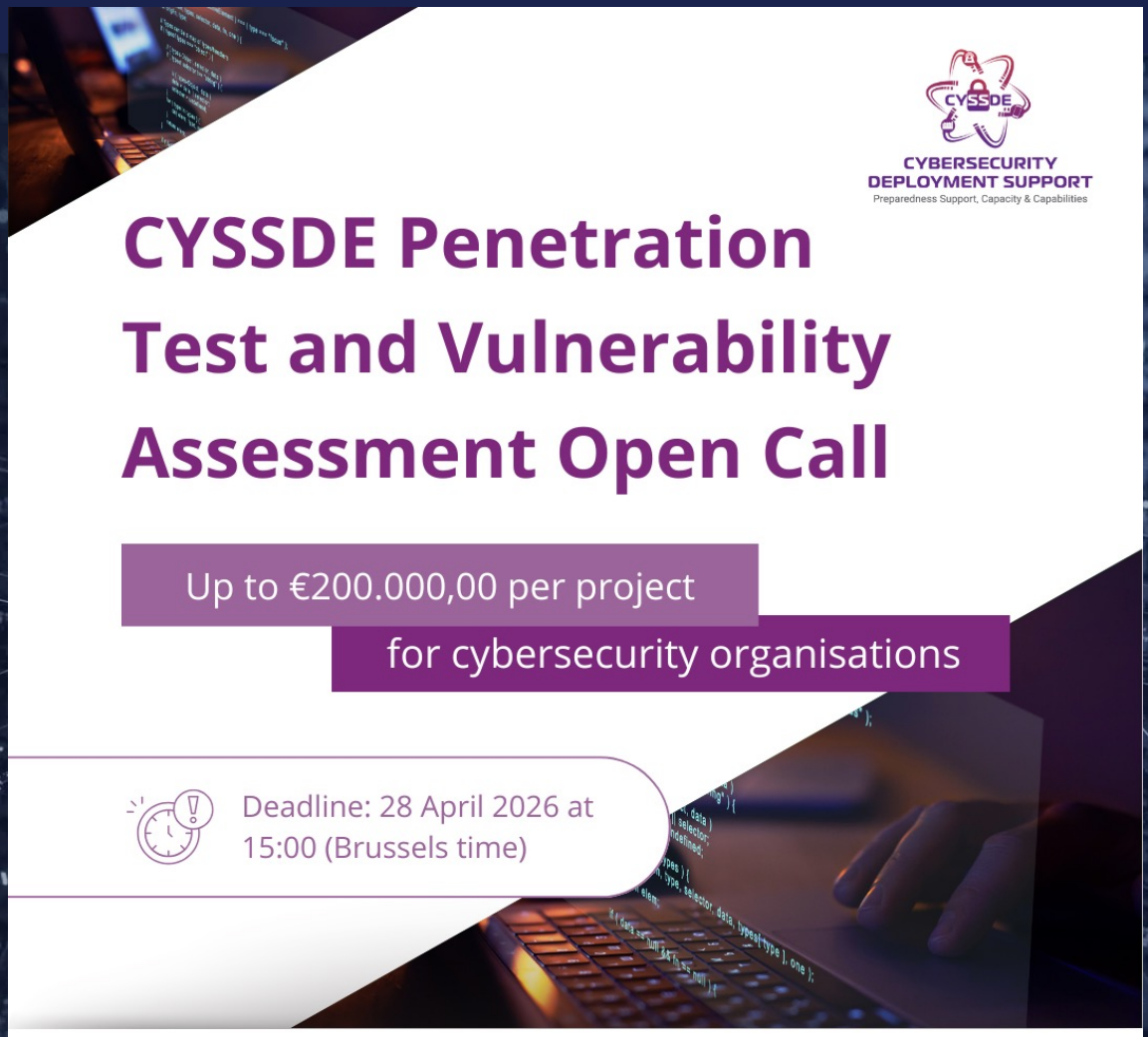


AGENDA : WELCOME TO CYSSDE.EU

- About CYSSDE
- Open Call 3
- Q&A
  - Questions related to Open Call 3 submission
  - Suggestions for participation
  - How to find support

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101158471

ABOUT CYSSDE

1. Support Digital Europe
2. Cybersecurity challenges
3. Cybersecurity expertise – capabilities
4. Cybersecurity capacity
    1. skilled professionals
    2. assessments – variety in quality and results
    3. support contributions of assessments in a global scheme (nr of CVEs)
5. support EU regulatory landscape
6. grow European Cybersecurity industry
7. Strengthen European competitive position

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
CYSSDE CYBERSECURITY DEPLOYMENT SUPPORT

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101158471

ABOUT CYSSDE.EU : EUROPEAN FUNDS FOR SUPPORT

Digital Europe Programme (DIGITAL)

Call for proposals

Deployment actions in the area of cybersecurity

(DIGITAL-ECCC-2023-DEPLOY-CYBER-04)

CYBERSECURITY DEPLOYMENT SUPPORT

Preparedness Support, Capacity & Capabilities

Version 1.0
16 May 2023

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101158471

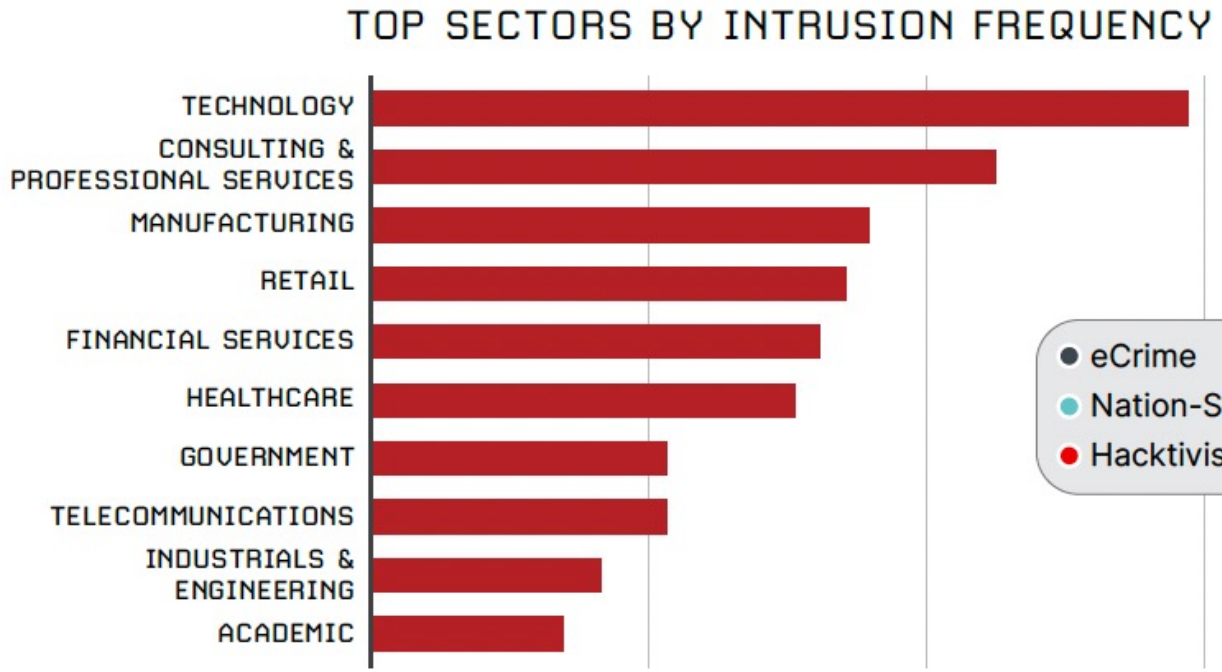
Co-funded by the European Union

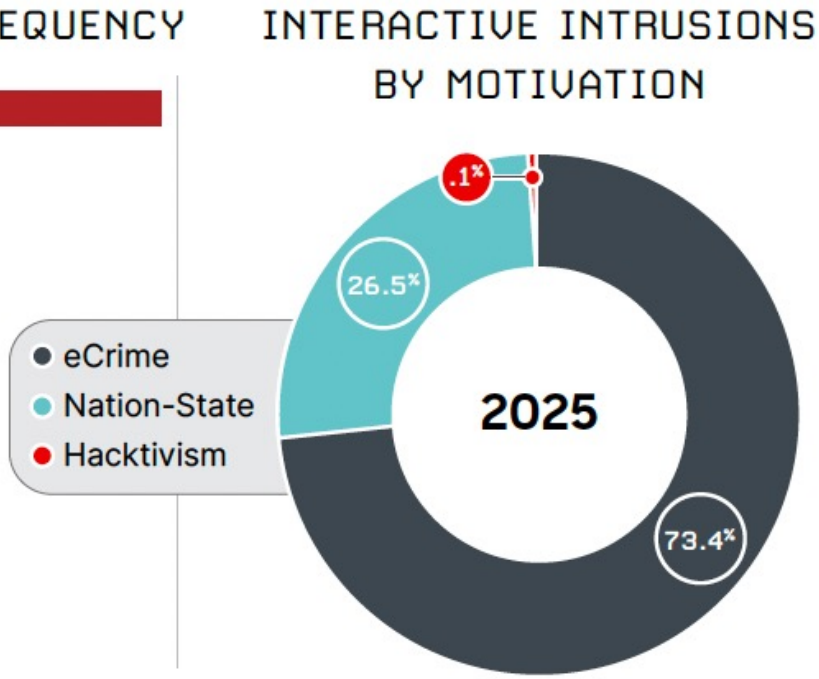
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

CYBERSECURITY DEPLOYMENT SUPPORT
Preparedness Support, Capacity & Capabilities

CYBERSECURITY IN 2026

"Retail & manufacturing were the sectors with most cyber incidents (~3,500)"*





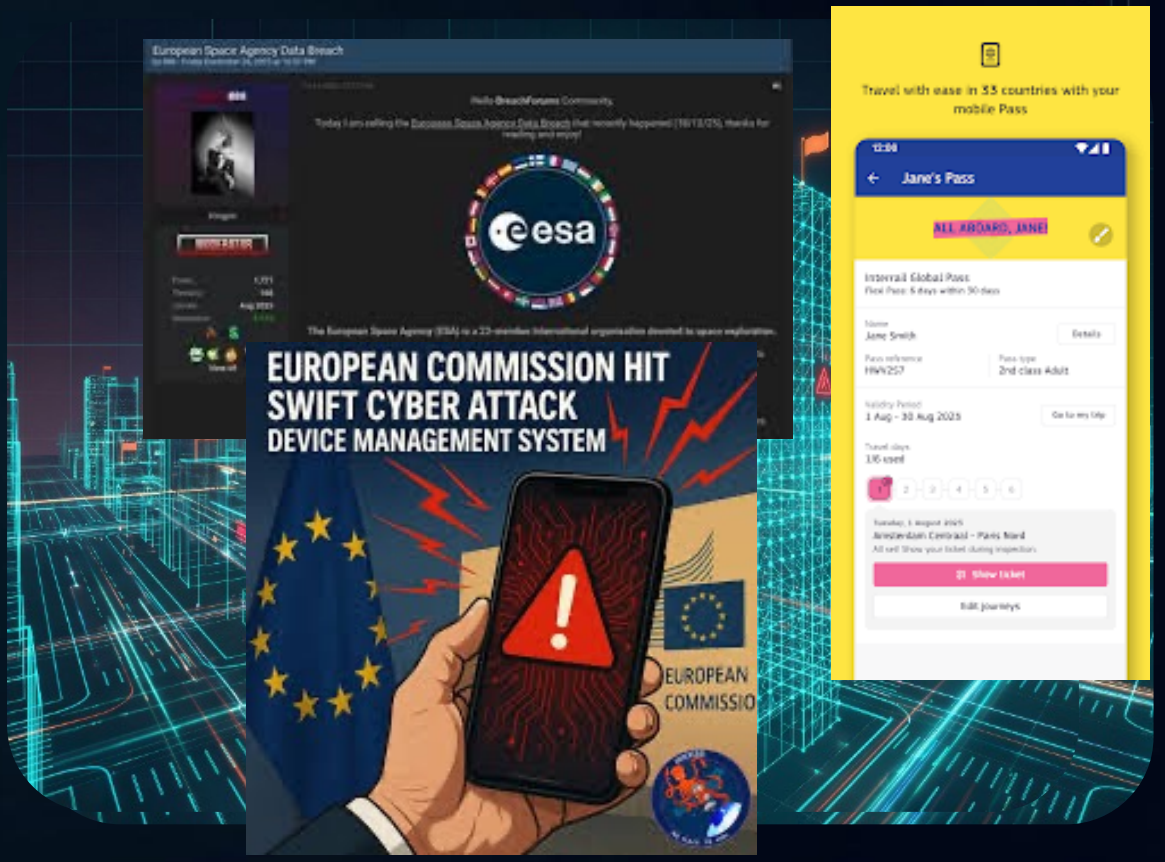
Sources : Crowdstrike 2025, *UK Gov 2025

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101128101

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
CYSSME

Reality Today: Breaches are still around

- Data Security Incident affecting DiscoverEU travellers, 13/01/2026
- European Space Agency Confirms Server Breach, 05/01/2026
- European Commission hit by cyberattackers targeting mobile management platform, 09/02/2026
- Number of personal data breaches in Europe increased by 22 per cent in 2025 – 1.2 billion in fines, DLA Piper 27/01/2026
- ENISA's 2024 analysis revealed 1,276 incidents, with system failures and health sector targets dominant.

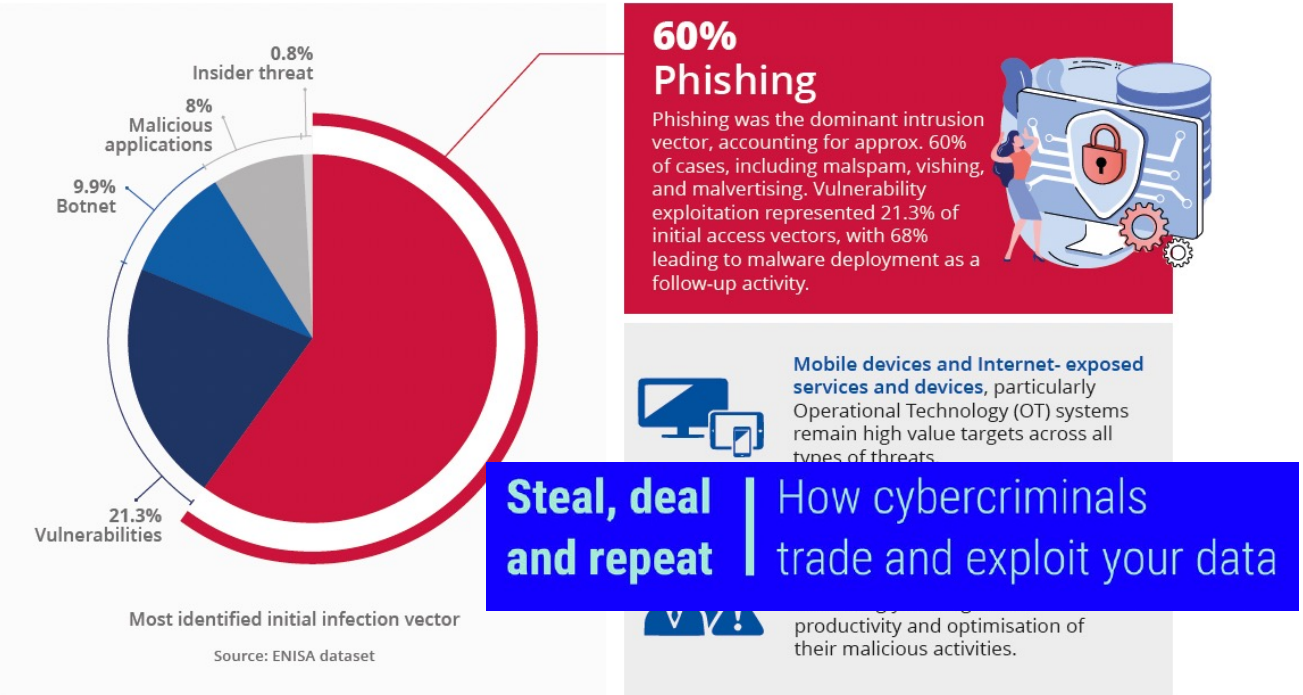


INCIDENTRON.EU

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101158471

This project is financed by Co-funded by the European Union ECCC

CYBERSECURITY IN 2026



Steal, deal and repeat | How cybercriminals trade and exploit your data

Source : ENISA threat landscape 2025, IOCTA 2025

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101128101

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
CYSSME

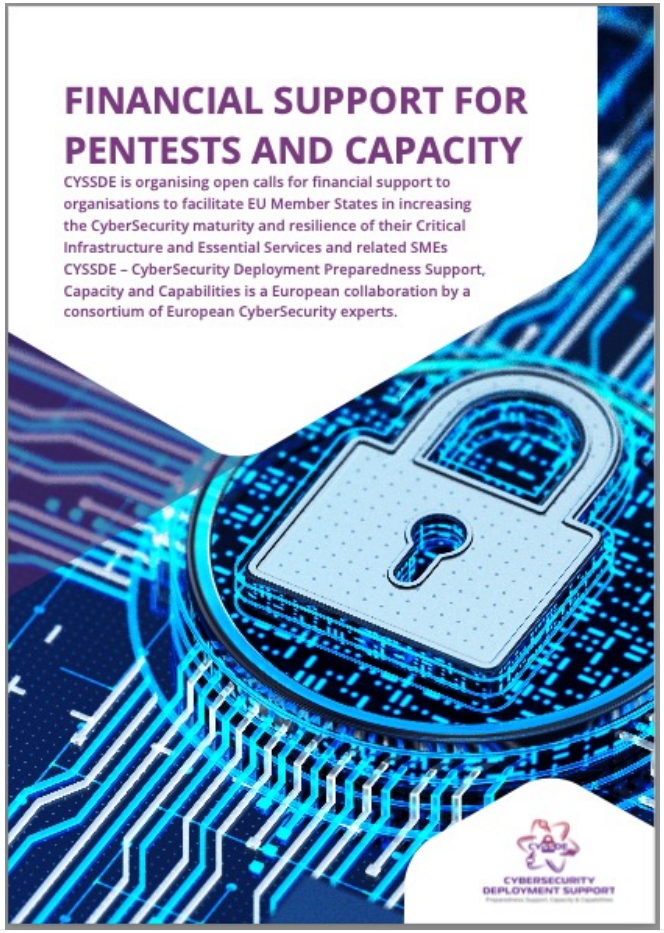
PARTNERS

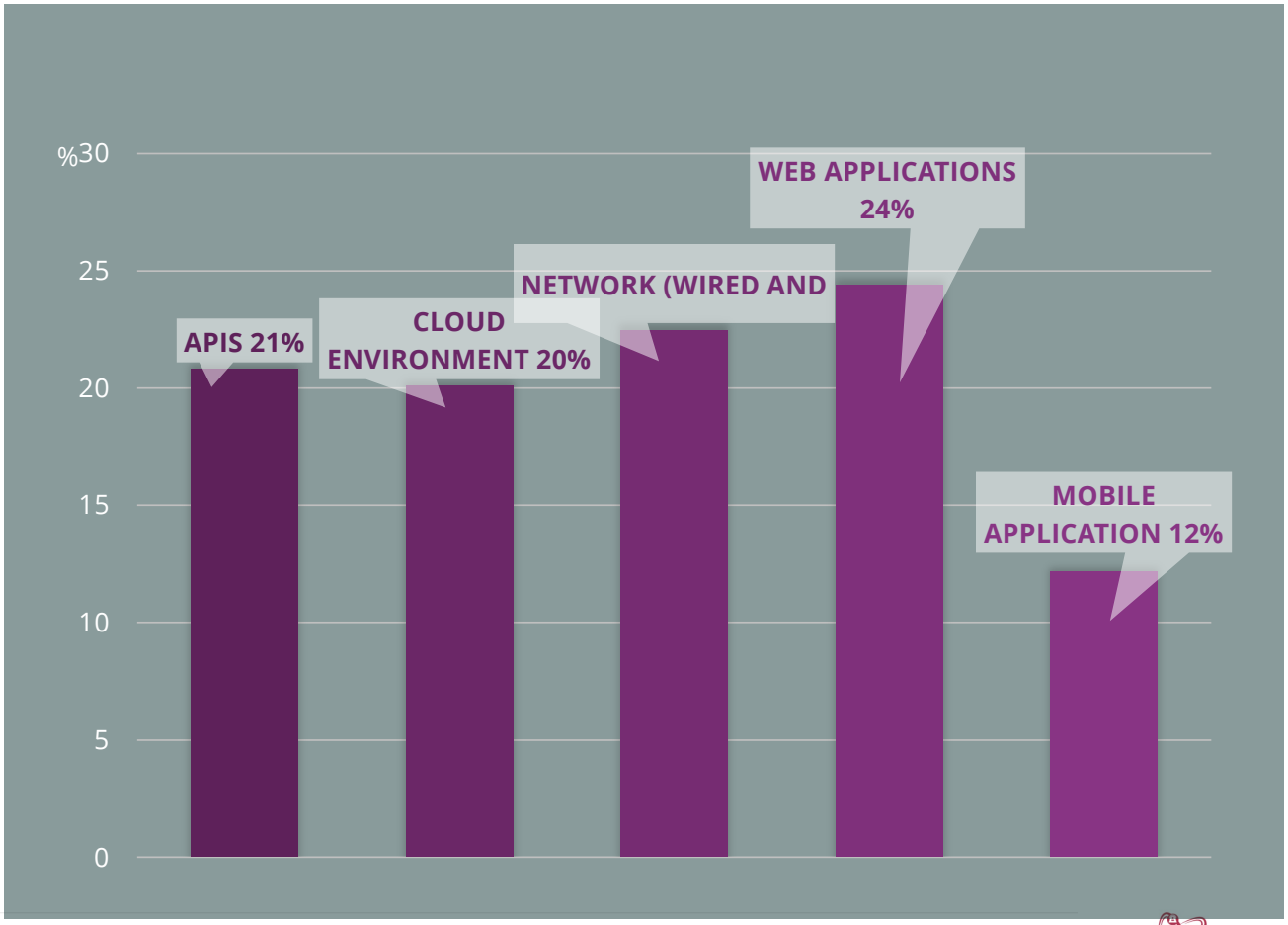
LSEC LEADERS IN SECURITY	FundingBox	incibe_ SPANISH NATIONAL CYBERSECURITY INSTITUTE	GUVERNUL ROMÂNIEI DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ
CYBER RANGES	TOREON Business driven cyber consulting	Ceeyu	NCC-PT PORTUGAL CYBERSECURITY COORDINATION CENTRE NCC-SI SLOVENIA CYBERSECURITY COORDINATION CENTRE NCC CENTRUL NAȚIONAL DE COORDONARE CYBERSECURITY ROMÂNIA

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101158471

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
CYSSDE CYBERSECURITY DEPLOYMENT SUPPORT Preparedness Support, Capacity & Capabilities

REFLECTIONS FROM OC2 : +121 APPLICANTS, 10 PROJECTS, +250 TESTS





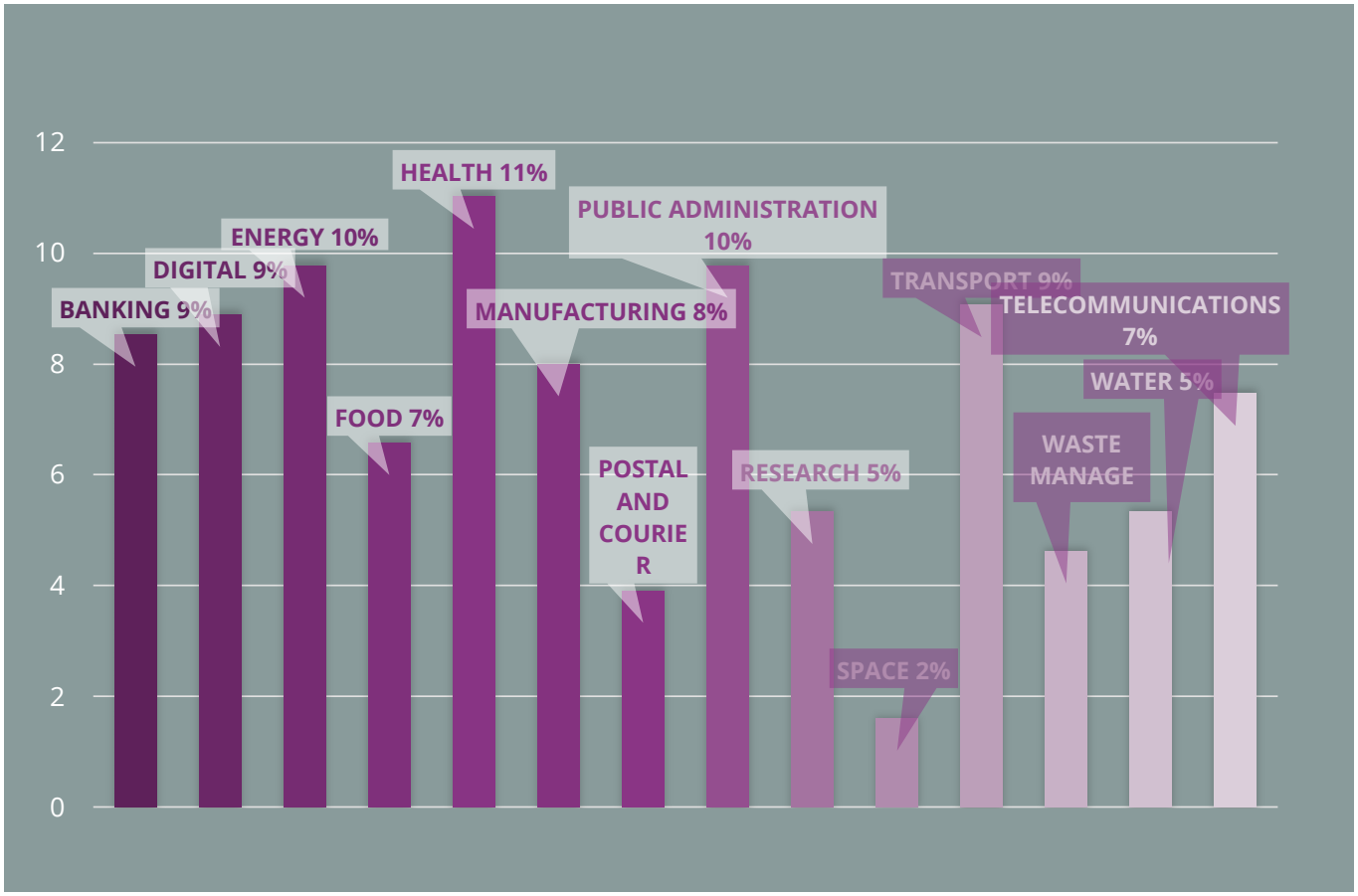
This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101158471

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

CYBERSECURITY DEPLOYMENT SUPPORT
Preparedness Support, Capacity & Capabilities

REFLECTIONS FROM OC2 : ALL DOMAINS, BUT LESS ON FOOD AND SPACE



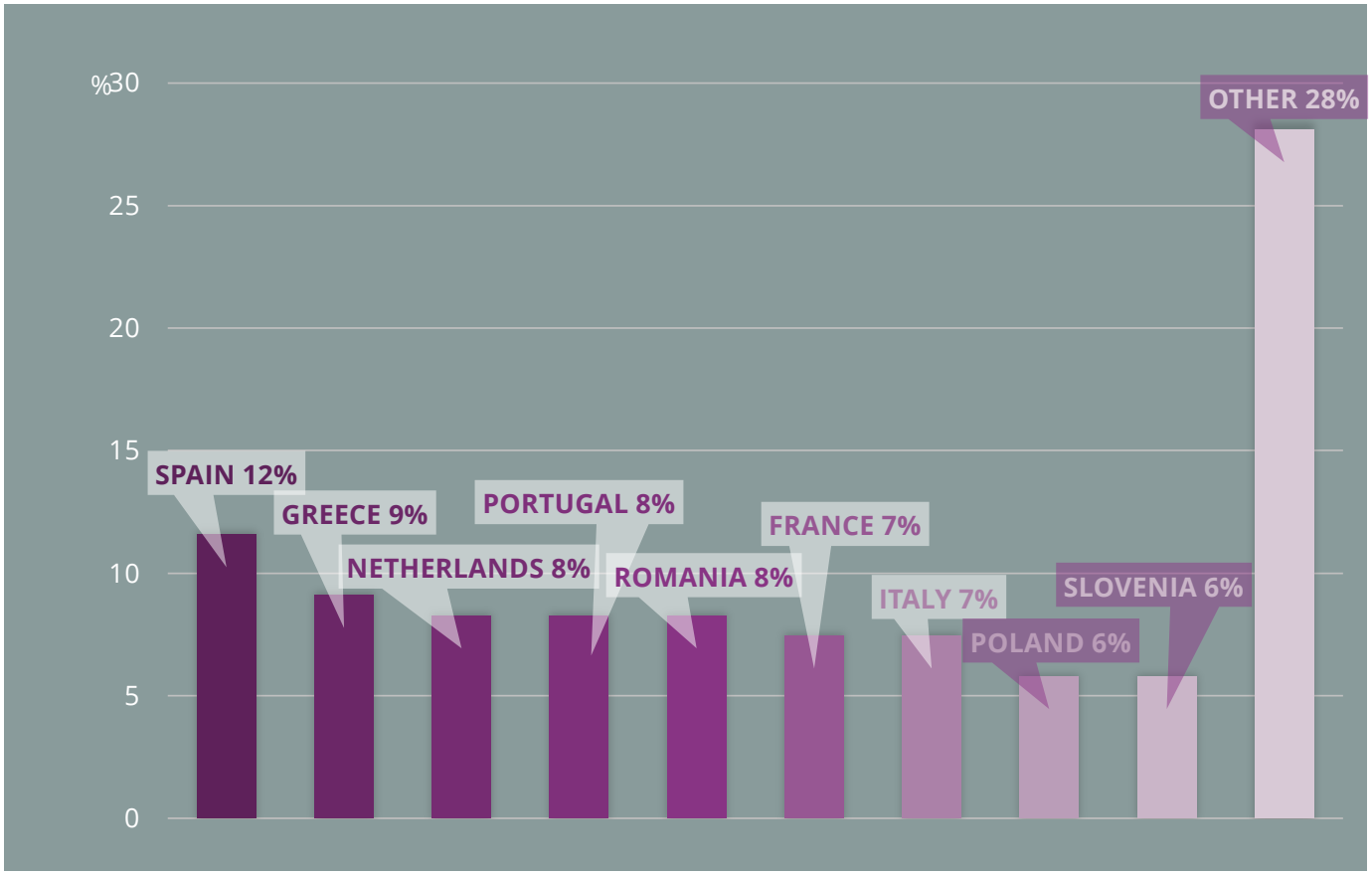
This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101158471

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

CYSSDE CYBERSECURITY DEPLOYMENT SUPPORT
Preparedness Support, Capacity & Capabilities

REFLECTIONS FROM OC2 : EUROPE-WIDE



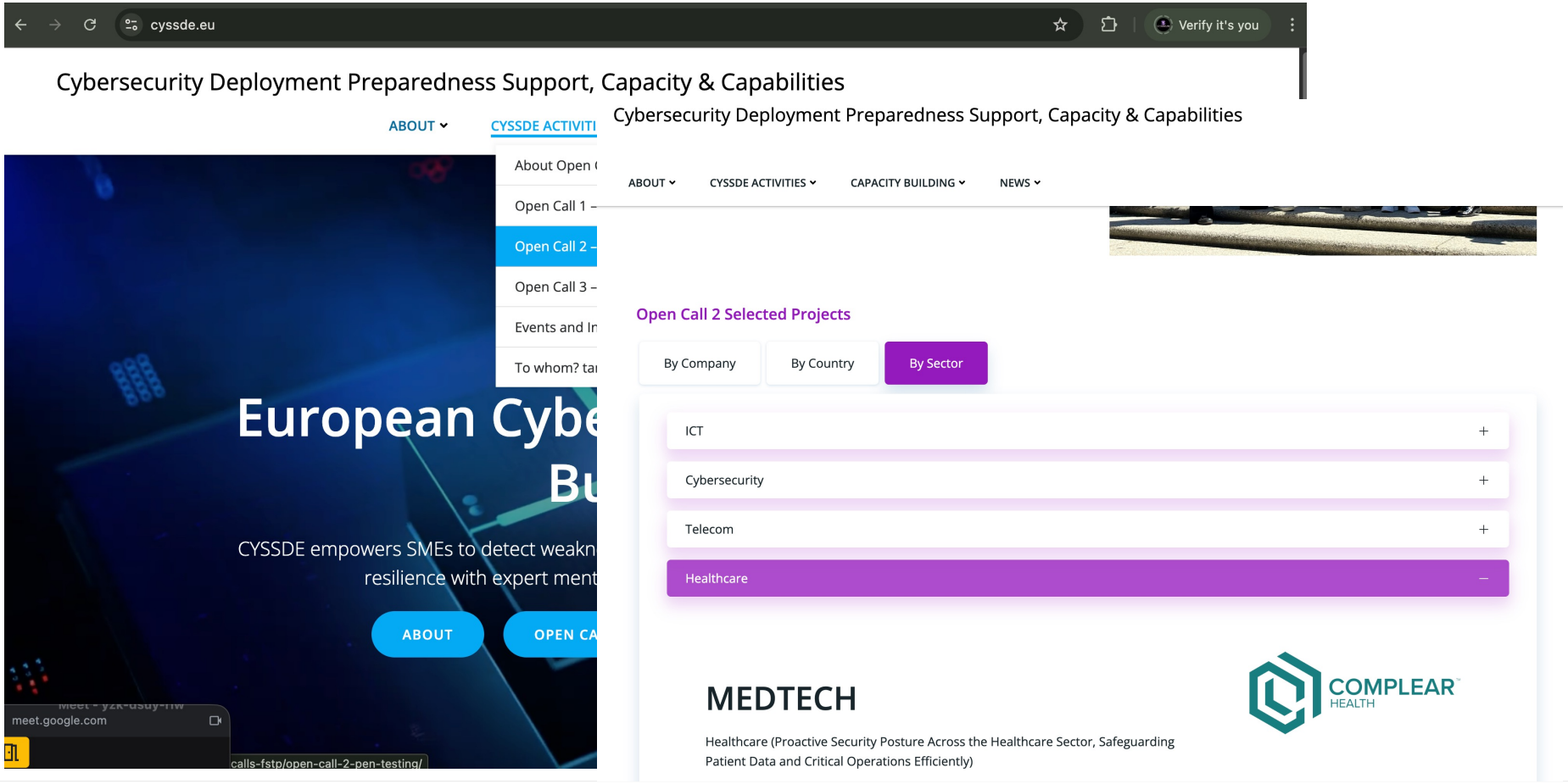
This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101158471

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

CYSSDE CYBERSECURITY DEPLOYMENT SUPPORT
Preparedness Support, Capacity & Capabilities

OC2 PROJECTS : THE 10 WINNERS



This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101158471

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

CYBERSECURITY DEPLOYMENT SUPPORT
Preparedness Support, Capacity & Capabilities

CYSSDE OC3 TARGETTING : CYBERSECURITY EXPERTS

Top Cybersecurity Companies

Cybersecurity companies are your defense against data loss, bot invasions, and account breaches. With a laser focus on predictive analytics, threat intelligence software, and risk mitigation, these cyber companies can mitigate and prevent cyber threats successfully. Fortify your operation with industry heavyweights like Microsoft, CrowdStrike, an...

vices Guide | Cybersecurity Trends >

141 Companies

Hourly Rates | Industry | Reviews | All Filters (2)

Search with AI

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101158471

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

CYSSDE CYBERSECURITY DEPLOYMENT SUPPORT
Preparedness Support, Capacity & Capabilities

OC2 PROJECTS : THE 10 WINNERS - SLOVENIA

CYSSDE PENETRATION TEST AND VULNERABILITY ASSESSMENT OPEN CALL

CYBERSECURITY DEPLOYMENT SUPPORT
Preparedness Support, Capacity & Capabilities

3fs

3fs is a software engineering and consulting firm, specializing in cutting-edge deep tech engineering, cybersecurity, and comprehensive digital transformation. Our extensive experience spans a diverse clientele, from innovative startups to Fortune 500 corporations, with a pronounced focus on highly regulated sectors like MedTech, FinTech, and Telecommunications. At the heart of our operations is a human-first approach to engineering, ensuring that our solutions are not only technologically advanced but also intuitive and user-centric. Security is ingrained in our development lifecycle through a robust DevSecOps methodology, allowing us to deliver world-class digital products with confidence. We empower our clients to navigate and innovate within the complex realms of cloud computing and the Internet of Things, consistently delivering solutions that are secure, scalable, and impactful.

WHY CYSSDE

Our participation in CYSSDE is a cornerstone of our commitment to bolstering cybersecurity resilience across Europe, providing a vital platform for our ANCHOR project. This initiative is designed to proactively address escalating cyber threats in Europe's most critical sectors, starting with healthcare. Through a series of comprehensive penetration tests and vulnerability assessments, we are dedicated to systematically identifying and neutralizing security weaknesses within sensitive ICT infrastructures. This work extends beyond testing—which often happens after the fact—by introducing proactive wargame training simulations. These scenarios are designed for essential personnel in critical organizations, who are often stretched thin, helping them become more resilient against future threats and directly supporting the objectives of the NIS2 directive to create a more secure digital fabric for all European citizens.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them. This project is supported by the European Cybersecurity Competence Centre and its members.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

CYBERSECURITY DEPLOYMENT SUPPORT
Preparedness Support, Capacity & Capabilities

OC2 PROJECTS : THE 10 WINNERS - GERMANY

CYSSDE PENETRATION TEST AND VULNERABILITY ASSESSMENT OPEN CALL

CYBERSECURITY DEPLOYMENT SUPPORT
Preparedness Support, Capacity & Capabilities

asvin

asvin GmbH, based in Stuttgart, develops innovative solutions for context-based cyber risk analysis, supported by AI-driven Cyber Threat Intelligence. The company focuses on industrial enterprises, critical infrastructure (KRITIS), and public sector clients. asvin helps organizations simplify risk management, strengthen the security of digital infrastructures, and ensure compliance with EU regulations such as NIS2 and the Cyber Resilience Act. Its platform delivers actionable insights to decision-makers, enhances operational resilience, and supports targeted security measures. While Cyber Threat Intelligence is part of the offering, it primarily serves to improve risk analysis and overall security rather than acting as the company's main USP.

WHY CYSSDE

Participation in the CYSSDE Open Call offers asvin a unique opportunity to collaborate with Europe's leading cybersecurity experts and access valuable support for developing its AI-driven Cyber Threat Intelligence solutions. By converting unstructured threat data into actionable insights for SOC analysts, CISOs, and regulators, asvin enhances the security and resilience of critical digital infrastructure. The program also allows alignment with EU frameworks such as NIS2 and the Cyber Resilience Act, reinforcing supply chain security across industries. Through participation, asvin not only strengthens its innovation capabilities but also contributes to a more secure and resilient European digital ecosystem.

chargeIQ

chargeIQ is an innovative company specializing in the management and automated billing of charging infrastructure for electric vehicles. With a modular, user-focused software platform, chargeIQ enables the efficient operation of private and semi-public charging points and supports emission-free mobility for various use cases. The platform is manufacturer-independent, offering flexibility in hardware, integration with advanced energy management systems, and seamless roaming network access. Core values include sustainability, openness, transparency, and integrity, with a strong emphasis on customer-focused solutions and ongoing improvement. ChargeIQ works with a wide-ranging partner network and drives innovation through research projects in the field of electromobility and charging security.

WHY CYSSDE

Participation in the CYSSDE Open Call is crucial for chargeIQ as it provides the opportunity to access substantial funding, mentoring, and support from leading European cybersecurity experts. Through this program, chargeIQ can strengthen its cybersecurity capabilities, conduct in-depth automated penetration testing both for charging stations from various manufactures and software providers, and ensure compliance with EU directives such as NIS2 and the Cyber Resilience Act. Engaging in the Open Call will not only enhance chargeIQ's security posture and innovation but also improve the overall resilience of critical digital infrastructure and contribute to the broader EU cybersecurity landscape.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them. This project is supported by the European Cybersecurity Competence Centre and its members.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

CYBERSECURITY DEPLOYMENT SUPPORT
Preparedness Support, Capacity & Capabilities

OC2 PROJECTS : THE 10 WINNERS - SPAIN

CYSSDE PENETRATION TEST AND VULNERABILITY ASSESSMENT OPEN CALL

CYBERSECURITY DEPLOYMENT SUPPORT
Preparedness Support, Capacity & Capabilities

TARLOGIC
CYBERSECURITY EXPERTS

Tarlogic is one of Europe's leading providers of advanced cybersecurity services, with an in-house team of over 150 specialists and more than 14 years of experience. The company is a trusted partner for organizations across critical industries, delivering solutions in auditing, penetration testing, vulnerability management, and incident response. Tarlogic's technology-agnostic and integration-oriented approach ensures services are seamlessly adapted to each client's ecosystem, enhancing resilience against evolving cyber threats while supporting operational efficiency and regulatory compliance. To date, Tarlogic has safeguarded over 300 clients throughout Europe with services including advanced penetration testing, security assessments, attack surface reduction, incident response, and cyber intelligence. Through innovation, technical excellence, and a client-centric vision, Tarlogic contributes to protecting critical infrastructure and advancing EU-wide cybersecurity objectives such as the NIS2 Directive.

WHY CYSSDE

Participating in CYSSDE is essential for Tarlogic as it amplifies our role in strengthening Europe's cyber resilience. Through more than 100 planned pentests and vulnerability assessments across 3 Essential Service Operators in different EU countries, we will help identify unknown vulnerabilities, validate security controls, and drive continuous improvement of defenses. These activities directly support the objectives of the NIS2 Directive, ensuring that entities critical to Europe's economy and society can mitigate risks and remain resilient against emerging threats. With more than 23 million EU clients impacted, the project's cross-border scope enhances Europe's collective security. CYSSDE also provides Tarlogic an international platform to promote results, reinforce our position as cybersecurity experts, and advance our internationalization goals, ensuring our work contributes both technically and strategically to addressing Europe's cybersecurity challenges.

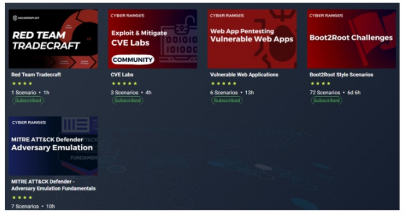
Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them. This project is supported by the European Cybersecurity Competence Centre and its members.

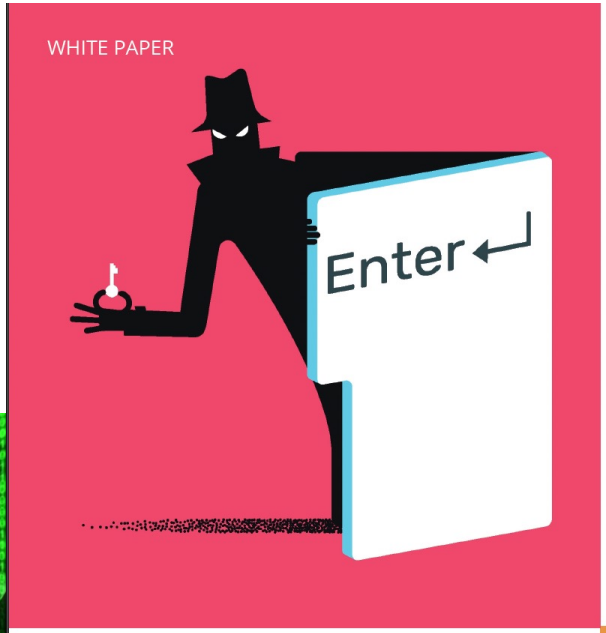
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

CYBERSECURITY DEPLOYMENT SUPPORT
Preparedness Support, Capacity & Capabilities

DIGITAL – CYBER – NIS2 - CYSSDE OFFERING



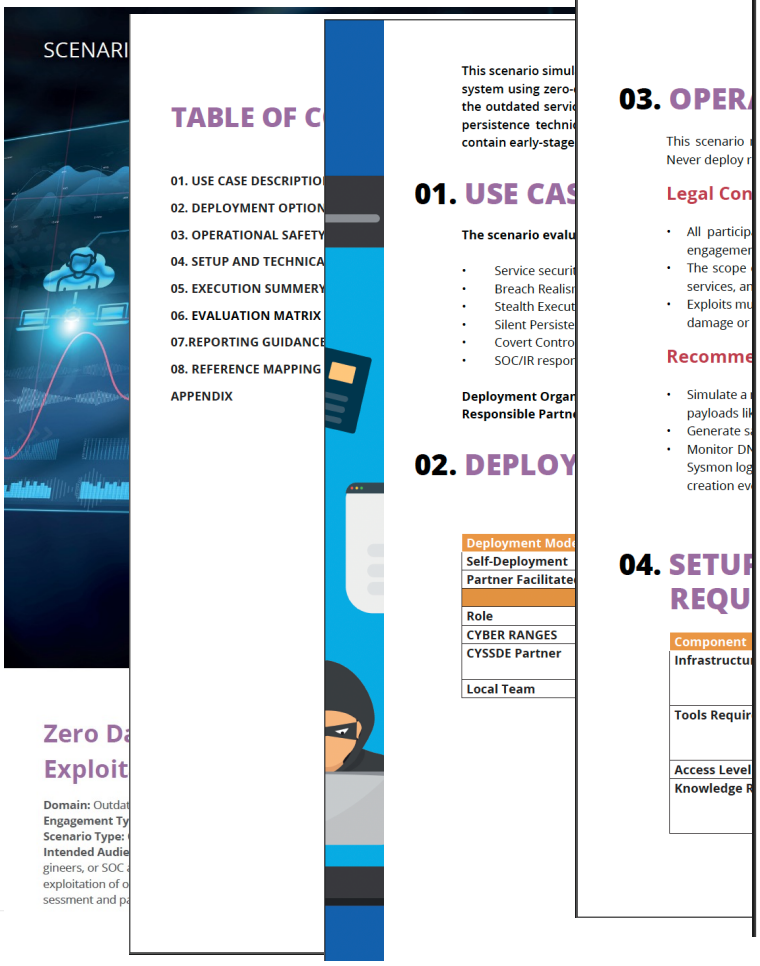
read more



This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101158471

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
CYBERSECURITY DEPLOYMENT SUPPORT
Preparedness Support, Capacity & Capabilities

CYSSDE PENETRATION TESTING SCENARIOS



05. EXECUTION SUM

Phase	Description
Recon & Setup	Kali Linux machi test machine wi tomcat service a rable print spoo passwords
Initial Access / Exploit execution	Nmap, Metasplo Defender logs, c spoofer, sliver c set-WMIEvent
Stealthy Execution	Standart User o
Persistence	Scanning, Red T work, C2 framev point monitorin ce and privesc, with simple tool
Privilege Escalation	Elevate privilege using known vul behaviors.
Command & Control (C2)	Maintain a steal on back to the a
Exfiltration	Simulate theft o data or manipul systems.
Exploit Detection	Monitor for TCP backs
Response	IR engagement, tem

06. EVALUATION MATRIX (D2.7 ALIGNMENT)

Dimension	Value
Resources Required	1–2 people (red teamers, or IT sec. engineers)
Cost	Minimal with open-source tools
Skills Needed	Basic scanning + Metasploit usage + C2 usage + privesc knowledge + persistence knowledge
Expected Outcome (Minimum)	Exploit sent and executed + exfiltration done succesfully, no detection
Expected Outcome (Maximum)	Exploit detected, service turned off, Metasploit failure, c2 failure
Continuous Assessment Ready?	Yes – simulate monthly, rotate templates
Support Needed?	Optional expert review
NIS2 Coverage Estimate	Article 21: ~90%, Article 23: ~50%, Article 24: ~0%, Article 20: ~40%

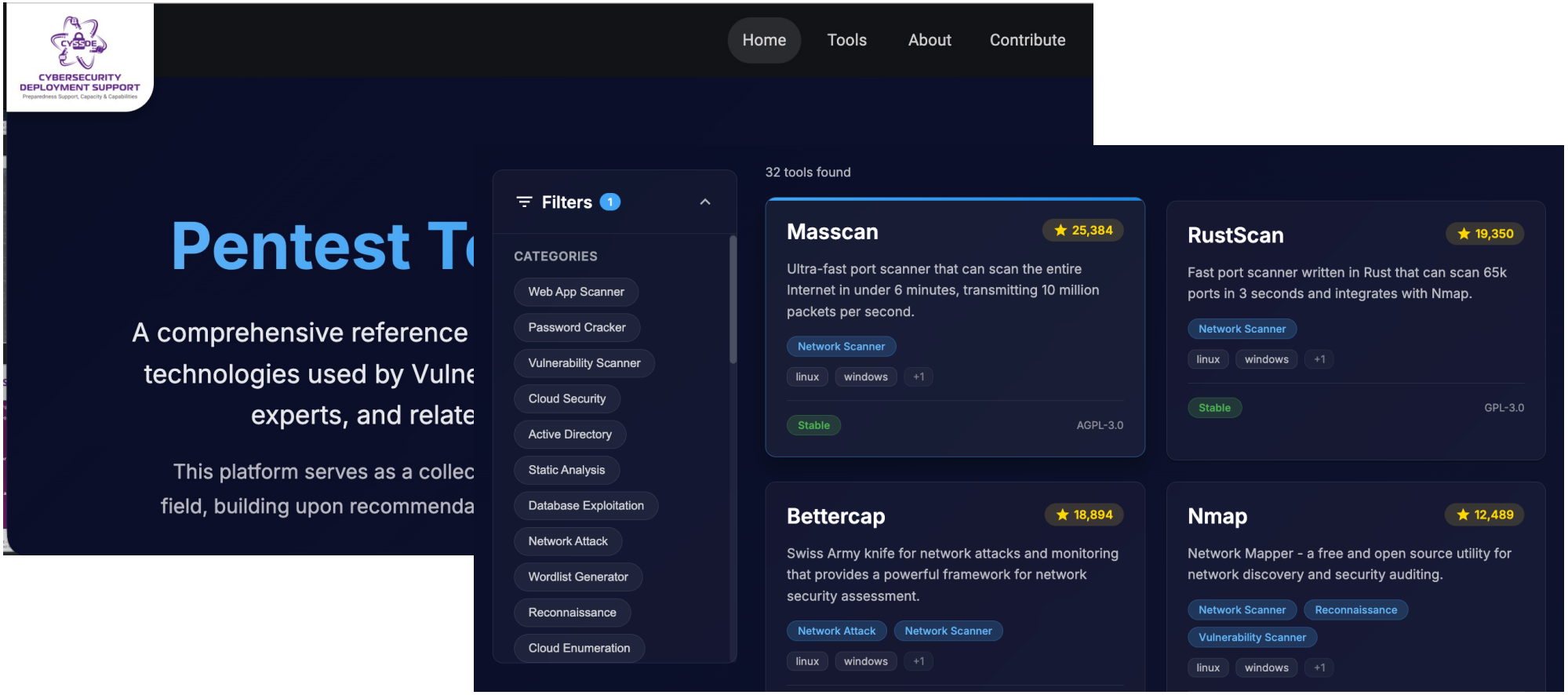
07. REPORTING GUIDANCE

Scenario Summary: Scanning the target tomcat service, executed exploit from Metasploit to gain system access, gain persistence and then doing privilege escalation. Exfiltrate using the tunnel opened with c2.
Key Findings: Awareness gaps, EDR log visibility, insufficient outbound traffic control, not segmented network
Business Relevance: Primary vector for ransomware, and insider compromise
Recommended Mitigations: - Apply network segmentation between enterprise and OT - se Web Application Firewalls (WAF) to block exploit attempts - Restrict PowerShell to Constrained Language Mode - Block WMI write access via GPO or endpoint hardening - Disable the Print Spooler service on non-print servers/workstations - Use Defender for Endpoint or Zeek to detect C2 behavior - Egress filtering: block outbound HTTPS to unknown domains

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101158471

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
CYSSDE CYBERSECURITY DEPLOYMENT SUPPORT Preparedness Support, Capacity & Capabilities

CYSSDE GUIDANCE – TOOLS – CYSSDE.EU



This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101158471

Funded by the European Union
ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE
CYBERSECURITY DEPLOYMENT SUPPORT
Preparedness Support, Capacity & Capabilities


OPEN CALL 3!!
CYSSDE
CYBERSECURITY DEPLOYMENT SUPPORT
Preparedness Support, Capacity & Capabilities
OPEN CALL
Penetration Test & Vulnerability Assessment
Up to 11-12 proposals funded!!!
Receive up to
200.000€
Opening Date
February 27th, 2026
10 AM Brussels time (CET)
Closing Date
April 28th, 2026
3PM Brussels time
(CET)
Co-funded by the European Union
Co-funded by the European Union under grant agreement N 101158471. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them
ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

CYSSDE OC3 IMPACT TARGETTING : CRITICAL INFRASTRUCTURE

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101158471

Co-funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

CYSSDE
CYBERSECURITY DEPLOYMENT SUPPORT
Preparedness Support, Capacity & Capabilities

CYSSDE OC3 IMPACT TARGETTING : NIS2 ENTITIES

Sector	Subsector	Jurisdiction	NIS-1 & CER entities (+ equivalent)	Large entities (more than 250 employees **or** more than 50 million revenue)	Medium (more than 50 employees **or** more than 10million revenue)	Small & Micro
Annex I: Sectors of high criticality						
1. **Energy**	Electricity; district Heating &cooling; Gas; Hydrogen; oil;	The Member State(s) where it is established	Essential	Essential	Important, except if identified as essential by Member State	Not in Scope, **except if identified as essential or important by national authorities** due to sole service, significant impact, essential to society
2. **Transport**	Air; Water; Rail; Road					
	Special case: Public Transport: **only** if identified as CER					
3. **Banking**	Credit institutions **(attention: DORA lex specialis)**					
4. **Financial Market Infrastructure**	Trading venues, central counterparties **(attention: DORA lex specialis)**					
5. **Health**	Healthcare providers; EU reference laboratories; R&D of medicinal products; manufacturing basic pharma products and preparations; manufacturing of medical devices critical during public health emergency					
	Special case: entities holding a distribution authorization for medicinal products: **only** if identified as CER					
6. **Drinking Water**						
7. Waste Water	(only if it is an essential part of their general activity)					
8. **Digital Infrastructure**	Qualified trust service providers					
	DNS service providers (excluding root name servers)	**One stop**: Only the MS where they have their main establishment		Essential		
	TLD name registries					
	Providers of public electronic communications networks	Member State in which they **provide their services**		Essential		Important, except if identified as essential based on National risk assessment
	Non-qualified trust service providers	The Member State(s) where it is established				
	Internet Exchange Point providers		Essential	Essential	Important, except if identified as essential by Member State	Not in Scope, **except if identified as essential or important**
	Cloud computing service providers	**One stop**: Only the MS where they have their main establishment				
	Data centre service providers					
	Content delivery network providers					
8a. ICT-service management	Managed (Security) Service Providers					
9. Public Administration entities	Of central governments (excluding judiciary, parliaments, central banks; defence, national or public security).	MS that established them		Essential		
	Of regional governments: risk based. (Optional for Member States: of local governments)			Important, except if identified as essential by Member State		
10. Space	Operators of ground-based infrastructure (by MS)	The Member State(s) where it is established		Essential	Important, except if identified as essential by Member State	Not in Scope, **except if identified as essential or important**
Annex II: other critical sectors						
1. Postal and courier services		The Member State(s) where it is established	Essential	Important, except if identified as essential by Member State		Not in Scope, **except if identified as essential or important by national authorities** due to sole service, significant impact, essential to society
2. Waste Management	(only if principal economic activity)					
3. Chemicals	Manufacture, production, distribution					
4. Food	Production, processing and distribution					
5. Manufacturing	(in vitro diagnostic) medical devices; computer, electronic, optical products; electrical equipment; machinery; motor vehicles, trailers, semi-trailers; other transport equipment (NACE C 26-30)					
6. Digital providers	online marketplaces, search engines, social networking	**One stop**: Only the MS where they have Main establishment				
7. Research	Research organisations **(excluding education institutions)**	Member State(s) where established				
Entities providing domain name registration services		**One stop**: Only the MS where they have Main establishment	*All sizes, but only subject to Article 3(3) and Article 28*			

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101158471

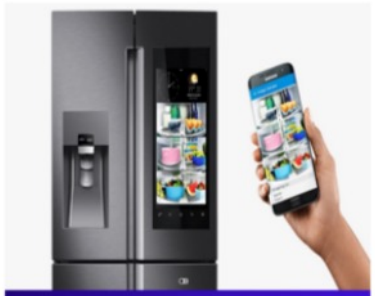
Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

CYSSDE CYBERSECURITY DEPLOYMENT SUPPORT
Preparedness Support, Capacity & Capabilities

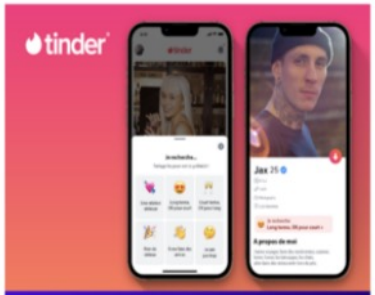
CYSSDE OC3 IMPACT TARGETTING : PDE MANUFACTURERS

Products with digital elements



Consumer products

Smart cities



Non-essential software

Critical products with digital elements

Firewalls

Industrial Control Systems

Essential software

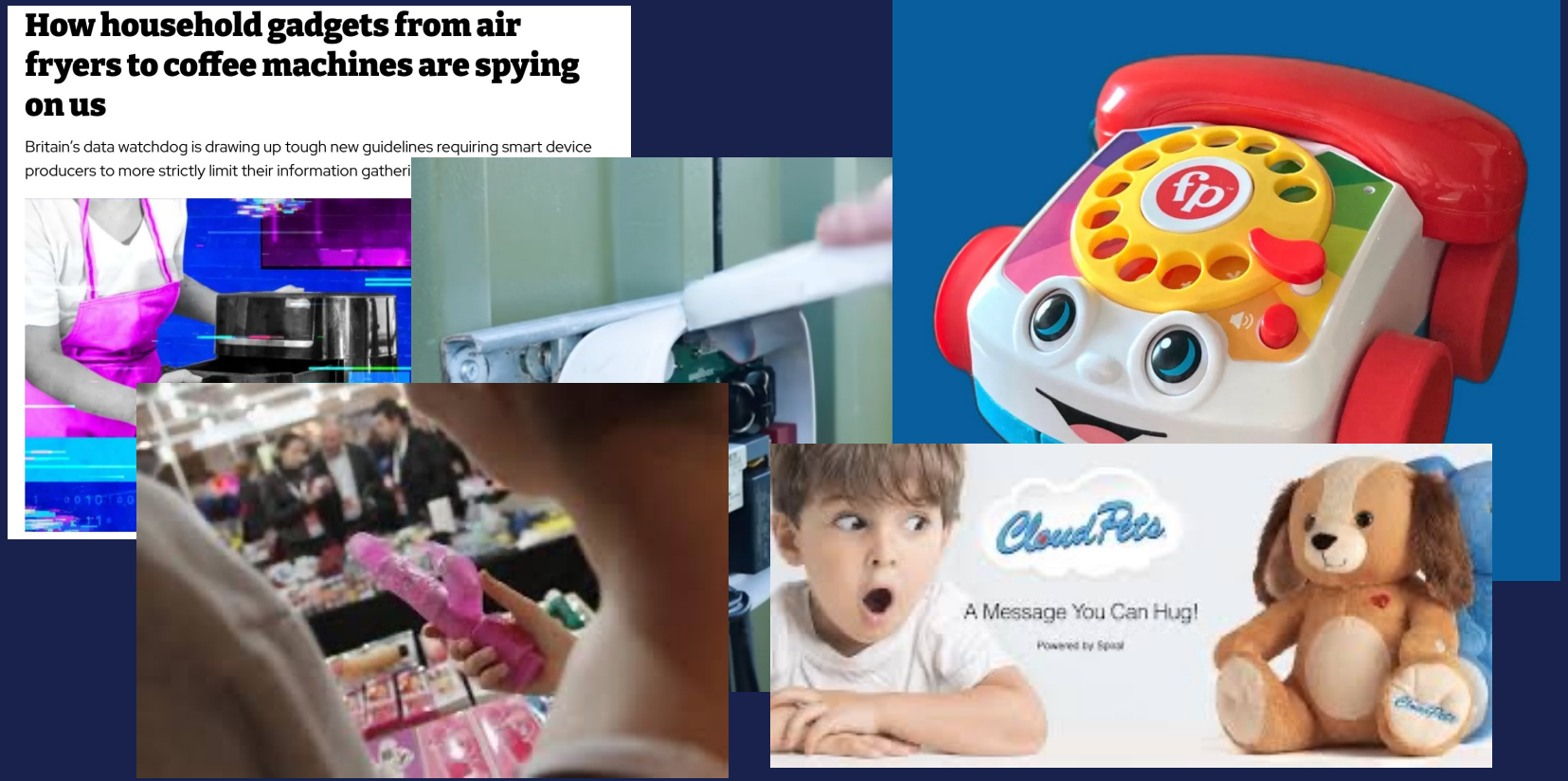
This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101158471

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

CYSSDE CYBERSECURITY DEPLOYMENT SUPPORT
Preparedness Support, Capacity & Capabilities

Consumer Electronics Cybersecurity



Business Electronics Cybersecurity

10,000+ Fortinet Firewalls Exposed To 5-Year-Old MFA Bypass Flaw Amid Active Exploitation

Cisco Identity Services Engine (ISE)

Twenty vulnerabilities in Access Manager, registration unit, and Exos server for corporate locking systems. Reporting took years.

Almost Two Dozen Vulnerabilities

Jan 26, 2026 at 9:08 pm CET

Co-funded by the European Union

ECCC

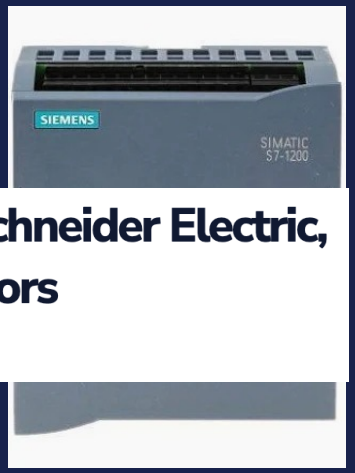
Critical Electronics Cybersecurity

CVE-2025-5310 – Dover Fueling Maglink X
manipulate fueling operations or delete configurations

CISA flags critical ICS vulnerabilities in Siemens, Schneider Electric, ABB equipment affecting critical sectors

APRIL 23, 2025

CVE-2020-28895 – Rockwell, 09/2025
1:1 NAT mapping for up to 32 devices, allowing machines with identical IP addresses to coexist on a single network



CVE-2022-38465 10/2022
bypass memory protection and execute arbitrary code on the PLC.

Benefits for Participants

Team up with others : partners, customers, suppliers, and discover joint challenges

Financing of Penetration Testing, Vulnerabliity Assessments for 50%. Also for tooling and capacity developments

Get additional mentoring for your activities, reach and support, but also to promote your results and get EU visibility

Enhanced collaboration with industry and expert peers to improve skills and share knowledge and expertise

Contribution to the development of EU cybersecurity resilience and protection by enabling capacity and capability – building

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101158471

Funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

CYSSDE CYBERSECURITY DEPLOYMENT SUPPORT Preparedness Support, Capacity & Capabilities

CYSSDE : GOALS AND EXPECTED OUTCOMES

230

Conduct **230 or more penetration tests and / or vulnerability assessmnets** across the EU

Identify and address **vulnerabilities** (with SMEs and / or Essential / Important Entities and critical infrastructure)

€4m

Manage a **funding pool** with over **€4m** available

Present and Enhance pentesting methods

Effective coordination and **capacity-building** in member states

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

CYBERSECURITY DEPLOYMENT SUPPORT

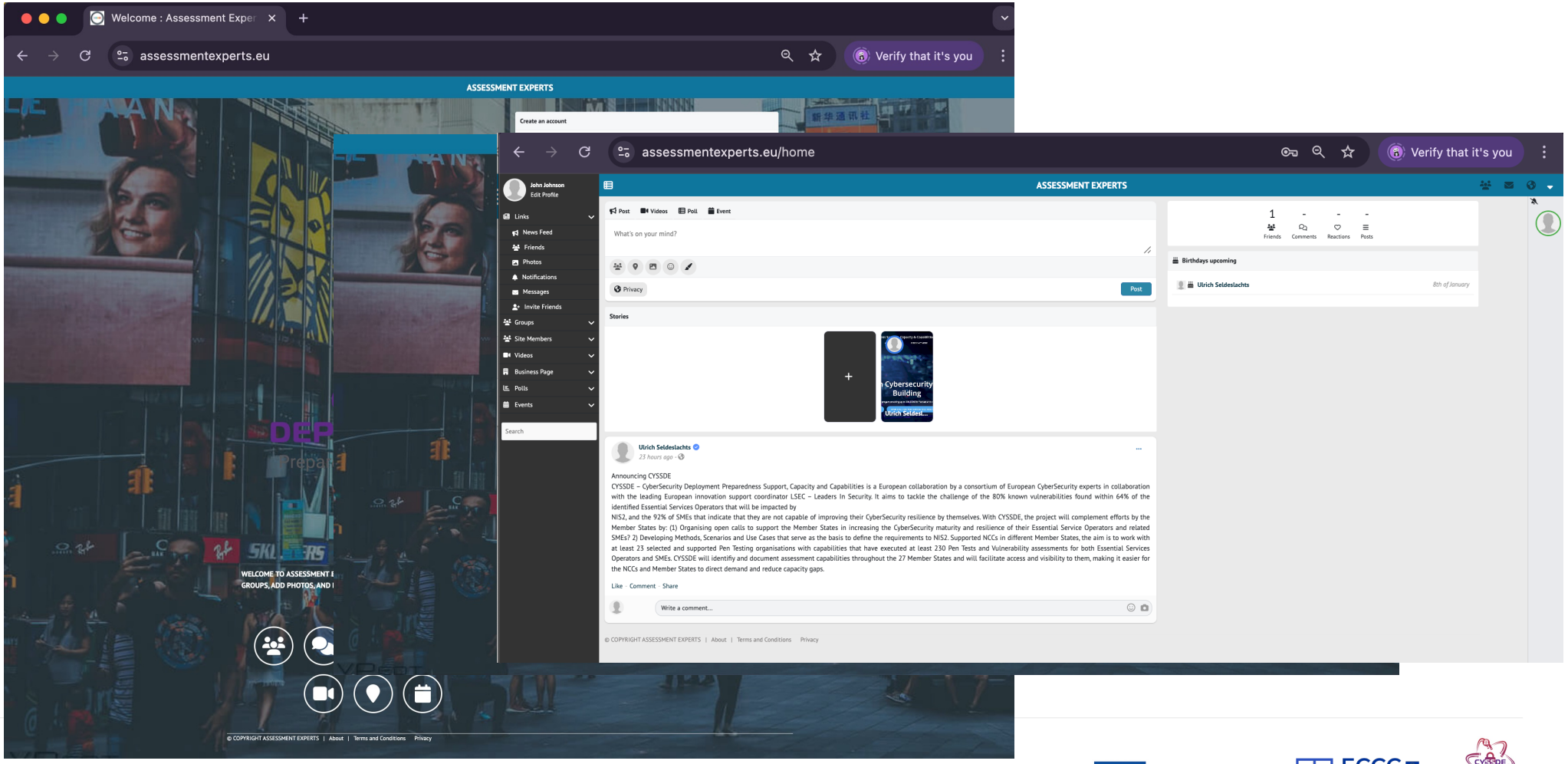
This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101158471

CYSSDE : NEXT STEPS

- Start OC3 application
- Sign up for CYSSDE activities – webinars, matchmakings - contribute
- Join the CYSSDE community of experts
- Talk to prospects / customers / partners / suppliers
- Publish Vulnerabilities and expand the Community

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101158471

SIGN UP TO : ASSESSMENTEXPERTS.EU



This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101158471

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
CYSSDE CYBERSECURITY DEPLOYMENT SUPPORT
Preparedness Support, Capacity & Capabilities


Cybersecurity Deployment Preparedness Support, Capacity & Capabilities
ABOUT
CAPACITY BUILDING
CYSSDE ACTIVITIES
CYSSDE
European Cybersecurity Capacity Building
Financial Support to Third Parties progam providing up to 200.000€ for Pentest and Vulnerability assessment activities.
ABOUT
OPEN CALL
LSEC
Got any questions? I'm happy to help.

www.cyssde.eu

Ulrich Seldeslachts

Mobile: +32 16 798585

Email: info@cyssde.eu

Co-funded by the European Union

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101158471