



Digital Europe Programme Cybersecurity Pitch ideas

Chaired by Roberto Cascella
ECCO Project Coordinator

ECCC Infoday Brussels – 09th July 2024

This deliverable was prepared for DG CNECT by the ECCO Consortium under contract^o CNECT/2022/OP/0033 and is the European Commission's property. The views expressed in this document are purely those of the authors and may not, in any circumstances, be interpreted as stating an official position of the European Commission. The European Commission does not guarantee the accuracy of the information included in this document, nor does it accept any responsibility for any use thereof.

Reference herein to any specific products, specifications, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favouring by the European Commission.

All care has been taken by the authors to ensure that they have obtained, where necessary, permission to use any parts of manuscripts including illustrations, maps, and graphs, on which intellectual property rights already exist from the titular holder(s) of such rights or from her/his or their legal representative.

© European Union, 2024

Session Agenda

Topic: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-CYBERSEC-02 - Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies (2024)

#	ORGANISATION	PRESENTER
1	CEFRIEL	Enrico Frumento
2	Binary Confidence	Peter Hudak
3	EMAG	Dariusz Rogowski
4	LSEC - Leaders In Security	Ulrich Seldeslachts
5	Matrix Internet	Jeff Sheridan

DIGITAL-ECCC-2024-DEPLOY- CYBER-07-CYBERSEC-02

Enrico Frumento
Cybersecurity Research Lead

enrico.frumento@cefriel.com
+39 0223954259

Cefriel - Politecnico di Milano
www.cefriel.com
Viale Sarca 226 – 20126 Milano - IT

[in https://www.linkedin.com/in/enricofrumento/](https://www.linkedin.com/in/enricofrumento/)

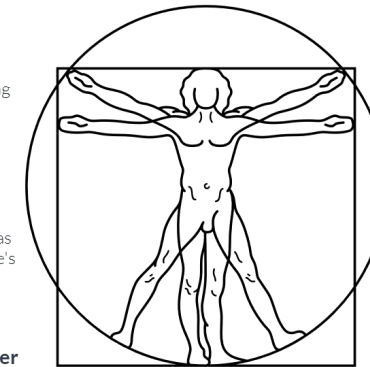
ADVANCED DIGITAL SKILLS AND TRAINING AS A CYBER RISK REDUCTION

- Our research is dedicated to rethinking cybersecurity from the vital perspective of the human element. → see [recently published whitepaper](#)
- Training/learning of employees and contractors is a critical step in **increasing the security of the human element**.
- The challenge is to **create impactful, long-lasting learning paths**.
- **Training is a cyber risk reduction method**
- **Improve the resilience of the human element**,
- This area of research aims to **transform training as a defence instrument fully**.

CALLS:

- We search for participation in a consortium
- Cefriel is a not-for-profit RTO and a SME

- 1. Special Education Tracks**
Special education tracks are built around the organisation's culture to communicate the emergencies and maximise the impact of training (e.g., People Analytics)
- 2. Vulnerability Assessment/Penetration Testing of the human element**
Vulnerability Assessment of the human element, such as phishing campaigns or simulated attacks, to test people's resilience, employees of IT staff (e.g., SDVA, FSVA).
- 3. Training as a defence instrument to reduce cyber risk**
Training pathways aligned with the European Competency Framework (e-CF) or minimum skill set but proportionate to the business role and assets under management



- 7. Integrated estimation of the cyber risk, including IT, OT and Human Risk**
Integration of human, operational technology, and information technology risk models (e.g., human risk management, integrated risk models)
- 6. AI for mitigation of the human-related threats**
The use of anti-deception systems and systems to assist people in suggesting correct behaviours and avoiding risks (e.g., mind firewalls, Human Sensor Networks).
- 5. Simulation of human-related threats and attack patterns**
Simulating in cyber ranges, for example, even human attacks, is necessary. For instance, including the human aspects of an attack alongside technology (e.g., gold teams, dedicated tabletop exercises)

Source: E. Frumento, "Full Spectrum Vulnerability Assessment (FSVA) in Cefriel", Medium [Online] Available at: <https://enrico-frumento.medium.com/full-spectrum-vulnerability-assessment-fsva-in-cefriel-f14cf4d80313>



Securea – method and tool to help with compliance

Peter Hudák, 9.7.2024

peter.hudak@binconf.com

We believe that everybody has the right to first-class cybersecurity.

binary
CONFIDENCE



Securea – method and tool

Real Life Challenges

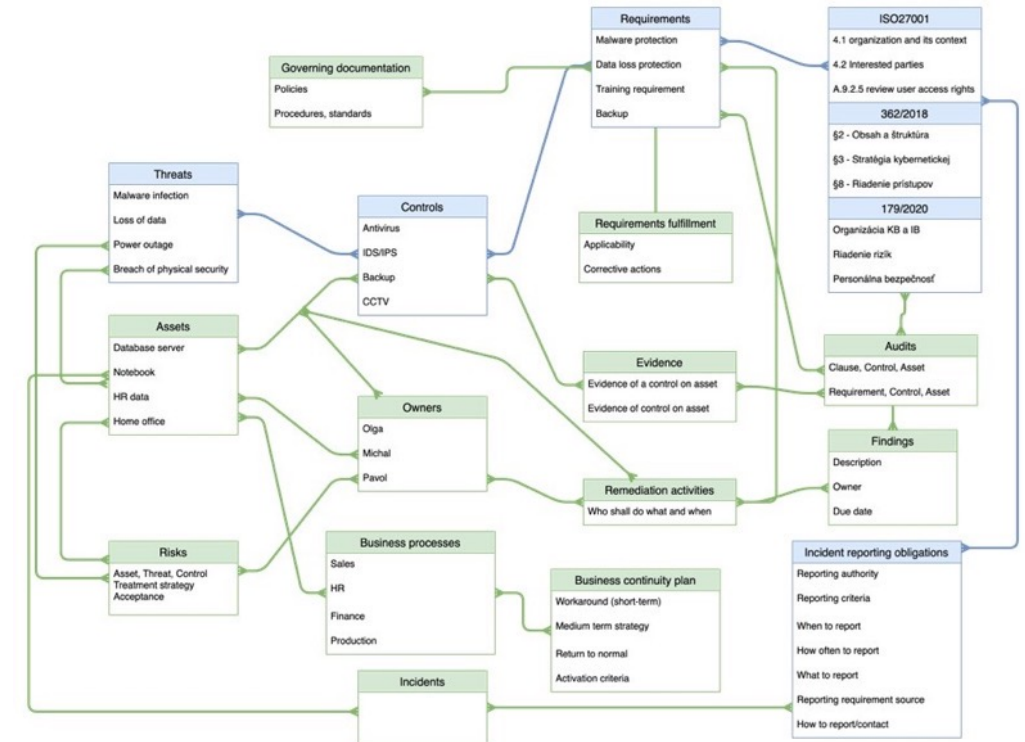
- Compliance with multiple regulatory frameworks, industry standards, international standards, client contracts (NIS2, DORA, ISO27001, TISAX, PCI-DSS, CIS, ...),
- Same requirements – different language – remixes,
- Spreadsheets with static data,
- Incident reporting – multiple classification schemes, different reporting requirements (content, frequency),
- Documented information - mapping and compliance,
- Mutual trust, customer-vendor relationships, audits,
- Lack of resources.

Securea – method and tool



The Securea Solution

- GRC tool with a single set of atomic requirements derived from implemented standards and mapped back to original standards and regulations
- Support for risk assessment and security posture directly mapped to atomic requirements, enabling reporting according to any processed regulation
- Support for incident classification and handling – incident reporting requirements derived from regulations or contractual arrangements
- Support for BCM, audit planning, documented information management
- Possible platform for exchanging partial results of risk assessments and compliance assessments among companies, auditors
- Pre-filled templates to jumpstart analysis





Current development status

- Pre-alpha proof of concept software product already available with basic functionality
- Template model with threats, controls, requirements, regulations and their relationships already developed and constantly enhanced

Need help with AI

- AI to analyze documented information and mapping to atomic requirements
- AI to fill in customer-provided questionnaires (everyone doing vendor assessments)

Project proposal: *Cybersecurity Development and Evaluation Reference Materials (CDERM)*

- Dariusz Rogowski, PhD, dariusz.rogowski@emag.lukasiewicz.gov.pl
- Łukasiewicz Research Network – Institute of Innovative Technologies EMAG, Katowice, POLAND
 - Accredited Laboratory and Certification Body
ISO/IEC 15408 (Common Criteria), IEC 62443-4-2 (Industrial components security)
- Consortium status: **needed**
- Anticipated role in the project: **Work Package leader**
- Topic:
 - DIGITAL-ECCC-2024-DEPLOY-CYBER-07-CYBERSEC-02 - Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies (2024)

Problem:

How to facilitate the security certification of products?

For vendors and consumers

- Building evaluation and certification awareness
- Preparedness for evaluation and certification processes
- “Security by design” to improve security functionality of products
- “Security by default” to deploy and use products securely by consumers

For labs and evaluators

- Recommended tools and knowledge needed for testing security functions
- More certifications and evaluations to build technical competencies in the field

For accreditation bodies and auditors

- Interlaboratory comparisons and proficiency testing
- Accreditation of CABs and determining the scope of accreditation

Solution:

Reference materials (RMs) to achieve security requirements on a given evaluation assurance (EAL) and security level (SL)

- **RMs for critical products with digital elements**
IACS, PLC, DCS, SCADA (Annex III to CRA), and IIoT (Annex I to NIS 2)
- **RMs for vendors:** a minimum set of documentation and security functions requirements (*parameters, configuration, technologies, best practices*) needed to gain conformance with a specific EAL and SL
- **RMs for labs:** a minimum set of knowledge, skills and tools requirements needed to run security evaluation, functional testing, vulnerability analysis and penetration testing for a specific EAL and SL
- **RMs for accreditation bodies:** a minimum set of activities and materials for interlaboratory comparisons and proficiency testing
- **Results:** strengthening capabilities to achieve compliance
 - **CSA** – Cybersecurity Act – assurance levels high, substantial, basic
 - **NIS 2** – Network and Information Security Directive
 - **EUCC** – The Common Criteria – based certification scheme, Evaluation Assurance Levels (EAL)
 - **ICCF** - IACS Cybersecurity Certification Framework, Security Levels (SL) for industrial components
 - **CRA** – Cyber Resilience Act on cybersecurity requirements for products with digital elements

Setting up the project

- Proposed coordinator/leader – **needed**
- Łukasiewicz – EMAG will provide:
 - Experts in the cybersecurity certification field – labs from Spain, Hungary
 - Collaboration, communication, awareness-raising activities, training
 - Support actions for further advances of cybersecurity certification
 - Support actions for industrial and IT stakeholders in the scope of IEC 62443, Common Criteria
 - Conformance gap analysis – assessment of the maturity of products and development environments
- Looking for partners:
 - Vendors – to validate reference materials in pilot evaluations
 - Experts supporting the implementation of NIS 2, CRA
 - ITSEFs, CBs, national accreditation bodies
 - Others interested in the topic scope



DIGITAL-ECCC-2024-DEPLOY-CYBER-07-CYBERSEC-02

Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies (2024)

LSEC CyberSecurity Innovations

Digital Security Catalyst



This project has been funded with support from the european commission 101128103 - CYSSME



Ulrich Seldeslachts,
July 8th 2024

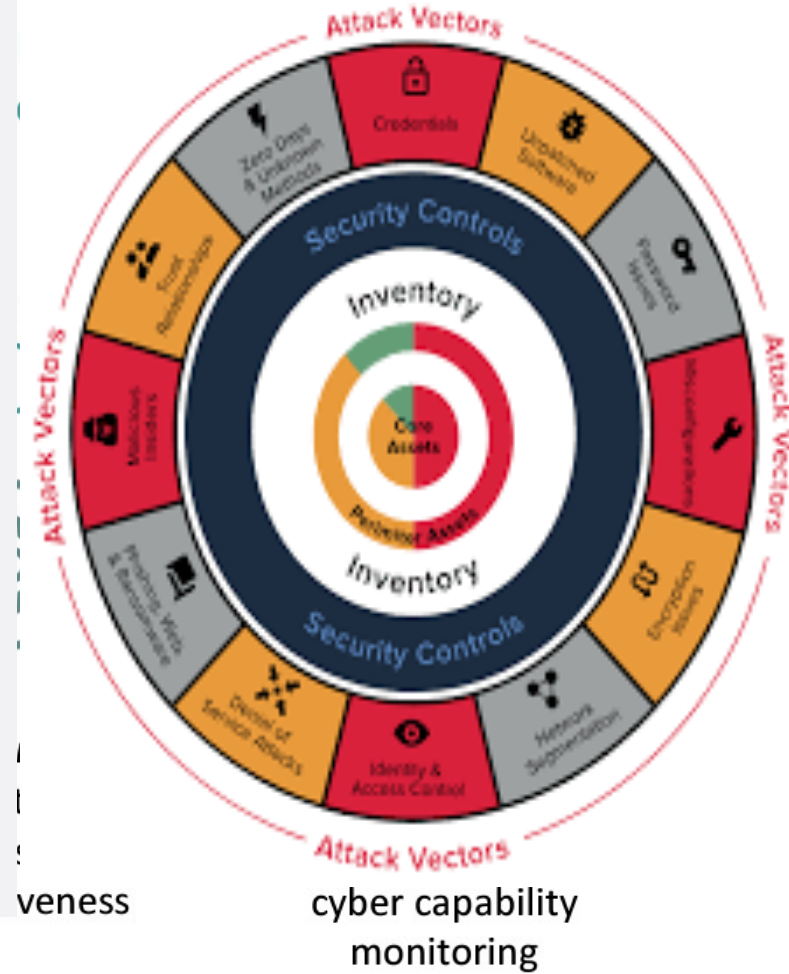
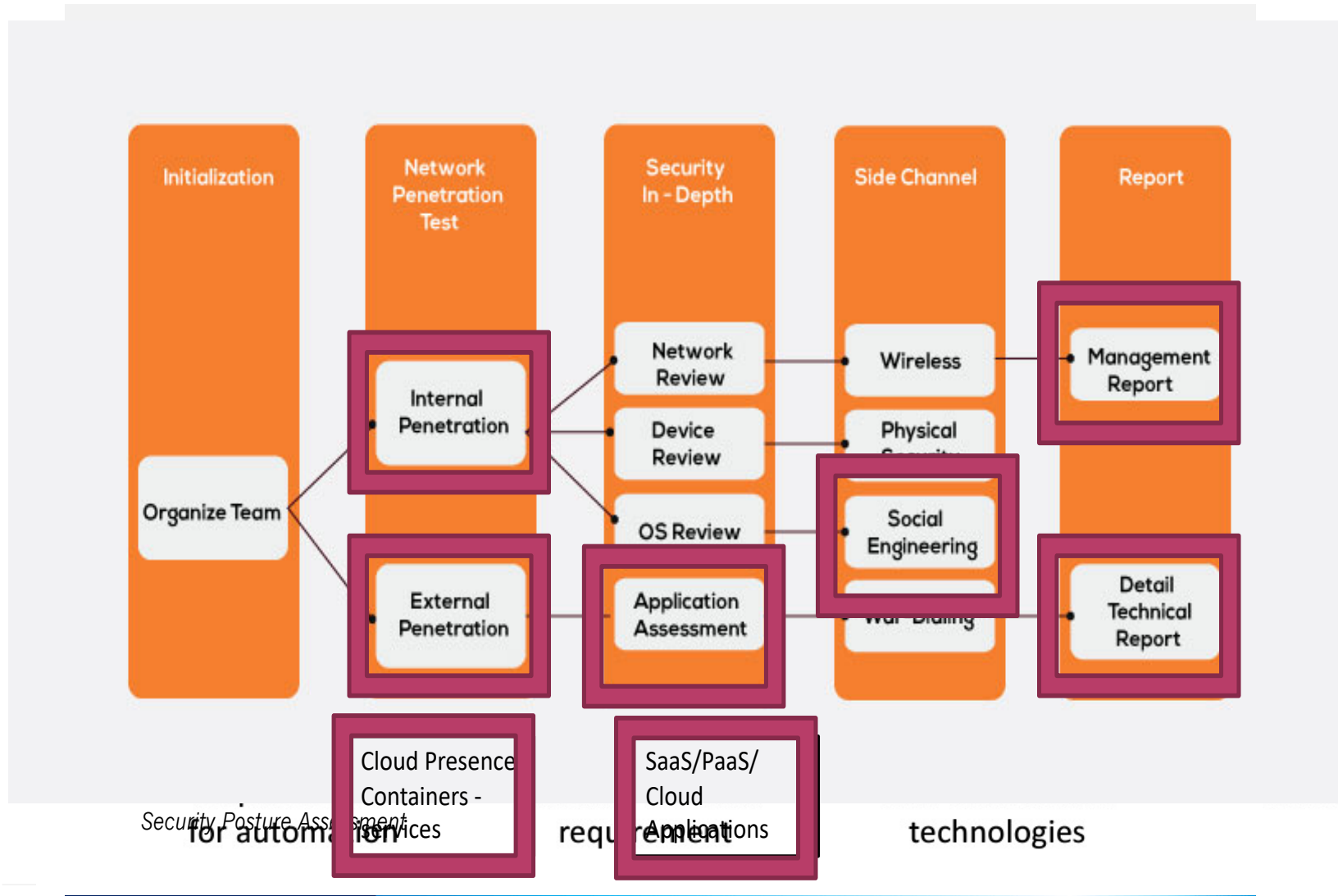


EXECUTIVE SUMMARY

- Preemptivity
 - Empowering integration of incident reporting from responder
 - Integrating controls from NIS2 – also from automated assessments – that lead to NIS2 compliance
 - Facilitating higher level dashboards for Essential and Critical Operators
 - Integrating secure dependency tracking mechanisms to track vulnerabilities and report back
 - Enhancing and securing information exchange
 - Operating in classified information
- Consortium:
 - Partners expertise in NIS2 compliance assessments and automation, in SBOM & in higher level of integrations
 - Looking for additional expertise and tooling
 - Looking for additional expertise in certification
 - Looking for Law Enforcement partners and Authorities for advise and validate



AUTOMATED (POSTURE) ASSESSMENTS (APAX)



NOT THE END

More information, slides and follow-up

www.lsec.eu

www.digitalsecuritycatalyst.com



AGENTSCHAP
INNOVEREN &
ONDERNEMEN



Q or C

Ulrich Seldeslachts

ulrich@lsec.eu

+32 475 71 3602





Transforming Europe Digitally

Matrix is a leading digital agency in Europe, with an empathetic culture, an international mindset and big ambitions.

We are a large, professional team bursting with ideas that help submissions to succeed.

With a strong track record of digital success and 4 in-house teams headed by experienced leaders, Matrix creates strong digital strategies. We believe that our vibrant, capable team has the perfect balance of youth, experience, energy and empathy.

We have leading roles on some of the most prestigious and ambitious digital projects in the EU.

www.matrixinternet.eu

info@matrixinternet.eu

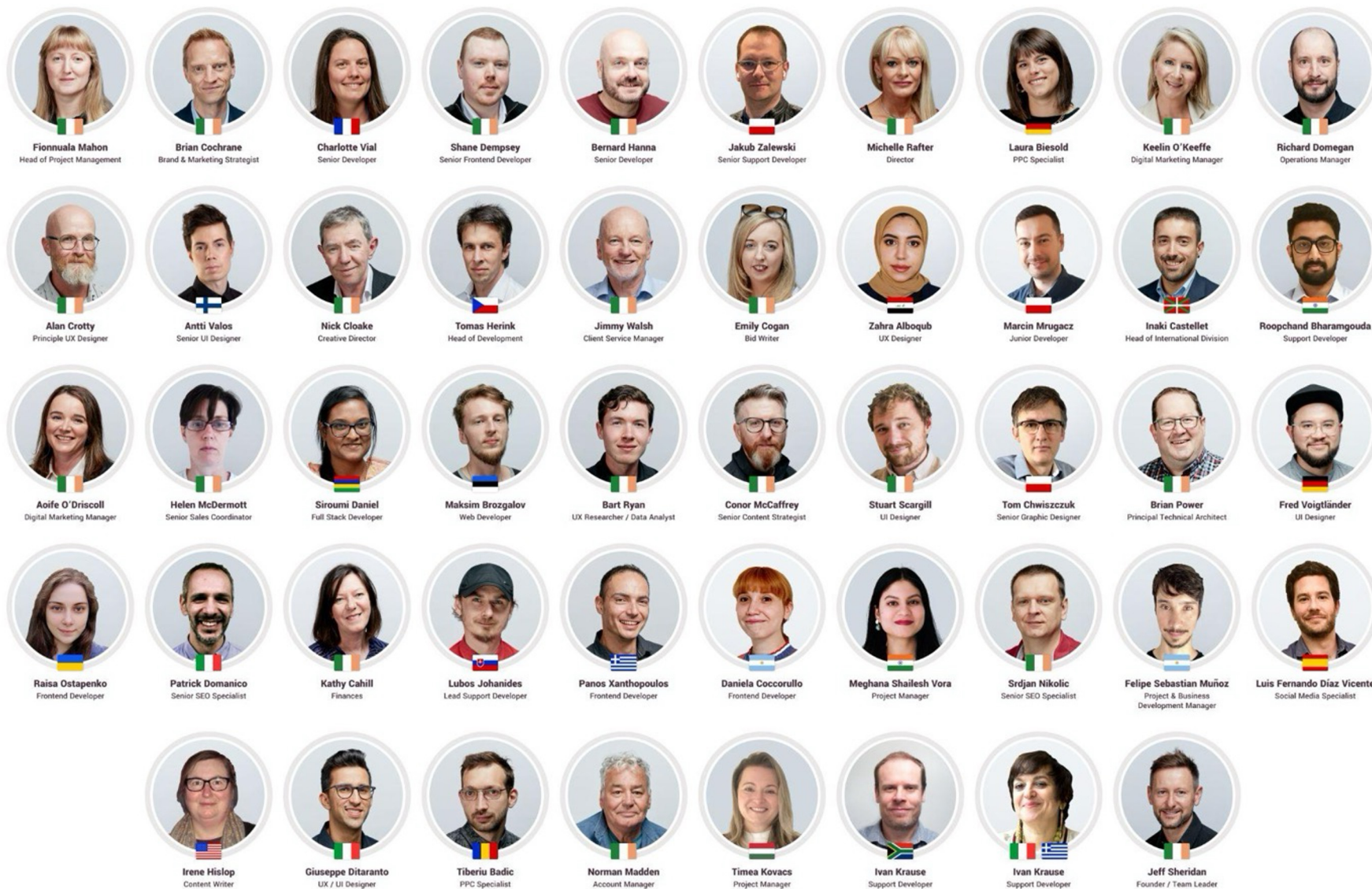




Our People - an effervescent team

We are a diverse, inclusive company with a global outlook and a 48-strong team hailing from 22 countries, with offices in Dublin and Brussels.

From idea to submission to delivery and impact, we bring colour and impact to every project.





Our Partners

We are partnered with over 250 organisations.

Our Projects

Project transforming Europe digitally.



DIGITAL-ECCC-2024-DEPLOY-CYBER-07-CYBERSEC-02 - Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies

We are building an ambitious submission to effect powerful and effective rollout, through high profile partners, new communities, industry engagement, established network leverage and cybersecurity credibility.

Our Consortium is building nicely with :

- **Leveraging current cyber projects / movements**
- **Europe wide digital collective organisations**
- **Europe-wide industry representatives**
- **Big-tech industry leaders**
- **Global training company**
- **Several national cyber clusters across Europe**

We are looking for additional expertise in :

- **Cyber legislation**
- **Large networks to leverage**
- **Strategic rollout**
- **Legislative implementation**

Session Agenda

Topic: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-KEYTECH - Development and Deployment of Advanced Key Technologies

#	ORGANISATION	PRESENTER
1	HIBATECH	Hinde Baddou
2	CEFRIEL	Enrico Frumento
3	LSEC - Leaders In Security	Ulrich Seldeslachts
4	South-Eastern Finland University of Applied Sciences – Xamk	Marie Skavø-Sinisalo
5	Resistine	Petr Chmelar

HIBATECH

Combatting phishing with AI

Hindebaddou@gmail.com / +352661949405

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-KEYTECH

PROBLEM STATEMENT

- Smishing, or SMS phishing, is a type of cyberattack where malicious actors use text messages to deceive recipients into revealing personal information or clicking on harmful links.
- Statistics: Over 56% of cyberattacks involve smishing, affecting millions of users and causing billions in losses annually.
- Impact: Victims suffer financial loss, identity theft, and compromised personal data.

Hindebaddou@gmail.com / +352661949405

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-KEYTECH

SOLUTION

Our innovative AI-based tool designed to detect and prevent smishing attacks.

Core Features:

Real-time SMS analysis
AI-driven detection algorithms
Instant user alerts and reporting
Privacy and data protection compliance

Hindebaddou@gmail.com / +352661949405

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-KEYTECH

CALL TO ACTION

- Banks
- Telecom Operator
- Financial Institution
- European and National Public Authorities

Hindebaddou@gmail.com / +352661949405

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-KEYTECH

DIGITAL-ECCC-2024-DEPLOY- CYBER-07-KEYTECH

Enrico Frumento
Cybersecurity Research Lead

enrico.frumento@cefriel.com
+39 0223954259

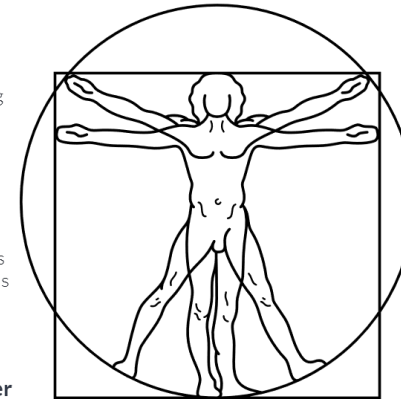
Cefriel - Politecnico di Milano
www.cefriel.com
Viale Sarca 226 – 20126 Milano - IT

[in https://www.linkedin.com/in/enricofrumento/](https://www.linkedin.com/in/enricofrumento/)

IMPORTANCE OF THE HUMAN ELEMENT

- Our research is dedicated to rethinking cybersecurity from the vital perspective of the human element. → see [recently published whitepaper](#)
- Full Spectrum Vulnerability Assessment (FSVA)
- A simulation of a "complete" attack, albeit simulated, acting in the ways and methods of real computer attacks, aims to test the "responsiveness" of the IT security team.
- What an FSVA stimulates is not the response to a specific problem but the ability to adapt and think independently when the worst happens, directly to the humans, skipping the technological layers.

- 1. Special Education Tracks**
Special education tracks are built around the organisation's culture to communicate the emergencies and maximise the impact of training (e.g., People Analytics)
- 2. Vulnerability Assessment/Penetration Testing of the human element**
Vulnerability Assessment of the human element, such as phishing campaigns or simulated attacks, to test people's resilience, employees of IT staff (e.g., SDVA, FSVA).
- 3. Training as a defence instrument to reduce cyber risk**
Training pathways aligned with the European Competency Framework (e-CF) or minimum skill set but proportionate to the business role and assets under management



- 7. Integrated estimation of the cyber risk, including IT, OT and Human Risk**
Integration of human, operational technology, and information technology risk models (e.g., human risk management, integrated risk models)
- 6. AI for mitigation of the human-related threats**
The use of anti-deception systems and systems to assist people in suggesting correct behaviours and avoiding risks (e.g., mind firewalls, Human Sensor Networks).
- 5. Simulation of human-related threats and attack patterns**
Simulating in cyber ranges, for example, even human attacks, is necessary. For instance, including the human aspects of an attack alongside technology (e.g., gold teams, dedicated tabletop exercises)

CALLS

- We search for participation in a consortium
- Cefriel is a not-for-profit RTO and a SME

Source: E. Frumento, "Full Spectrum Vulnerability Assessment (FSVA) in Cefriel", Medium [Online] Available at: <https://enrico-frumento.medium.com/full-spectrum-vulnerability-assessment-fsva-in-cefriel-f14cf4d80313>



DIGITAL-ECCC-2024-DEPLOY-CYBER-07-KEYTECH

Development and Deployment of Advanced Key Technologies

LSEC CyberSecurity Innovations

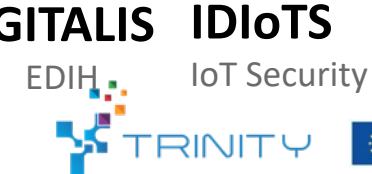
Digital Security Catalyst



This project has been funded with support from the European Commission
101128103 - CYSSME



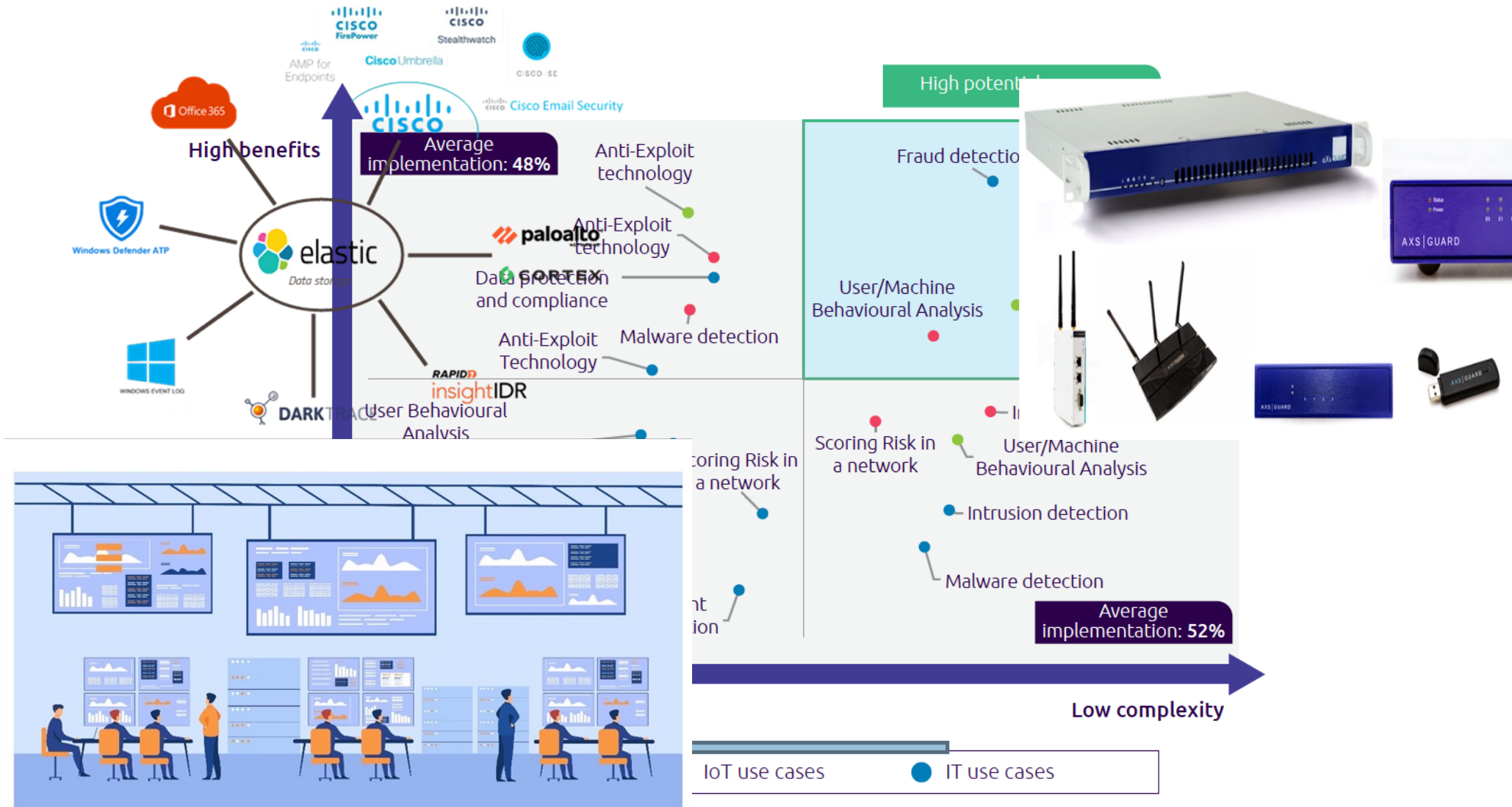
Ulrich Seldeslachts,
July 8th 2024



EXECUTIVE SUMMARY

- CTAI
 - Faster access to LLM by facilitating access to GenAI
 - Building on top of expertise of ML / Advanced Analytics to speed up impact capabilities
 - Assessing new AI-capabilities in Cybersecurity
 - Digital Twin developments
 - Real-time analysis dashboarding and proactive instrumentation
 - Automating Data Impact and AI impact
- Consortium:
 - Partners expertise in CTI, SOC, AI, AI for Cybersecurity and commercial tooling and deployment
 - Looking for additional expertise in CTI, SOC analysis and advanced AI models
 - Looking for additional Malware Analysis expertise and APT analysis intelligence
 - Looking for automated incident investigation tooling to integrate

CSAI



SOC OPERATIONAL EXCELLENCE

OPERATIONAL COST REDUX

NOT THE END

More information, slides and follow-up

www.lsec.eu

www.digitalsecuritycatalyst.com



AGENTSCHAP
INNOVEREN &
ONDERNEMEN



Q or C

Ulrich Seldeslachts

ulrich@lsec.eu

+32 475 71 3602



South-Eastern Finland University of Applied Sciences, Xamk



12 000 degree students
34 000 open university students

223

Projects,
31 international



1000 employees



Cybersecurity is
our DIH spearhead



4 campuses



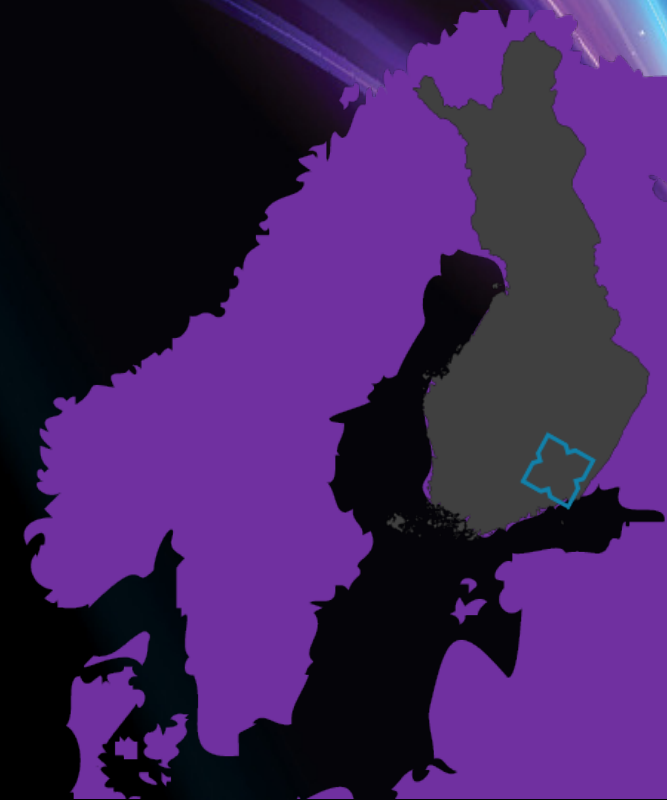
50 Bachelor's Degree
36 Masters's Degree programmes



Turnover 100 MEUR
RDI 32.1 MEUR

We have no partners yet and are looking for other 2-4 Universities (of Applied Sciences) for example from Nordics/ Baltics and/or Poland. We can be also a plug-in another project.

Interest in Ukraine related projects.



Marie Skavø-Sinisalo, Project Manager
marie.skavo-sinisalo@xamk.fi
+358 45 11 33787
Kaakkois-Suomen Ammattikorkeakoulu Oy
www.xamk.fi
Business ID 2472908-2
VAT number FI24729082



REGIONAL
COUNCIL
KYMEN
LAAKSO



Co-funded by
the European Union

Cyber-
resilient
Kymen-
laakso

Free & open (source) SOC tools

Project Focus: Deployment of free and open solutions in European SMEs for enhanced cybersecurity by implementing cost-efficient SOC tools.

Suggested examples of used **key technologies:** SecurityOnion, Opensearch, ELK-stack etc.

For: Critical infrastructure SMEs & their immediate suppliers in water utilities, energy and healthcare.

Why: major cybersecurity challenges for NIS2 SMEs, is the lack of low-budget solutions as well as experts / expertise.

Overview of the objectives and our proposal

Alignment with Program Objectives:

1. State-of-the-Art Technologies Deployment

- Utilization and implementation of open technologies for automated threat detection and log analysis.

2. Breakthroughs in Digital Technologies

- Leveraging simulated environments and scenarios to generate performance data for further development possibilities, such as training AI models.
- Utilizing Big Data Analytics for large-scale data processing and real-time insights.

3. Improvement of Cybersecurity Capabilities

- Enhancing SMEs' detection and prevention capabilities through advanced tools and techniques.
- Scaling cybersecurity solutions to meet the needs of complex environments.

4. Innovative Data Processing and Analysis

- Automating real-time pattern recognition and vulnerability scanning.
- Enabling efficient data analysis and actionable insights for cybersecurity professionals.

5. Strengthening Cyber Threat Information (CTI)

- Improving SMEs' abilities to inform authorities on emerging cyber threats by giving improved detection and reporting capabilities.

Conclusion:

Our proposal aligns closely with the Call for proposal's objectives by leveraging free and open technologies to empower European SMEs with limited resources with robust cybersecurity capabilities. By deploying these solutions, we aim to enhance detection, response, and overall cybersecurity resilience, contributing to a safer digital environment of our European society.

Cybertraining Hospital

Concept is being developed in a current, running CyberCare Kymi project. A possible plug-in into another project.

Mission: To build on top of existing training hospitals a new layer: cybercrises training environment for health care professionals.

Goal:

- Fortify the healthcare sector's cybersecurity, shortening incident response times, safeguarding lives and preserving patient safety.
- Changing healthcare training for SMEs and health sector.

Plan:

- Investment part: hospital equipment and tech, planning and building virtual simulation and attack platform.
- Planning and carrying out real-life cyber incident training for healthcare workers.
- Simulate cyber threats and breaches in a safe environment.
- Specialized programs and workshops for recognizing, preventing and responding to cyber incidence.
- Prepare a report on the results of the training results achieved during the project and recommended best-practices.



Resistine

AI CyberSecurity Assistant
so that SOC analysts have a meaning of life

Petr Chmelar

@chmelarp

petr@resistine.com

+420 602 54 2468

Berlin DE – Brno CZ

www.resistine.com

Cybersecurity Risk SoC VPN
 Detection and Response DDoS Firewall
 DLP IDS EDR
 Headache
 Authentication

Enterprise-level cybersecurity today?

Too much data*
 Lack of skilled

3.4M people* tired

Insurance Router
 Windows Antivirus NIST
 Security Information XDR NIS2
 Protect
 BackUp Zero Trust
 Ransomware Endpoint NDR Update
 Threat Intelligence Password Management
 ISO 27000 SIEM
 eats Analysts

Low Training*



*Source: ISC2 - 2023 Cyberthreat Defense Report

Real Difference

based on 20 years of cyber-research at multiple EU projects, NIST and NATO CCDCOE


The Open Source AI Cyber-Assistant XDR


- detects vulnerabilities and advanced persistent threats
- suggests solutions and
- communicates with everyone to provide training and

to improve cybersecurity according to NIS2
affordable and easy to use

Project idea: **To learn from each SOC click!**
so that SOC analysts have a meaning of life




←  Resistine ▾  

 **Assistant** 3 min

Hey, there is some malware on Mike's computer.

It doesn't have an antivirus.

I can install it and restart the computer... 



Do it!





Resistine

looking for partnerships

to make the world **safer and more free**

Berlin DE – Brno CZ

www.resistine.com

Session Agenda

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

#	ORGANISATION	PRESENTER
1	iThing AB	Conny Broberg
2	APWG.EU	Adriana Freitas
3	LSEC - Leaders In Security	Ulrich Seldeslachts



PROJECT PITCH @ ECC 2024

CTO CONNY BROBERG

ITHING AB SWEDEN

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER - PREPAREDNESS SUPPORT
AND MUTUAL ASSISTANCE, TARGETING LARGER INDUSTRIAL OPERATIONS AND
INSTALLATIONS

COLLABORATIVE CYBERSECURITY

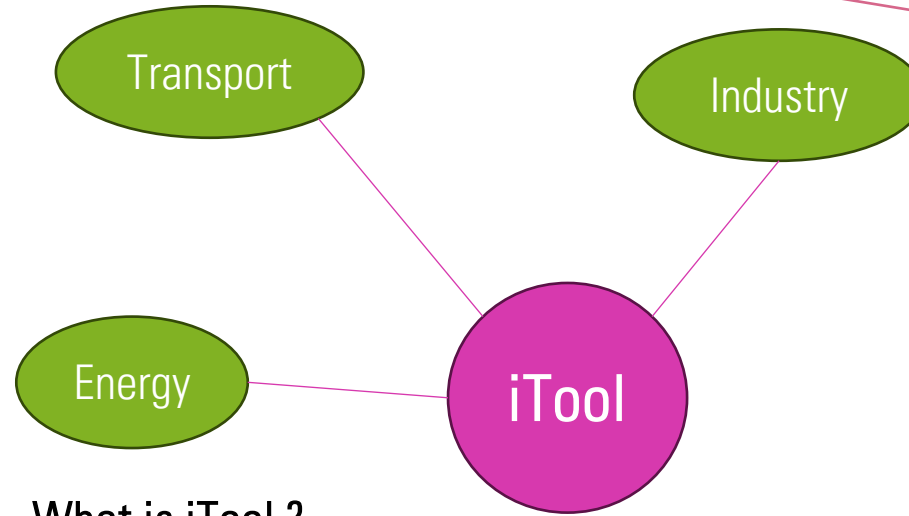


We are a Swedish deep tech company that today support customer with our experience and energy, because we like to help customer that have issues with process or knowledge of system design, electronics, Cybersecurity or Functional safety,

We are finished with our work when customers are satisfied.

Proud to be allocated in LIDKÖPING, Sweden close to Lake Vänern.

Our customers are Industrial, Automotive or Product developers.



What is iTool ?

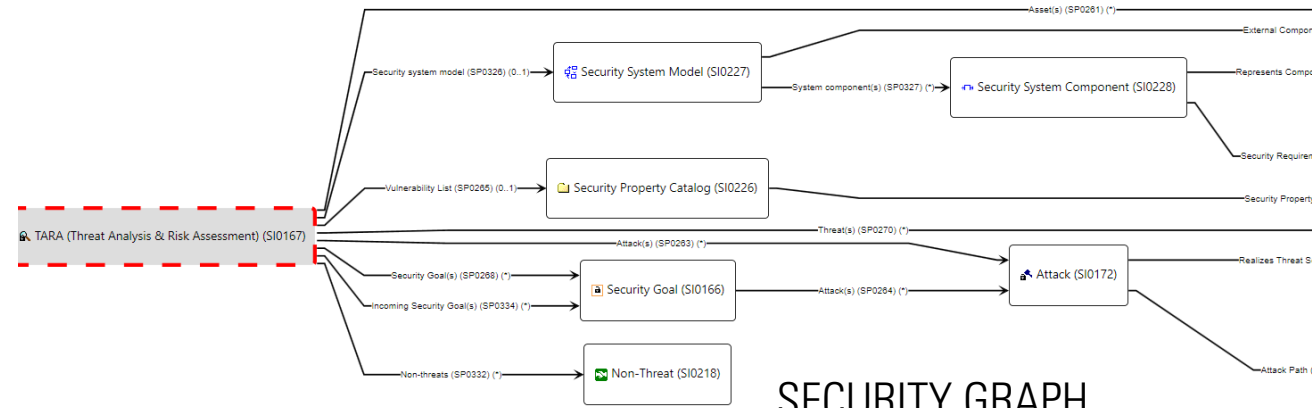
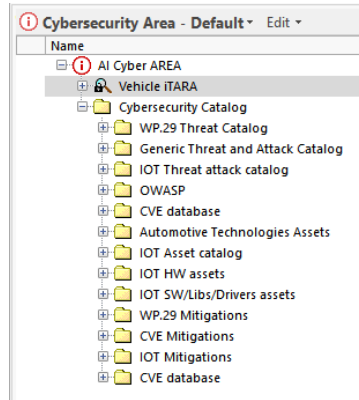
It is driven by the Systemweaver core and with an unique metamodel that define the systems to be analyzed and tested. iTool will be your single source of truth and shared in realtime with modelbased design.

Project goal: Define a shared metamodel for industrial operations analyzes withing Cybersecurity. Methods for develop Cyber database. Easy share of information in realtime, threats, mitigations.

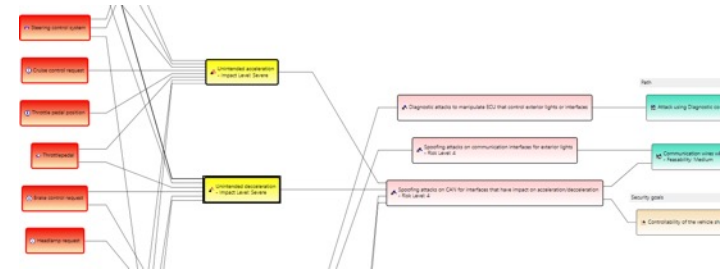
Define penetration tests from systems.

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

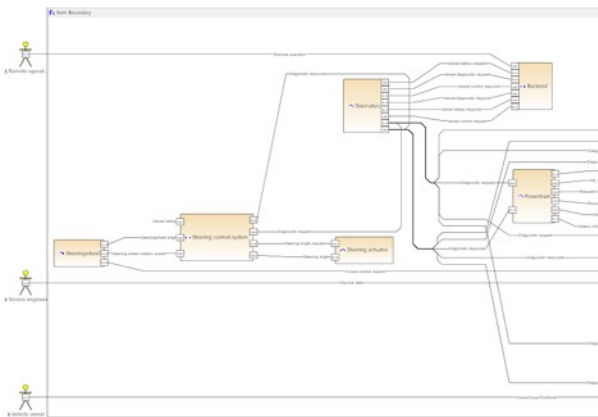
METAMODEL AND TOOL



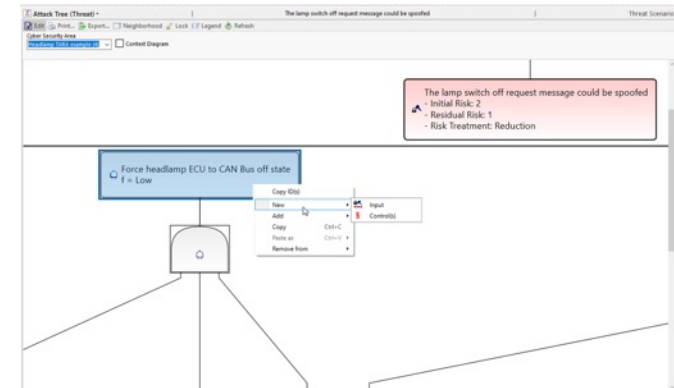
SECURITY GRAPH



SYSTEMMODEL



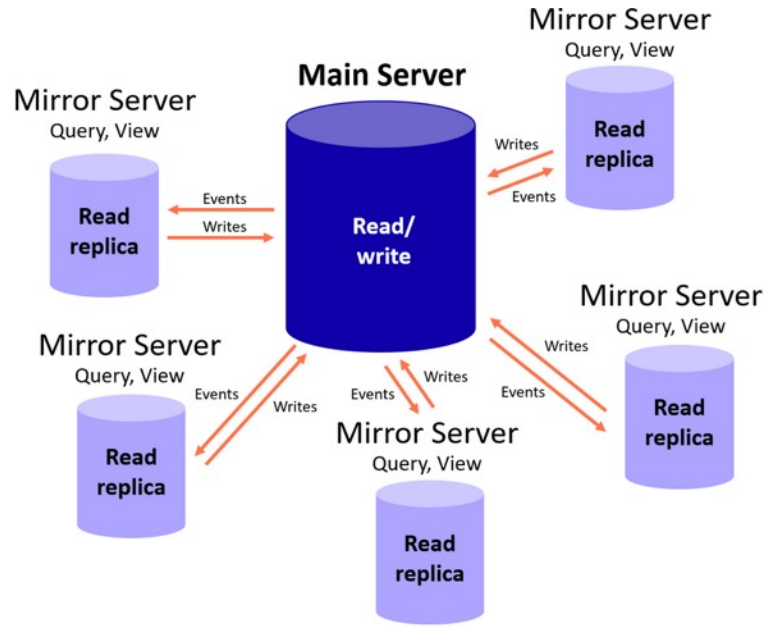
- iTool give all stakeholders through:
- Threat Analysis and Risk Assessment
 - Functional Security Concept
 - Technical Security Concept
 - Requirements specification and traceability
 - Test specification and management
 - Process management
 - Tool qualification
 - Document generation
 - Security case, planning, management and more



iTool will be your single source of truth and shared in realtime .

Risks and threats, CVE database, mitigations can be shared within nations and with local LLM model use of AI to find updates and new threats.

- [-] Cybersecurity Catalog
 - [+] WP.29 Threat Catalog
 - [+] Generic Threat and Attack Catalog
 - [+] IOT Threat attack catalog
 - [+] OWASP
 - [+] CVE database
 - [+] Automotive Technologies Assets
 - [+] IOT Asset catalog
 - [+] IOT HW assets
 - [+] IOT SW/Libs/Drivers assets
 - [+] WP.29 Mitigations
 - [+] CVE Mitigations
 - [+] IOT Mitigations
 - [+] CVE database





Conny Broberg

CTO

0706-921119
conny@ithing.se



Mikael Johansson

COO

0704-150199
mikael@ithing.se



Together we challenge issues within Cybersecurity



Contact us for collaboration within Cybersecurity projects we are happy to support!

<https://ithing.se>

PILAR0: Preparedness and Integrated Large-scale Assistance for Resilient Operations

- *Adriana Freitas*
- *adriana@apwg.eu*
- *APWG.EU*
- *Role: WP leader*
- *DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER - Preparedness Support and Mutual Assistance, Targeting Larger Industrial Operations and Installations*



**CYBERSECURITY
CALLS**

PILAR0/ Preparedness and Integrated Large-scale Assistance for Resilient Operations

APWG Contribution

1. Partner Collaboration and Networking

- Building Strong Consortia
- Hosting Collaborative Events

2. Penetration Testing and Vulnerability Assessment Support

- Collaborative Penetration Testing
- Utilizing Cyber-Ranges

3. Threat and Risk Assessment Collaboration

- Implementing Threat Assessments
- Continuous Risk Monitoring

4. Consulting and Advisory Services

- Expert Recommendations

5. Dissemination and Awareness Campaigns

- Cybersecurity Awareness Initiatives
- Stakeholder Engagement



PILAR0/ Preparedness and Integrated Large-scale Assistance for Resilient Operations

Integrated Cybersecurity Platform:

- *User-friendly interface for creating and managing Requests for Proposals (RFPs) for penetration testing and threat assessment.*
- *AI-driven recommendations for specifying testing requirements based on industry benchmarks and historical data.*
- *Streamlined process for receiving and evaluating competitive bids using AI algorithms for vendor suitability assessment.*

Tailored Penetration Testing Scenarios:

- *Customized AI-enhanced scenarios covering networks, applications, virtualization, cloud solutions, industrial control systems, and IoT.*
- *AI tools and templates to dynamically adjust scenarios based on real-time threat intelligence and emerging cybersecurity trends.*

Automated Procurement and Vendor Selection:

- *AI-powered system for automated bid analysis and comparison, optimizing vendor selection based on performance metrics and historical data.*
- *Criteria-based evaluation ensuring alignment with security requirements and budget constraints, enhanced by AI-driven analytics.*

Secure Collaboration and Communication:

- *AI-assisted secure channels for real-time interaction and collaboration between industrial companies and cybersecurity vendors.*
- *AI algorithms for automated anomaly detection and threat monitoring within communication channels to enhance security.*

Support and Training:

- *AI-driven insights and recommendations embedded in support resources and training materials to optimize platform utilization.*
- *Continuous AI-based updates and enhancements to improve usability, functionality, and security posture based on user feedback and evolving cybersecurity threats.*

PILAR0: Preparedness and Integrated Large-scale Assistance for Resilient Operations

Industrial players, energy, transport and banking, and entities in other relevant sectors.

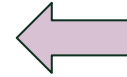
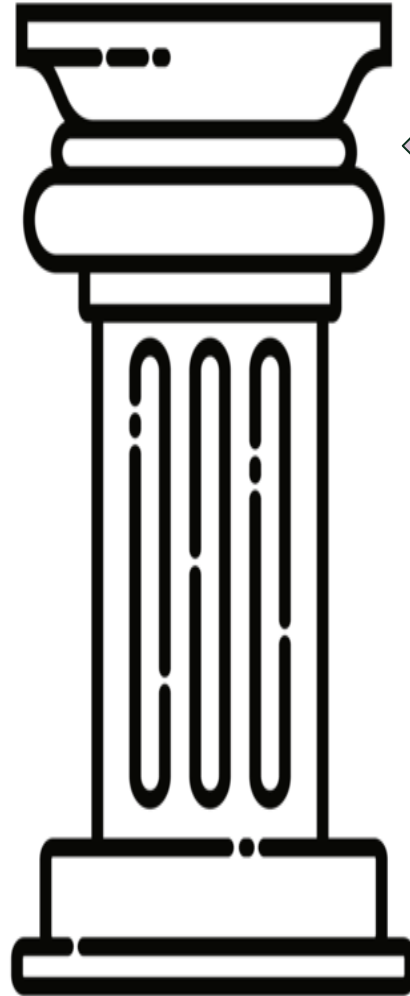
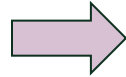
**National cybersecurity authorities,
National cybersecurity competence centres,
National Coordination Centres**

Integrated Cybersecurity Platform

- *interface for (RFPs) for penetration testing and threat assessment.*
- *AI-driven recommendations*
- *Receiving and evaluating competitive bids using AI*

Tailored Penetration Testing Scenarios

Automated Procurement and Vendor Selection:



Cybersecurity Providers

Secure Collaboration and Communication:

- *AI-assisted secure channels for real-time interaction and collaboration between industrial companies and cybersecurity vendors.*
- *AI algorithms for automated anomaly detection and threat monitoring within communication channels to enhance security.*

Support and Training:

- *Continuous AI-based updates and enhancements to improve usability, functionality, and security posture based on user feedback and evolving cybersecurity threats.*

PILAR0/ Preparedness and Integrated Large-scale Assistance for Resilient Operations

- Project participants - Existing consortium:
 - Proposed coordinator: Not yet
 - Partners / Other participants: 3
- Looking for the partners below:

1. Cybersecurity Technology Providers

- Cybersecurity Software Companies
- Penetration Testing Firms
- Cyber-Range Developers

2. Research and Academic Institutions

- Universities and Research Centers: Institutions conducting cutting-edge research in cybersecurity, artificial intelligence, big data analytics, and related fields. They can contribute to the development of innovative solutions and technologies.
- Cybersecurity Competence Centers: National or regional centers specializing in cybersecurity research, training, and policy development.

3. Governmental and Regulatory Bodies

- National Cybersecurity Authorities:
National Coordination Centers (NCCs)

4. Consulting and Advisory Firms

- Cybersecurity Consulting Firms
- Risk Management Specialists

5. Industry Associations

- Sector-Specific Associations: Organizations representing critical infrastructure sectors (e.g., energy, transport, finance) that can mobilize their members and provide sector-specific insights.



DIGITAL-ECDC-2024-DEPLOY-CYBER-07-LARGEOPER

Preparedness Support and Mutual Assistance, Targeting Larger Industrial Operations and Installations

LSEC CyberSecurity Innovations

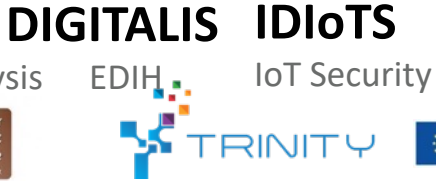
Digital Security Catalyst



This project has been funded with support from the European Commission
101128103 - CYSSME



Ulrich Seldeslachts,
July 8th 2024



EXECUTIVE SUMMARY

- Using best of breed expertise and experiences to lead Open Calls for pentesting and vulnerability assessments
 - Enhancing existing platforms for continuous testing
 - Enhancing and securing information exchange for exploitable vulnerabilities and dependency tracking
 - Operating in classified information
 - Enhancing cyber ranges and testing scenarios
 - Capability of setting methods and requirements for Open Calls and leading by example
 - Potentially testbeds and assessment platforms
- Consortium:
 - Best of breed partners in European projects and organising FSTP and delivering impact on those FSTP's in economic growth and sustainability

APAX

Posture Analysis



LSEC
LEADERS IN SECURITY

INTRODUCING CYSSDE.EU (DEPLOY-CYBER-06)

- Up to 200k EUR for pen-testing and vulnerability assessments of SMEs, critical infrastructure and applications and devices for critical infrastructure and security
- Together with the Member State NCCs
- Joint methodology development of assessments and capacity building
- First Open Call expected to be launched before the end of 2024



ALIGNING CYSSME.EU (CYBER-03-UPTAKE-CYBERSOLUTIONS)

CYSSME - CyberSecurity for SMEs supported by the EC ABOUT

CyberSecurity and Data Protection for Small, Medium and Micro Enterprises

deploying solutions, serving targeted European SMEs

CYBERSECURITY **SUPPORTED BY THE EC**

EU supported cybersecurity

- 1. CybersSecurity Analysis**
assessment
compliance check
- 2. Tooling**
implementing
cybersecurity
technologies
- 3. Service & Management**
- 4. Network**
supporting public and
private financing



CYBERSECURITY MATURITY IMPROVEMENT

INTERACT

CYBERSECURITY OFFERING

CyberSecurity for European Micro and Small, Medium sized Enterprises by European CyberSecurity solutions and expertise SME providers

1

NETWORK AND END POINT SECURITY

immediately protect network and computers.

2

THIRD PARTY RISK

your and your supplier's vulnerabilities visibility

3

COMPLIANCE MANAGEMENT

dashboard and underlying tools
Be prepared for NIS2.

4

INDUSTRIAL

detecting, monitoring and controlling operational appliances

Not the end

More information, slides and follow-up
www.cyssme.eu – www.cyssde.eu
www.lsec.eu



Q or C
Ulrich Seldeslachts
ulrich@cyssme.eu
+32 475 71 3602



Networking

A dedicated room has been setup for meeting with the pitch presenters

➔ Follow the indication to the rooms downstairs



Thank you