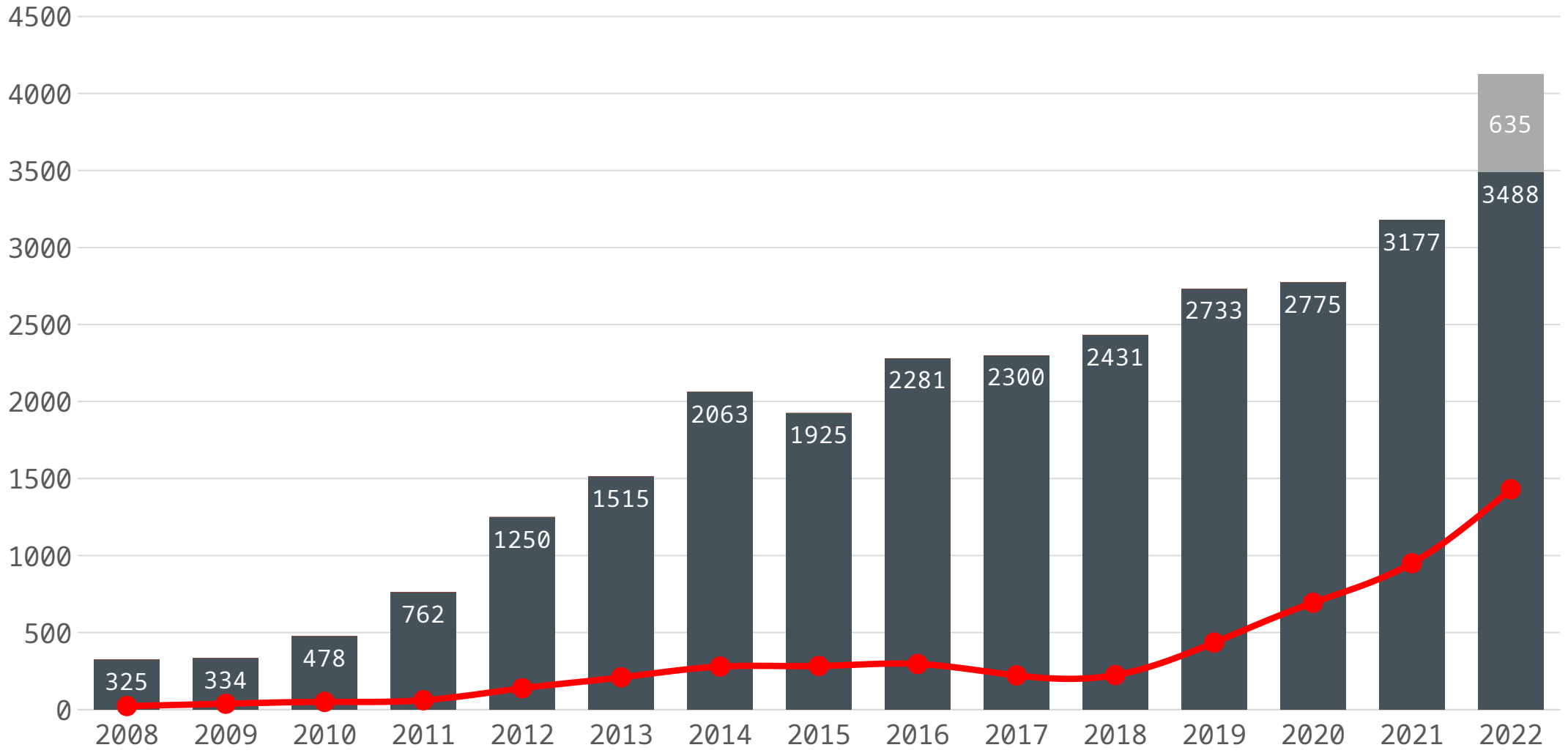
TEAM UPDATE

TF-CSIRT meeting

Bucharest, 25.5.2023

INCIDENTS PER YEAR



PLANNED ACTIVITIES IN 2023

- Tier 1 support
- Phishing automation and publicly available blocklists (+ CNW WG initiative)
- Support of nuclear cybersecurity via SNSA
- Support&training in Montenegro
- CyberSEAS partner
- NIS2 implementation

VARNI NA INTERNETU

- 10 years (steady financing)
- Activities thru the whole year
- ECSM coordination
- Varni v pisarni – Safe in the office
- Cooperation with stakeholders
  - Awareness raising of senior citizens: MOL, MDP

NIS2

"EXPLOSION" OF OBLIGEE

expands the circle of obligee (Article 2) to:

- in addition to the essential ones, also "important subjects"
- providers of public EC networks and publicly available EC services
- trust service providers
- top level domain name registries and domain name system service providers
- public administration entities at the central state and regional level
- entities that "register domain names, regardless of their size"

- introduces the term "near miss"

NATIONAL STRATEGY (ARTICLE 7)

- defines policies and other mandatory parts
- a mechanism for identifying the appropriate means
- vulnerability management
- education and training
- citizen awareness plan
- availability, integrity and confidentiality
- renewal at least every 5 years

CSIRT TEAMS (ARTICLE 11)

2. Države članice zagotovijo, da imajo njihove skupine CSIRT skupno potrebne tehnične zmogljivosti za izvajanje nalog iz odstavka 3. Države članice zagotovijo, da se njihovim skupinam CSIRT dodelijo zadostna sredstva za zagotovitev ustreznega števila osebja, ki skupinam CSIRT omogoča razvoj njihovih tehničnih zmogljivosti.

(3.e) conducting, at the request of a material or significant entity, a **proactive review of the network and information systems** of that entity to detect vulnerabilities that could have a material impact;

(3) CSIRT groups may conduct proactive and unobtrusive inspections of publicly accessible network and information systems of essential and important entities. Such scanning is performed to detect vulnerable or unreliably configured network and information systems and to notify the relevant entities. **Such screening must not have a negative impact on the operation of the entities' services.**

(4) CSIRT groups **cooperate with relevant stakeholders from the private sector** to achieve the objectives of this directive.

VULNERABILITY DISCLOSURE (ARICLE 12)

- one CSIRT per MS is the coordinator
- tasks:
  - identification of relevant subjects and establishment of contact with them;
  - supporting natural or legal persons reporting vulnerabilities, and
  - negotiating timelines for disclosure and management of vulnerabilities affecting multiple entities.
- ENISA maintains a vulnerability register (has a copy of the CVE register)

HIGHLY CRITICAL SECTORS (PR. I)

1. energy (electricity, district heating and cooling, oil, gas, hydrogen)
2. transport (air, rail, water, road)
3. banking
4. financial market infrastructure
5. health
6. drinking water
7. waste water
8. digital infrastructure (IXP, DNS, ccTLD, cloud services, data centers, content delivery, trust services, public communication networks, publicly available services)
9. management of ICT services
10. public administration
11. space

OTHER CRITICAL SECTORS (PR. II)

- postal and courier services
- waste management
- manufacture, production and distribution of chemicals
- production, processing and distribution of foodstuffs
- production (medical and diagnostic devices, production of computers, electronic and optical products, electrical devices, other machines and devices, motor and other vehicles)

CyberSEAS

Cyber Securing **E**nergy **D**ata **S**ervices

This project has received funding from the European Union's Horizon 2020
research and innovation programme under grant agreement No 101020560

About the project

CyberSEAS at a glance

Topic:	SU-DS04-2018-2020 Horizon 2020
Grant Number:	101020560
Total Cost:	€ 10.067.121,25
EC Contribution:	€ 7.999.113,64
Start Date:	01/10/2021
End Date:	30/09/2024

CyberSEAS: improving the cyber security of the European Electrical Power and Energy Systems.

Coordinator Technical coordinator

29 partners

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020560

Strategic objectives

- SO1 - Countering the cyber risks related to the highest impact attacks against Electrical Power and Energy Systems (EPS)
- SO2 – Protecting consumers against personal data breaches and cyber attacks
- SO3 - Increasing security of the Energy Common Data Space (enhancing the governance relating to exchanging operational data across interconnected EPS)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020560

Solutions

- CyberSEAS delivers an open and extendable ecosystem of 30 customisable security solutions providing effective support for key activities, and in particular:
  - risk assessment,
  - interaction with end devices,
  - secure development and deployment,
  - real-time security monitoring,
  - skills improvement and awareness,
  - certification, governance and cooperation.
- Out of the 30 solutions, 20 will reach TRL[1]8+ (System complete and qualified) and 10 TRL[1]7 (System prototype demonstration in operational environment).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020560

[1]TRL - Technology readiness level

CyberSEAS solutions

	Provided by	Tool	Tool features/objectives
1	ACS	CyberRange	Advanced simulation solution to easily model IT/OT systems composed of tens or hundreds of machines and simulate realistic scenarios including real cyber-attacks
2	CINI	ATRS	Advanced Tamper Resistant Storage
3	CINI	BP-IDS	Intrusion detection system acting based on business/process level KPIs
4	CINI	CI SOC	Advanced SOC with features dedicated to CIs
5	CINI	HwTEE	JNI-based bridge for Intel SGX TEE technology
6	CINI	PKI	High-performance secure enclave for cryptographic key management.
7	CINI	SIEM	Fully fledged SIEM solution with enhanced situation awareness capabilities
8	CINI	Virtual Testbed	Cyber-range training environment providing EPES users with a virtual SCADA setup
9	CREN ENG, SYN	ETSI Standard Countermeasures	Upscale of the H2020 SUCCESS ETSI Standard Countermeasures Guidelines and Tools
10	ENG	ALIDA	Micro-service oriented platform for the composition, deployment and execution of Big Data Analytics (BDA) services implementing an extensive set of supervised and unsupervised machine learning algorithms
11	ENG	D.HUB	Digital Platform Services for secure hosting of managed EPES services
12	ENG	ESOC	Correlates events from cyber and physical sources / proposes intrusion responses using ML

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020560

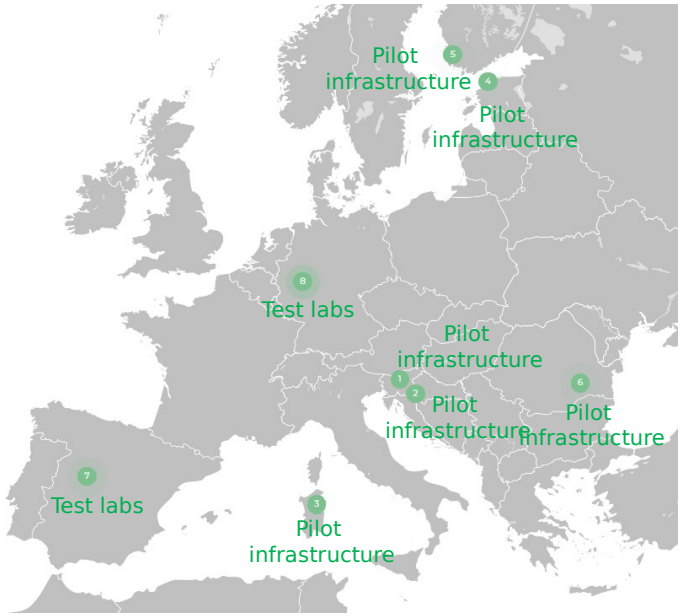
CyberSEAS solutions

13	ENG	IEC 62443-4-2	Security patterns and libraries to implement IEC 62443-4-2
14	ENG	OPENESS.edu	Analytics and skills manager tools monitor trainee progress and adapting learning paths
15	ENG	Situational picture dashboard and visual analytics	Based on EPES-specific situational awareness knowledge model, a set of algorithms and components for multi-dimensional information fusion and integration on resilience indicators and relevant events (with exploitation of historical stored data and other external information) integrated to deliver effective real-time C/P situational pictures of the EPES CIP with higher level information.
16	ENG	SSecA	Software module for the secure connection of smart meters with the operator cloud, ensures integrity of collected measurements and enables anomaly detection on edge sides.
17	ENG	RATING	Risk Assessment tool for INtegrated Governance, allowing organizations to conduct cyber and privacy risk assessments.
18	ENG	TO4SEE	Measure Social Engineering (SE) Exposure of an organization and detect SE ongoing attacks
19	Fraunhofer	Testing lab	Provides a safe environment where a complete and integrated testing of cybersecurity solutions can be performed. While a simple IT test can be performed in many laboratories, this laboratory has a unique combination of IT solutions and real power equipment at 1:1 scale.
20	Fraunhofer	SAPPAN Toolbox	1) Anonymization tool for cybersecurity data abstraction: ensures that when specific ML classifiers are shared between different organizations, they do not leak private information 2) Tool for federated threat detection and intelligence sharing 3) Tool for managing cybersecurity threat intelligence: effective handling for analysts to prioritize threats based on severity levels / includes partial automation of mitigation response
21	GT	MIDA	Cloud control tool
22	ICS	Penetration testing framework	CEH (Certified Ethical Hacker) recommendations compliant equipment and programs for pen-testing campaigns
23	IKE	Evaluation lab	Infrastructure to define and execute cybersecurity evaluation strategies
24	IKE	Heindall	An automatic vulnerability detection system for IEDs
25	RWTH	Attack-Defence Simulator	Cyber-Enriched Attacked Defence Simulator: Simulation approach for attack-defence-simulation to study potential attack and countermeasures evolution
26	SQS	SQS Test Lab	Testing laboratory for Common Criteria and LINCE evaluations
27	STAM	DAISY	Decision-support tool based on quantitative risk assessment of attacks on the infrastructure including terroristic attacks
28	STAM	KARMA	Modelling framework for safety and security risk assessment of CIs
29	SYN	Federated Learning Framework	Machine Learning/ Deep Learning framework that enhances confidentiality among the CIs, without moving sensitive data from their original sources.
30	WINGS	ARTEMIS	1) information collection, through sensors and actuators (e.g., meters, cameras, etc.) 2) insights and predictions, through AI algorithms applied to collected data The platform will be enhanced with new means for protecting the devices of the extended digital surface of the future grid, addressing data breach cases, conducting identification and addressing cascading effects.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020560

Pilots

- **CyberSEAS solutions will be validated** through experimental campaigns consisting of 100+ attack scenarios.
- The pilot scenarios will be reproduced in lab for a preliminary evaluation of CyberSEAS features and tools. (Labs: Ikerlan, Software Quality Systems, Fraunhofer FIT and RWTH Aachen University).
- And after their final tuning the scenarios will be deployed in one of the **6 infrastructures provided by CyberSEAS partners**
  - **Estonia**
  - **Finland**
  - **Italy**
  - **Romania**
  - **Slovenia+Croatia**



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020560

Slovenian-Croatian pilot project

- **Challenges of continuous and uninterrupted collection of non-energy related data.**
  - ELES and OPERATO collect and use environmental data from different sources to optimize network power flows close to real time using novel system for dynamic line rating called SUMO. This data automatically feeds SUMO that is connected with SCADA systems supporting real time system operation.
- **Challenges of cooperation between TSO[1]s, aggregators, retailers and diverse prosumers, when using public communication networks.**
  - It addresses cyber-security challenges of current energy-domain data exchanges using economically favourable (public) communication connections compliant to technical standards and propose new means of secure communications supporting wide cooperation with aggregators as well as open governance solutions for cooperation. It connects with the Slovenian CERT.
- **Challenges of cyber-security governance across organisations**
  - extending to the national agencies and CERT.
- **Challenges of cross-border cooperation among Slovenian and Croatian TSO[1] (HOPS).**
  - The campaign will use the MeliCERTs platform/tools, with partner SI-CERT. It will also address structural data exchange between Eles and HOPS for the needs of the Virtual Cross-border Control Center.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020560

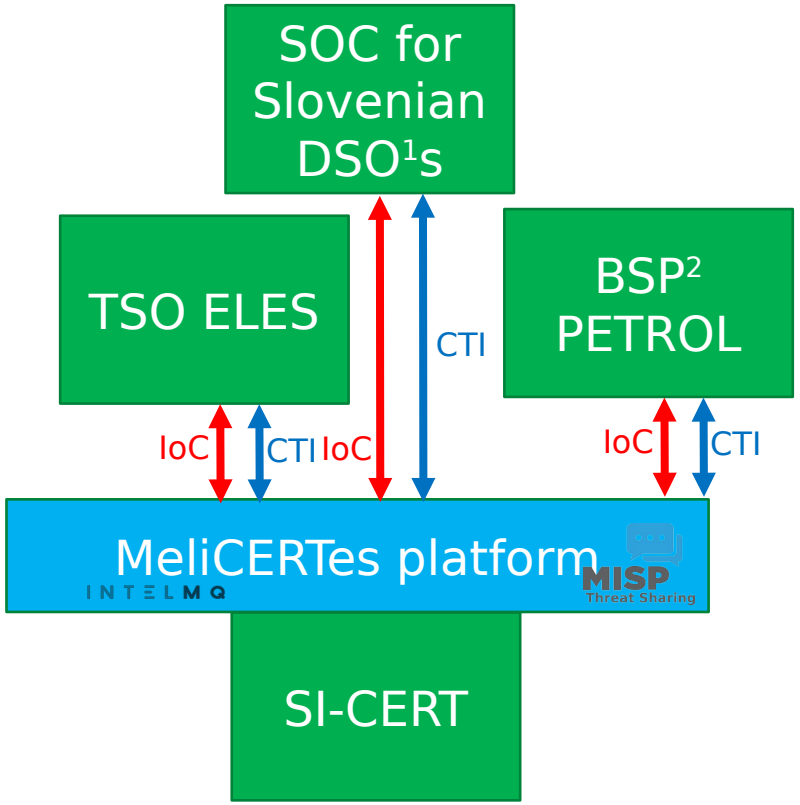
[1]TSO – Transmission system operator

Slovenian-Croatian pilot project's topics

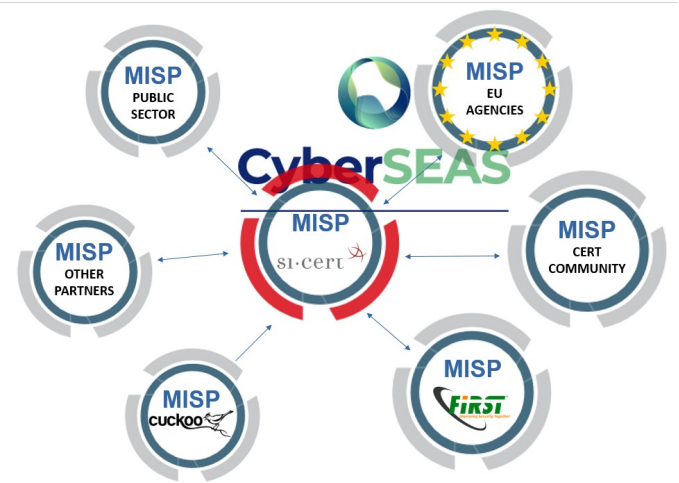
PARTNER	Topic 1 (Securing energy and non-energy data exchanges)	Topics 2 (Cyber-security cooperation scenarios / governance model)	Topic 3 (Cyber-security cooperation scenarios / governance model) Cross-border	Main assets related to the pilot project
ELES (Slovenian TSO) **OPERATO (Doughter company of ELES)**	X	X	X	Transmission power system, SCADA/EMS, Balancing Services Market Platform, SUMO Dynamic Rating system, Sincro.grid VCC
HOPS (Croatian TSO)			X	Transmission power system, Sincro.grid VCC
PETROL	X	X		Distributed energy resources, Ve.TER Virtual Power Plant platform
INFORMATIKA	X	X	(X)	SOC
SI CERT		X	X	MeliCERTes platform
ICS	X	X	X	Penetration testing equipment

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020560

Exchange of feeds, events and incidents



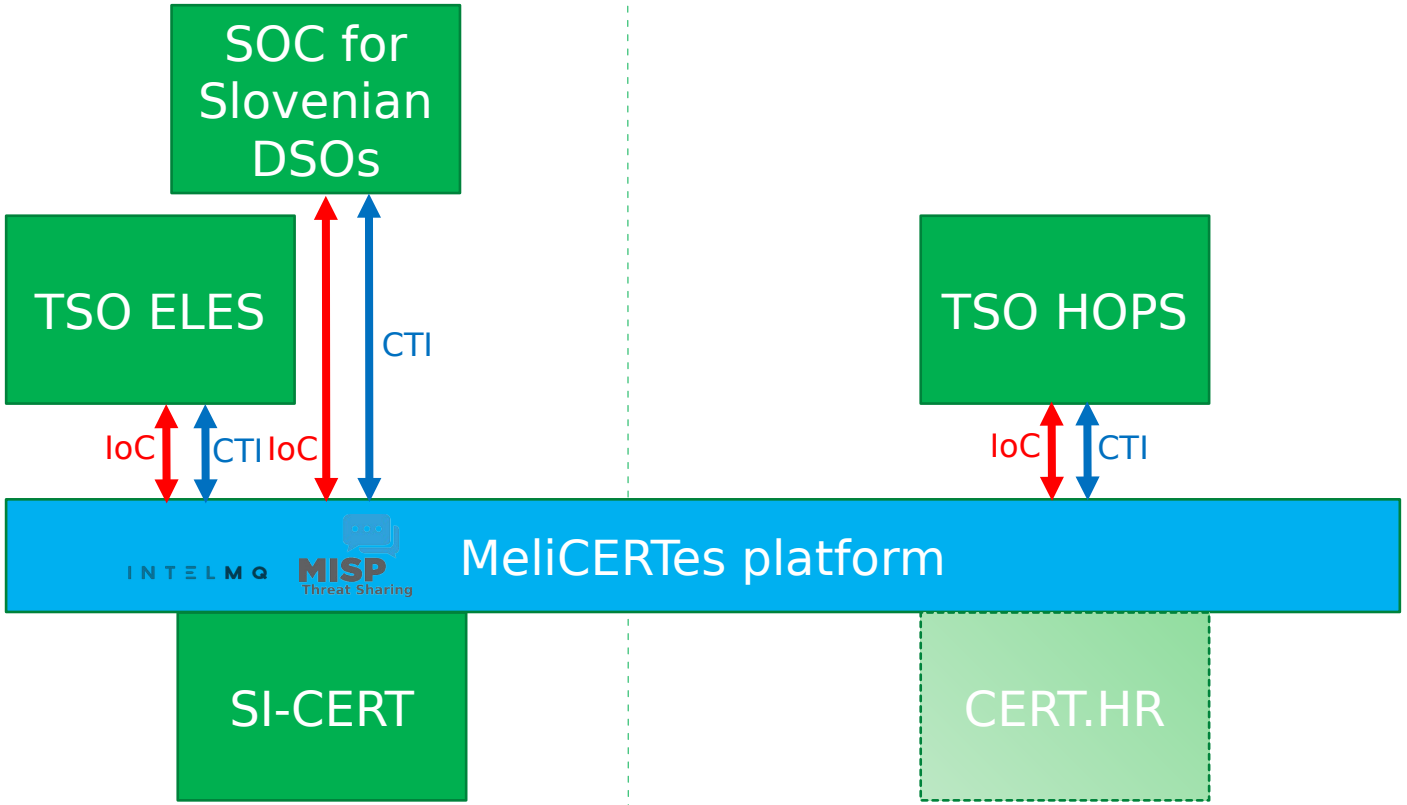
- Indicators of compromise (IoC)
- Cyber Threat Intelligence (CTI)



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020560

[1]DSO – Distribution system operator
[2]BSP – Balancing service provider

Exchange of feeds, events and incidents



- Indicators of compromise (IoC)
- Cyber Threat Intelligence (CTI)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020560

Stakeholders welcome

- Be informed about main projects processes and technical developments in the area of EPES
- Possibility for exchanging best practices and latest experiences in EPES environment
- Possibility to influence on preparation of new EU regular framework in the area of EPES with proposals and suggestions
- Possibility to influence on preparation of new standardization framework in the area of EPES with proposals and suggestions
- Become an important part of the expert network for sharing new security-related ideas in the EPES area

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020560

Thank you!

Matej Breznik
SI-CERT
matej.breznik@cert.si

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020560