CybrOps Pitch Deck

Adrian Ifrim | CEO, Cristian Mocanu | CTO

Ideas for cybersecurity projects under DEP and HE calls

National Coordination Centre (NCC-PL)

September 2024

CybrOps

Cybersecurity

We give peace of mind for those who develop the future by securing their digital infrastructures. Our experience and skills allow allows us to uncover exposures *before* they are exploited.

We have the skill, patience, and desire to uncover hidden flaws that may otherwise remain dormant.

We help protect your data, critical infrastructures, and intellectual property from advanced security threats by testing your assumptions.

We are highly specialized in securing complex information systems supporting critical process for payment systems, healthcare, manufacturing, and cloud-based applications.

Our expertise supports businesses, governments, and organizations improve their cyber resilience.

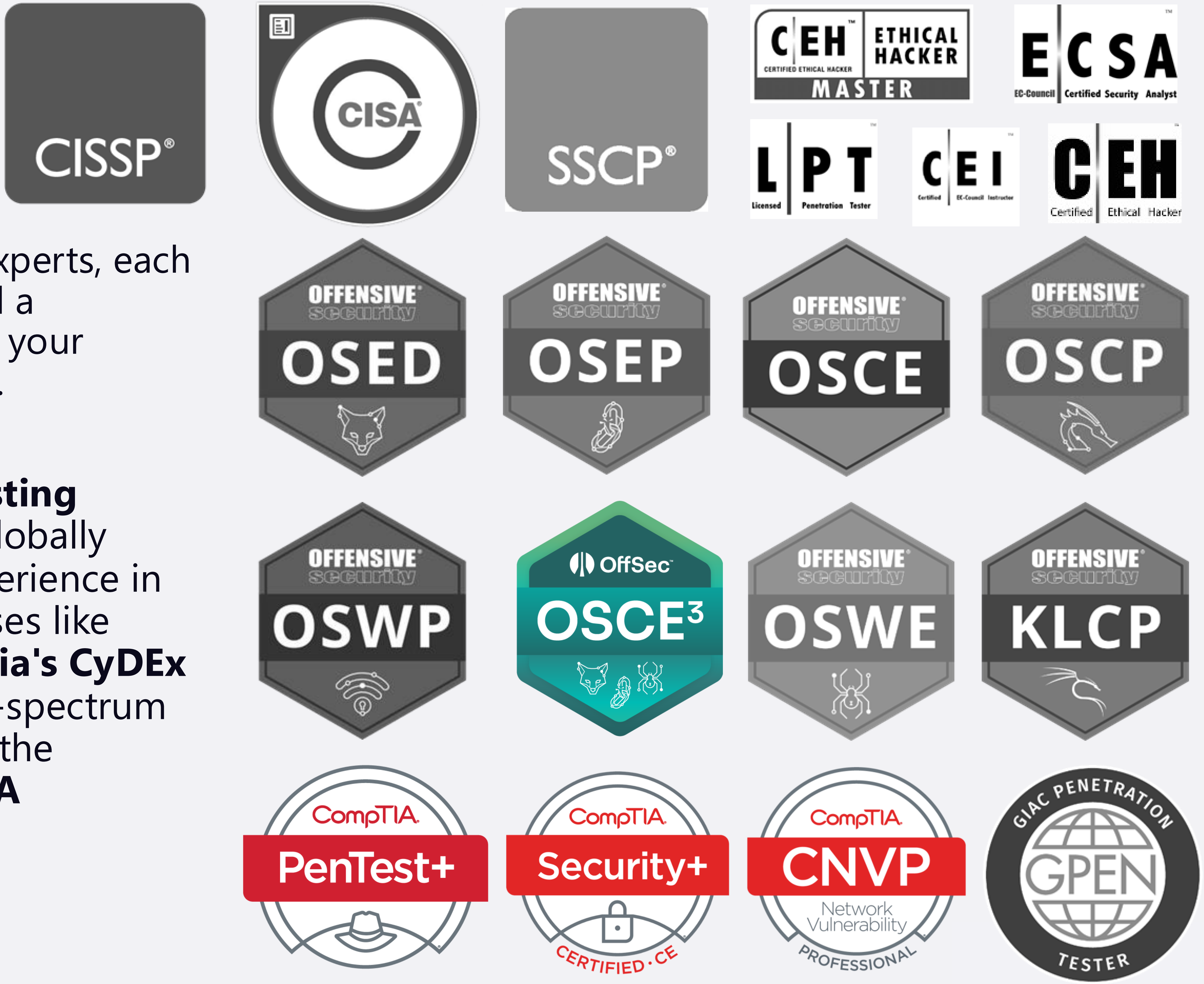
We are on a mission to transform the way organizations reach and maintain digital operational resilience by shifting the focus from effort to **performance**.

CybrOps

Our credentials

Our team is composed of dedicated experts, each possessing specialized knowledge and a commitment to applying their skills to your projects, ensuring outstanding service.

As a **NIS Audit and Penetration Testing accredited company** with over 25 globally acknowledged certifications and experience in high-profile cyber wargaming exercises like **NATO's Locked Shields** and **Romania's CyDEx** we are well-equipped to provide full-spectrum knowledge and confidently meeting the requirements of **TIBER-EU** and **DORA** guidelines.


CISSP®
CISA
SSCP®
C|EH ETHICAL HACKER MASTER
CERTIFIED ETHICAL HACKER
E|CSA EC-Council Certified Security Analyst
L|PT Licensed Penetration Tester
C|EI Certified EC-Council Instructor
C|EH Certified Ethical Hacker
OFFENSIVE security OSED
OFFENSIVE security OSEP
OFFENSIVE security OSCE
OFFENSIVE security OSCP
OFFENSIVE security OSWP
OffSec OSCE³
OFFENSIVE security OSWE
OFFENSIVE security KLCP
CompTIA PenTest+
CompTIA Security+ CERTIFIED · CE
CompTIA CNVP Network Vulnerability PROFESSIONAL
GIAC PENETRATION GPEN TESTER

Our experience

Central European Banks

Europe

Our team members, carried out penetration tests and adversarial simulation according to TIBER-EU Framework for three European Central Banks. Tests were carried on infrastructure and applications for interbank payments, as well as for invoicing and electronic archiving.

Penetration tests were carried out at both application and infrastructure (network) level, manual and automatic tests were carried out to detect vulnerabilities and exploit them to assess their potential impact. The testing activities focused on typical security errors and architecture flaws in authentication, authorization, cryptography, or session management subsystems.

The Red Teaming exercises had certain goals (access to SWIFT, Domain Admin privileges) that had to be achieved for the success of the simulation.

Public Sector

Romania

We have provided Cyber Security consulting and Penetration Testing services for two public institutions in Romania. Our engagement focused on thoroughly assessing the security of the Public Funds management application, aiming to identify vulnerabilities and enhance overall security measures.

Our team conducted comprehensive penetration tests, for the application and its underlying. We employed a combination of manual and automatic testing techniques to simulate real-world cyber-attacks and identify potential entry points. The assessment covered application security errors, architecture flaws, and external perimeter vulnerabilities.

As a result, we provided a detailed report with prioritized recommendations for remediation allowing our Clients to strengthened the security posture of the Public Funds management application.

NATO Locked Shields & Romania National Cyber Drill Exercises

Europe | Romania

The NATO Locked Shields exercises focus is on realistic scenarios, cutting-edge technologies and simulating the entire complexity of a massive cyber incident, including strategic decision-making, legal and communication aspects.

For two days more than 2000 participants from 32 nations engage in the protection of national IT systems and critical infrastructure under the pressure of a large-scale cyberattack at the annual live-fire cyber defense exercise Locked Shields.

CybrOps team members were invited by the Romania's Ministry of Defense to participate in 2019, 2021, 2022, 2023 and 2024 annual exercises as part of the offensive teams but also as Team Leaders.

Penetration Testing and Red Teaming for International Financial Institutions

FSI Clients

We were engaged in caring out complex scenario-based Threat Intelligence Ethical Red Teaming exercises for entities serving critical functions for the European financial ecosystem. We have carried out over 300 penetration projects and multiple red teaming engagements for over ten financial institutions. The scope was to assess the level of resilience of all three pillars: cyber, human and process. We have tested critical functions and and their supporting assets - financial applications available in both web and mobile versions (iOS, Android), components in banking infrastructure (banks/ ATMs/SWIFT) including Wi-Fi networks but also physical security systems.

The TIBER-EU based engagements were focused on simulating Advanced Persistent Threats tactics, techniques and procedures with the objectives related to client Crown Jewels (access to high-value payments systems, reporting systems, client/employee data, IP data). The penetration tests were aimed at identifying vulnerabilities in the security configurations of the external perimeter and approaching the tests from both black-box and grey-box perspective.

CybrOps

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER
Preparedness Support and Mutual Assistance, Targeting Larger Industrial Operations and Installations

Support for testing for potential vulnerabilities:

- Development of penetration testing scenarios. The proposed scenarios may cover Networks, Applications, Virtualisation solutions, Cloud solutions, Industrial Control systems, and IoT.
- Support for conducting testing of essential entities operating critical infrastructure for potential vulnerabilities.
- Support the deployment of **digital tools** and **infrastructures supporting the execution of testing scenarios** and for conducting exercises such as the **development of standardized cyber-ranges or other testing facilities**, able to mimic features of critical sectors (e.g., energy sector, transport sector etc.) to facilitate the execution of cyber-exercises, in particular within cross-border scenarios where relevant.
- Evaluation and/or testing of MS cybersecurity capabilities (including capabilities to prevent, detect and respond to incidents).
- Consulting services, providing recommendations on how to improve infrastructure security and capabilities.

Support for threat assessment and risk assessment:

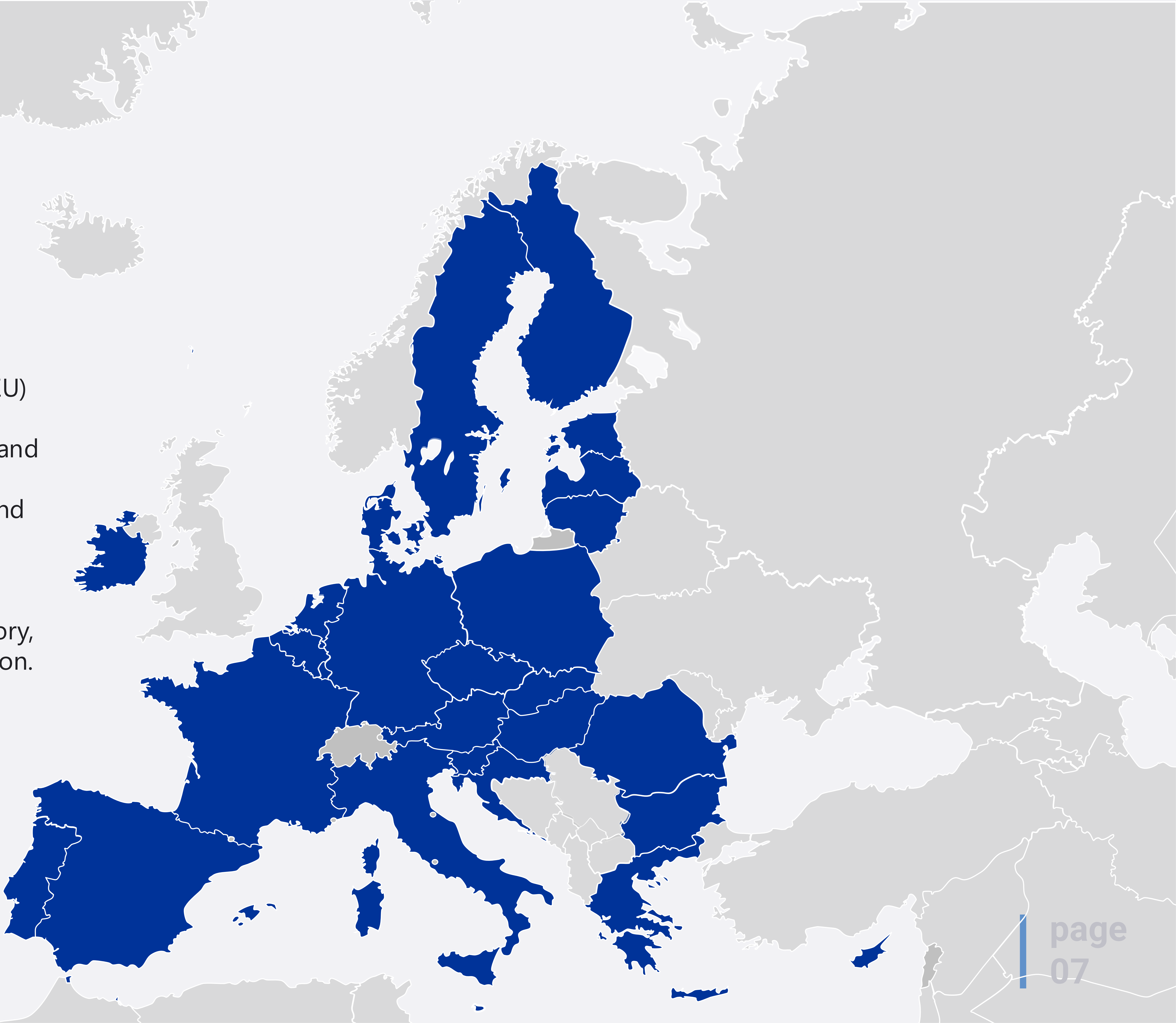
- Threat Assessment process implementation and life cycle
- Customised risk scenarios analysis.

Risk monitoring service:

- Specific continuous risk monitoring such as attack surface monitoring, risk monitoring of assets and vulnerabilities.

CybrOps and it's team of **accredited NIS auditors** can provide these services for entities (including SMEs and start-ups) in sectors indicated as critical infrastructure sectors in **NIS** Directive such as energy, transport and banking, and entities in other relevant sectors.

CybrOps
Partners needed



Targeted stakeholders
This topic targets in particular industrial players, national cybersecurity authorities, national cybersecurity competence centres, National Coordination Centres (as defined in Regulation (EU) 2021/887), private entities and any other relevant stakeholders with the capacity to aggregate demand from end beneficiaries, to launch tenders for procurement in the cybersecurity market space and to run downstream calls for allocating Financial Support to Third Parties.

Submissions from consortia, despite not mandatory, will positively contribute to the impact of the action.

CybrOps

CybrOps
Our vision

Operators of critical infrastructure providing essential services, have at times multiple new regulations coming out in short period of time. These must be promptly ingested and enforced.

CybrOps vision has a long-term strategy behind it. We're not only planning on building a more cyber resilient Europe, but aim to cause a major paradigm shift on how cybersecurity is tackled.

The ultimate objective of our efforts is for those with management roles in cyber security to make informed decision, based on relevant data.

The team
Experienced professionals

Adrian Ifrim
CEO | Co-founder

17 years in Cyber Security
IT & Business expertise
Focus on partnerships
MBA, MSc Cyber Security

Started dismantling computers and networks at a very early age.
Curios by design.

Cristian Mocanu
CTO | Co-founder

15 years in Cyber Security
Board member Certification Bodies
Focus on team development
MSc Cyber Security

More than 15 years of deep technical experience in tactical network exploitation for public and private institutions across Europe

Paul Irofti
Chief Research Officer

Associate professor at Dep. of Computer Science of the Faculty of Mathematics and Computer Science, University of Bucharest
PhD in Systems Engineering
Expert in anomaly detection, signal processing, numerical algorithms & optimization

Deloitte. vodafone ING UniCredit cegeka ANCOM

Central Banks	Private Banks	Insurance	Telecom	Healthcare
Media	Public Institutions	Energy	Automotive	Utilities
	30000+ hours	1000+ projects	32+ certifications	

Contact
Working together

Adrian Ifrim
CEO | Co-founder

17 years in Cyber Security
IT & Business expertise
Focus on partnerships
MBA, MSc Cyber Security

Started dismantling computers and networks at a very early age.
Curios by design.

Cristian Mocanu
CTO | Co-founder

15 years in Cyber Security
Board member Certification Bodies
Focus on team development
MSc Cyber Security

More than 15 years of deep technical experience in tactical network exploitation for public and private institutions across Europe

Q&A

We are on a mission to transform the way organizations reach and maintain digital operational resilience. We provide capabilities that allow organizations to shift focus from effort to performance and capabilities to measure success.

We are committed to providing thorough and expert-level testing services. We never compromise on the quality of our testing.

CybrOps

Bucharest, Romania
e. office@cybrops.io
w. https://cybrops.io
t. +40 775 250 124