departments within each organisation and cover a wide range of different Player types within the scope of the exercise scenario.
- Consider potential customisation of media and simulation of real-world pressure. If Players do not feel have the impression that media injects are targeted to them or they do not naturally feel the pressure, it is essential to create a realistic environment where they genuinely feel the urgency and intensity.

4. Communicate and promote the possibility to tailor the exercise scenario (for national contexts)

Ensuring the exercise scenario is relevant and aligned with the specific national context is crucial for enhancing the effectiveness of the exercise. The feedback indicated that the scenario was not always tailored to the unique needs of each Member State/organisation and participating Union Entities, which limited their applicability and impact.

Recommendations for improvement:

- Collaborate with local Planners and national authorities to ensure the relevance of the scenario. Engaging with these groups during the planning phase can provide valuable insights into the specific threats and vulnerabilities pertinent to each member State/organisation.
- Train the Planners on how to tailor the scenario, while maintaining coherence with the common scenario, to reflect the specific contexts and potential crisis situations unique to each Member State/organisation specific threats and challenges.

5. Offer a dashboard for tracking inject delivery and results

The feedback from the exercise highlighted the necessity of a centralised dashboard for Planners. This dashboard would ensure that they have a clear understanding of what injects have been delivered along with their status. Such a system would support Planners in following the progress of execution, however this is limited in budget and resources. It will also allow for comprehensive post-exercise evaluation.

Recommendations for improvement:

- Develop a dashboard to track inject deliveries. This would allow Planners to monitor if and when injects were sent, ensuring real-time visibility and accountability. At the end of the exercise, the dashboard would allow for a comprehensive analysis to determine if the injects were addressed, offering an objective evaluation method, beyond self-assessment from Players.

Lessons identified

from organising and planning Cyber Europe 2024

Lesson identified	Owners for mitigation	Target deadline
1. Ensure technical and logistical preparation	ENISA and MS Planners	Before the next exercise
2. Facilitate earlier decision making with Planners	ENISA	Before the next exercise
3. Provide detailed documentation and information sharing in a centralised location	MS Planners	Before the next exercise

1. Ensure technical and logistical preparation

During the exercise, several technical and logistical challenges were encountered, including difficulties with tools applicable to the exercise context and the late dissemination of critical information. These issues delayed Players' ability to optimally perform.

Recommendations for improvement:

- Ensure the early release of information regarding the technical tools. Providing details about the tools well in advance will allow participants to familiarise themselves with the tools and troubleshoot potential issues beforehand.
- Schedule preparatory sessions where Players can practice using the tools in a controlled environment so it will minimise last-minute technical disruptions.

2. Facilitate earlier decision making with Planners

A critical lesson identified from the exercise is the importance of ensuring earlier decision making with Planners and managing their expectations effectively. It is about motivating the Planners to start preparing earlier together with ENISA which will allow them to contribute meaningfully to the design and development of the exercise, ensuring their insights and expertise are integrated from the start.

Recommendations for improvement:

- Schedule regular working sessions with the Planners to agree on the exercise content. This ensures that Planners are well-informed and can provide valuable input. During these meetings they can also share their insights and concerns.

3. Provide detailed documentation and information sharing in a centralised location

A final lesson identified from the exercise highlights the importance of providing detailed documentation and information sharing for Planners and other stakeholders involved.

Recommendations for improvement:

- Promote and communicate that there is a centralised documentation repository available for storing and sharing detailed documentation related to the exercise. By doing this, you ensure easy access for all relevant stakeholders.
- Conduct regular information sharing sessions. By scheduling periodic information sharing sessions or workshops to disseminate key insights, best practices, and lessons learned from other exercises across different teams and departments you ensure that Planners/stakeholders stay up-to-date and can adopt best practices.

Lessons identified

from Players' self-assessment

As previously mentioned, the analysis presented in this section results from data obtained from at least 64% of the Players involved in this exercise.

Preparedness

Before Cyber Europe 2024, Players had moderate confidence in key areas, with substantial room for improvement in familiarity and communication practices. After the exercise, there was a noticeable positive shift in Players' self-assessment across several metrics such as promoting initiatives to increase awareness and implementing business continuity processes. The exercise pinpointed areas needing improvement, such as resource adequacy and cross-border coordination.

Initially, more than half of the experts had reservations about their preparedness. Post-ex, 82% indicated they could effectively implement business continuity processes within their organisations and 64% of Players expressed intent to promote cybersecurity awareness initiatives within their organisations. This improvement highlights the benefits of targeted training and preparedness initiatives.

Collaboration

Before Cyber Europe 2024, the confidence levels among Players varied across different areas of collaboration and was mainly moderate. Effective information sharing across Players saw high confidence levels. Overall, the pre-event data highlights room for improvement in certain aspects of collaboration.

Upskilling and training

Post-event performance highlights the value of hands-on training and practical simulations. 83% of Players expressed their intent to evaluate and improve their skills by participating in future exercises, showing sustained and growing enthusiasm for ongoing professional development in cybersecurity.

Incident Management

Before the exercise, Players exhibited varied levels of confidence in their cybersecurity incident management abilities, highlighting a general sense of uncertainty and the need for enhanced training and preparedness. Slightly less than half of the Players were unsure or

lacked confidence in their capacity to disseminate situational information effectively during the exercise. After the event, Players' assessments were notably positive, demonstrating that their capabilities in detecting, analysing, and responding to cybersecurity incidents are established.

Cyber Europe 2024 significantly enhanced Players' views on preparedness and confidence in handling cybersecurity incidents. This increase in confidence underscores the value of such simulation exercises in reinforcing practical skills and adherence to established procedures. However, to ensure consistently high performance across all scenarios, ongoing training and targeted improvements are recommended.

Awareness

Cyber Europe 2024 was designed to evaluate awareness of cybersecurity-related issues and underscore the importance of cybersecurity preparedness. The exercise aimed to raise Player's cybersecurity awareness within their organisation and enhance their skills. Following the exercise, a notable 64% of Players expressed their intention to promote initiatives to increase cybersecurity awareness within their organisations.

Cooperation and information sharing

This capability area aimed to assess Players' participation in EU and other relevant networks, including CSIRTs networks, and their cooperation at national, EU, and international levels. Before Cyber Europe 2024, confidence levels varied, with moderate preparedness and room for improvement with regards to collaboration. After the exercise, there was a noticeable improvement in cooperation and information sharing, with strong performance in communicating data breaches and coordinating responses. However, participation in EU-level networks remained moderate, indicating potential for enhanced engagement.

Moving forward

The process of converting identified lessons into tangible improvements requires careful analysis and establishing effective strategies for their implementation, including testing their effectiveness.

The first step is to evaluate each lesson for its relevance and the impact it has on current practices, followed by identifying specific areas for improvement in current procedures, training plans, resource allocation or even policies. All involved stakeholders must then prioritise these findings based on urgency and feasibility, ensuring that the most pressing issues are addressed first. Next, a clear action plan should be developed on how prioritised improvements can actually be implemented.

In the specific case of the organisation of Cyber Europe exercises, this means outlining how these identified lessons can be integrated into future editions. By systematically implementing agreed upon and prioritised changes, together with all Member States and other involved organisations, ENISA can ensure that upcoming editions of the exercise remain effective and aligned with its strategic objectives, fostering a culture of continuous improvement that prepares EU for future challenges.

In the case of acting upon findings at organisation, sector or Member State level, ENISA is bound by its mandate and can, in most cases, suggest best practices and provide guidance at best. The steps required in order to achieve substantial advancements in preparedness and resilience are in the hands of the organisation, sector or Member State who identified them.

What ENISA can do, is enabling replaying (parts of) the scenario at Member State or sectorial level, providing the opportunity to test implanted changes for their effectiveness. The scalability of this particular option will depend on demand and prioritisation.

04

PART 04:

CLOSING REMARKS

Closing remarks

We are pleased to conclude this After-Action Report with an affirmation of the success of Cyber Europe 2024, a milestone event that highlighted the critical need for ongoing investment and frequent exercises. It is imperative that organisations take immediate action to refine their processes based on the insights gained from this exercise, and make sure to not delay the implementation of these lessons and improvements until the next exercise.

Our ability to bring thousands of participants together to test their cybersecurity skills and enhance cross-border collaboration continues to be a significant achievement. This year's exercise demonstrated the importance of SOPs and playbooks as essential components for enhancing response capabilities. The key objectives included improving readiness to handle cyber threats, enhancing coordination with supply chain actors, and ensuring timely, high-quality information exchange during crises. Overall, the key objectives were met; however, there is still room for improvement for the different sectors to become fully cybersecurity-ready and resilient.

Looking ahead, the lessons identified from Cyber Europe 2024 will be important in shaping the design of future exercises. Our collective commitment is not only to learn from these lessons but also to take proactive steps to enhance our cybersecurity resilience. The ongoing efforts and support from all parties involved are vital as we continue to strive for further exercises and investment in cybersecurity. As a result, this report plays a pivotal role in guiding future iterations of Cyber Europe, in line with ENISA's ongoing commitment to enhancing cybersecurity capabilities across the EU.

We would like to extend our gratitude to everyone involved in the planning, preparation, execution, and evaluation of Cyber Europe 2024. Your dedication and hard work have been crucial to our success, and we look forward to building on this strong foundation as we prepare for Cyber Europe 2026 and beyond. Together, we are committed to creating a safer and more resilient digital environment for the European Union.

Christian Van Heurck for the CBU TREX Team and ENISA.

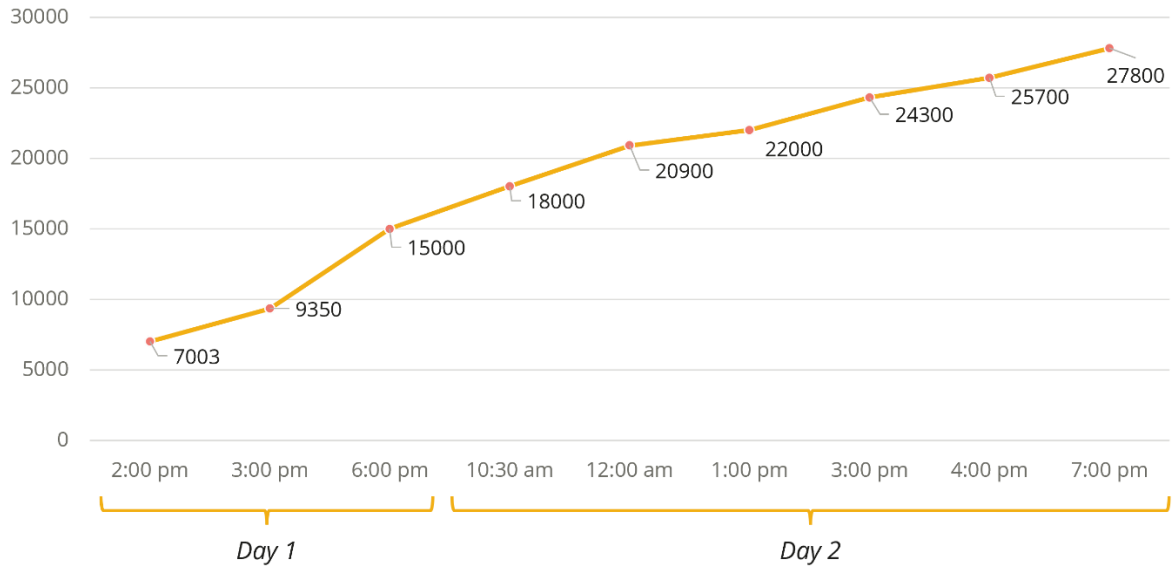
ANNEX

Cyber Europe 2024 in numbers

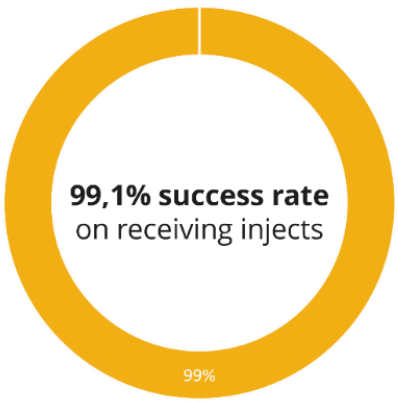
Graph 1: Participation in Cyber Europe 2024

30 countries	4 EU-level networks	4 EUIBAs
• 27 Member States • Norway, Switzerland • United Kingdom	• Cybersecurity: CSIRTs Network, EU-CyCLONe • Energy: ENTSO-E, DSO Entity	• CERT-EU • EUROPOL • ACER • ENISA Operational Cooperation Unit

Graph 2: Email delivery during Cyber Europe 2024



Graph 3: Success rate of sending and receiving injects



Mapping of Players' roles with European Cybersecurity Skills Framework

Player	ECSF[6] mapping	ECSF applicable tasks in the context of CE24
Security / ICT expert	Cyber Threat Intelligence Specialist	• Implement threat intelligence collection, analysis and production of actionable intelligence and dissemination to security stakeholders • Identify and assess cyber threat actors targeting the organisation • Identify, monitor and assess the Tactics, Techniques and Procedures (TTPs) used by cyber threat actors by analysing open-source and proprietary data, information and intelligence • Produce actionable reports based on threat intelligence data • Elaborate and advise on mitigation plans at the tactical, operational and strategic level • Coordinate with stakeholders to share and consume intelligence on relevant cyber threats
	Digital Forensics Investigator	• Identify, recover, extract, document and analyse digital evidence • Preserve and protect digital evidence and make it available to authorised stakeholders • Inspect environments for evidence of unauthorised and unlawful actions • Systematically and deterministic document, report and present digital forensic analysis findings and results

[6] European Cybersecurity Skills Framework (ECSF) — ENISA

	Cyber Incident Responder	• Identify, analyse, mitigate and communicate cybersecurity incidents • Document incident results analysis and incident handling actions • Cooperate with Secure Operation Centres (SOCs) and Computer Security Incident Response Teams (CSIRTs) • Cooperate with key personnel for reporting of security incidents according to applicable legal framework
Crisis management expert	Cyber Incident Responder	• Develop, implement and assess procedures related to incident handling • Communicate cybersecurity incidents • Establish procedures for incident results analysis and incident handling reporting • Document incident results analysis and incident handling actions • Cooperate with Secure Operation Centres (SOCs) and Computer Security Incident Response Teams (CSIRTs) • Cooperate with key personnel for reporting of security incidents according to applicable legal framework
CISO *(optional player)*	Chief Information Security Officer	• Report cybersecurity incidents, risks, findings to the senior management • Ensure the organisation's resiliency to cyber incidents • Manage continuous capacity building within the organisation • Review, plan and allocate appropriate cybersecurity resources
Legal analyst *(optional player)*	Cyber Legal, Policy and Compliance Officer	• Ensure compliance with and provide legal advice and guidance on data privacy and data protection standards, laws and regulations • Assist in designing, implementing, auditing and compliance testing activities in order to ensure cybersecurity and privacy compliance • Cooperate and share information with authorities and professional groups

		• Manage legal aspects of information security responsibilities and third-party relations
DPO *(optional player)*		• Ensure compliance with and provide legal advice and guidance on data privacy and data protection standards, laws and regulations • Assist in designing, implementing, auditing and compliance testing activities in order to ensure cybersecurity and privacy compliance • Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organisation • Monitor audits and data protection related training activities • Cooperate and share information with authorities and professional groups • Manage legal aspects of information security responsibilities and third-party relations
HR *(optional player)*		• Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organisation

Glossary

Term	Description
CERT-EU - *Cybersecurity Service for the Union institutions, bodies, offices and agencies*	An inter-institutional service provider administratively hosted in the European Commission. They contribute to the security of the ICT infrastructure of their 80+ constituents by helping them prevent, detect, mitigate and respond to cyberattacks, and by acting as the cybersecurity information exchange and incident response coordination hub for all of them. For more information refer to CERT-EU
CSIRTs Network (CNW) - *Computer Security Incident Response Teams Network*	A network composed of EU Member States' appointed CSIRTs and CERT-EU ("CSIRTs network members"). The European Commission participates in the network as an observer. For more information refer to CSIRTs Network and CSIRTs Network — ENISA (europa.eu).
EC3 - *European Cybercrime Centre*	The European Cybercrime Centre (EC3) was set up by Europol to strengthen the law enforcement response to cybercrime in the EU and thus to help protect European citizens, businesses and governments from online crime. For more information refer to European Cybercrime Centre - EC3 | Europol
ENISA - *The European Union Agency for Cybersecurity*	The Union's agency that is dedicated to achieving a high common level of cybersecurity across Europe. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure.
EU-CyCLONe - *The European Cyber Crisis Liaison Organisation Network*	A cooperation network for Member States national authorities in charge of cyber crisis management. The network was launched in 2020 and formalised in 2023 with entrance into force of NIS2 art 16. For more information refer to EU CyCLONe — ENISA (europa.eu)
Hotwash	An assessment done after the exercise to evaluate the overall response and identify areas for improvement.
Local Planner	A local Planner is a coordinator who operates at the organisational level. Local Planners work directly with the National Planners to ensure consistency within the overall national exercise strategy.

National Planner	A coordinator who operates at the member state level within an organisation. They are in direct contact with ENISA. During Cyber Europe 2024, it was National Planners who were on site in Athens.
NCSA - *National Cybersecurity Authority*	To prevent cyber-incidents, NCSA through the National Computer Security Incident Response Team (CSIRT), provides immediate incident response in order to contain the situation, minimise damage and draw lessons for future preventions.
NIS2 - *Network and Information Security Directive*	Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)
Planners' exercise guide	A document provided to Planners, containing all the essential information and instructions required to successfully execute the exercise. It includes detailed technical information and serves as a guide to assist Planners on how to better help Players.
Player	Players are the individuals or teams actively engaged in responding to and solving the challenges, or injects, during a cybersecurity exercise. These participants are not just 'playing a game'; they are designated professionals who perform real-world, critical tasks in the exercise, reflecting the responsibilities they would have during an actual cyber incident. Players can include cybersecurity experts, incident response teams, crisis management personnel, and other relevant stakeholders from a participating organisation. Players receive information via injects and respond through their usual communication channels. It's important to note that Players communicate with each other as they would during a real-life crisis.
Social listening	A method where shared posts on social media and general sentiment are evaluated to gain insights into participants' reactions and public opinion.
SOP - *Standard Operating Procedure*	A standard operating procedure is a set of step-by-step instructions for performing a routine activity. SOPs should be followed the same way every time to guarantee that the organisation remains consistent and in compliance with industry regulations and business standards.

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

ISBN: 978-92-9204-679-8
DOI: 10.2824/2285347