



ENERGY SHIELD

**ENERGYSHIELD PROJECT
SHIELDING THE POWER GRID FROM
CYBERATTACKS**

2nd ESCI workshop, 27-29th of April 2022

Facilitator: Otilia Bularca, Project Manager, SIMAVI



4/27/2022



AGENDA

01

ABOUT THE PROJECT

02

TOOLS & PILOTS

03

PROJECT 2 POLICY

04

LESSONS LEARNED





ENERGY SHIELD

ABOUT THE PROJECT



4/27/2022




















ENERGYSHIELD PROJECT IN A NUTSHELL

- **Title:** Integrated Cybersecurity Solution for the Vulnerability Assessment, Monitoring and Protection of Critical Energy Infrastructures
- **Type of Action:** Innovation Action
- **Topic:** SU-DS04-2018-2020
 - Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks and data breaches
- **Goal**
 - EnergyShield captures the needs of Electrical Power and Energy System (EPES) operators and combines the latest technologies for vulnerability assessment, supervision and protection to draft a defensive toolkit.
- **Start date:** 1st of July 2019
- **Duration:** 36 months
- **Grant:** € 7,421,437.38

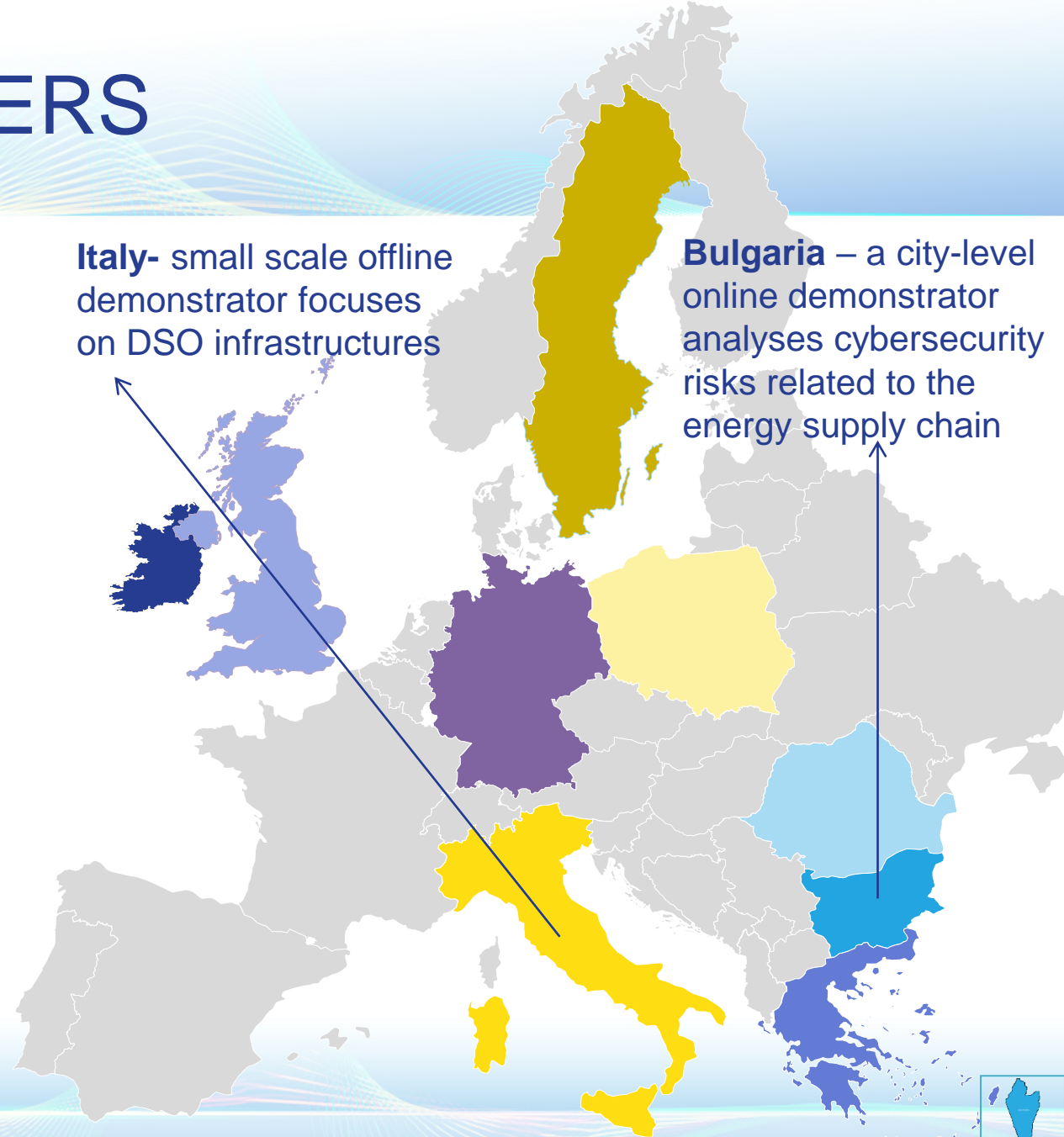


CONSORTIUM PARTNERS

- Romania:** Software Imagination & Vision 
Software Imagination & Vision
- Germany:** PSI Software AG 
- Israel :** SI-GA Data Security (2014) LTD 
OT Solutions
- L7 Defense LTD** 
- Sweden:** foreseeti AB 
 Kungliga Tekniska Hoegskolan 
- UK:** Tech Inspire LTD 
 City University Of London 
- Ireland:** Konnekt Able Technologies 
- Greece:** National Technical University Of Athens 
- Bulgaria:** Software Company EOOD 
 Kogen Zagore EOOD 
 MVETS Lenishta OOD 
 Elektroenergien Sistemen Operator EAD 
 CEZ Distribution Bulgaria AD 
 MIG 23 LTD 
 DIL DIEL 
 IREN SPA
- Italy**

Italy- small scale offline demonstrator focuses on DSO infrastructures

Bulgaria – a city-level online demonstrator analyses cybersecurity risks related to the energy supply chain

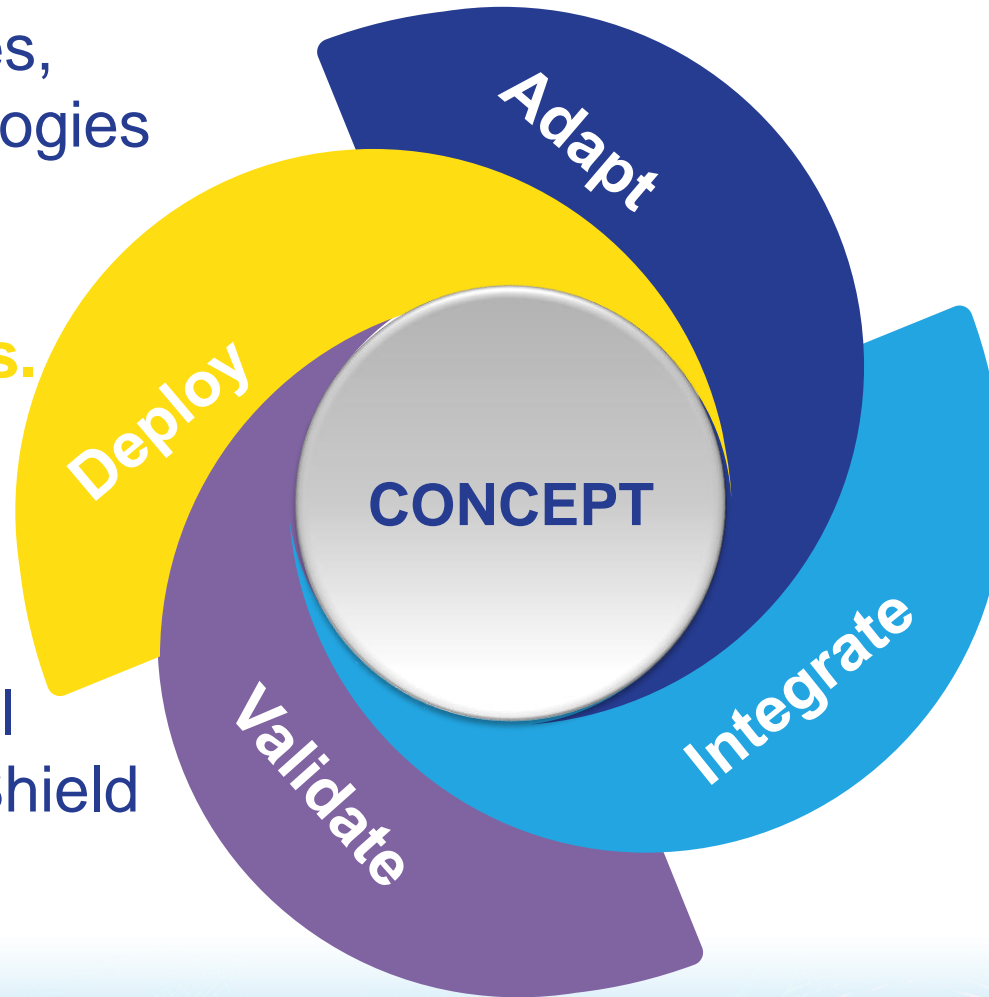




WHAT DID WE AIM FOR

Deploy best practices, guidelines, methodologies and encourage the adoption of EnergyShield **results**.

Validate the practical value of the EnergyShield **toolkit** with EPES stakeholders.



Adapt and improve available **tools** to support Electrical Power and Energy System (EPES) in fighting against cyber attacks.

Integrate the cybersecurity tools in **a holistic solution** with assessment, monitoring, protection and learning capabilities.



ENERGY SHIELD

TOOLS AND PILOTS



4/27/2022



HOW DID WE ORGANIZE THE ACTIVITIES?



Assessment tools

- Provide information on most critical attack vectors and probable paths

Monitoring tools

- provide early warning on incoming attacks and malware

Learning and sharing

- provide feedback on the proposed attack vectors by enabling real-time incident logging and analysis

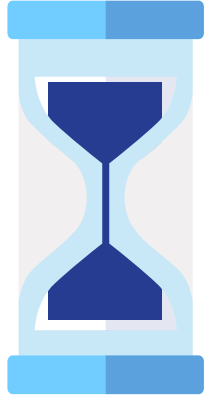


ENERGYSHIELD PILOTS COMPARATIVE APPROACH

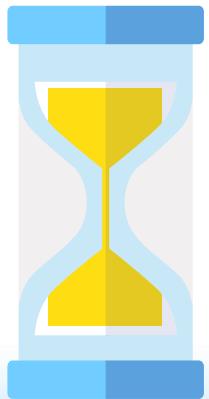
	Bulgarian Pilot	Italian Pilot
Location	District of Sofia and Pernik, Kyustendil, Blagoevgrad, Vidin, Montana, Vratsa, Plevan and Lovech districts.	DSO network of the city of Turin, Italy
Aim	Study the cascading effects of cyberattacks throughout the value chain and analyse cybersecurity risks related to the cyber supply chain	The feasibility study (and possible offline trial on a dedicated, simulation area of the networks control systems, if feasible) will be set on Turin DSO network.
Innovation	Mitigate cyber attacks and data breaches taking into account decentralised architecture and all stakeholders of the value chain,	Possibility to test an integrated suite of cyber security tools; Defining evaluation KPIs of the testes solutions with all stakeholders involved
Approach	Involving several generators including distributed power generation (hydro and solar PV) as well as several primary substations, secondary substations and end users.	Identifying the most relevant threats and vulnerabilities in each subsystem of the network; Identifying the most effective measures to protect the systems;
Outcome	Full end-to-end demonstrator involving all stakeholders of the EPES value chain Online trial	Evaluate the most effective solutions (hardware and software solutions, organizational approaches, changes in the procedures and qualified the staff in this field) for industrialization Offline trial



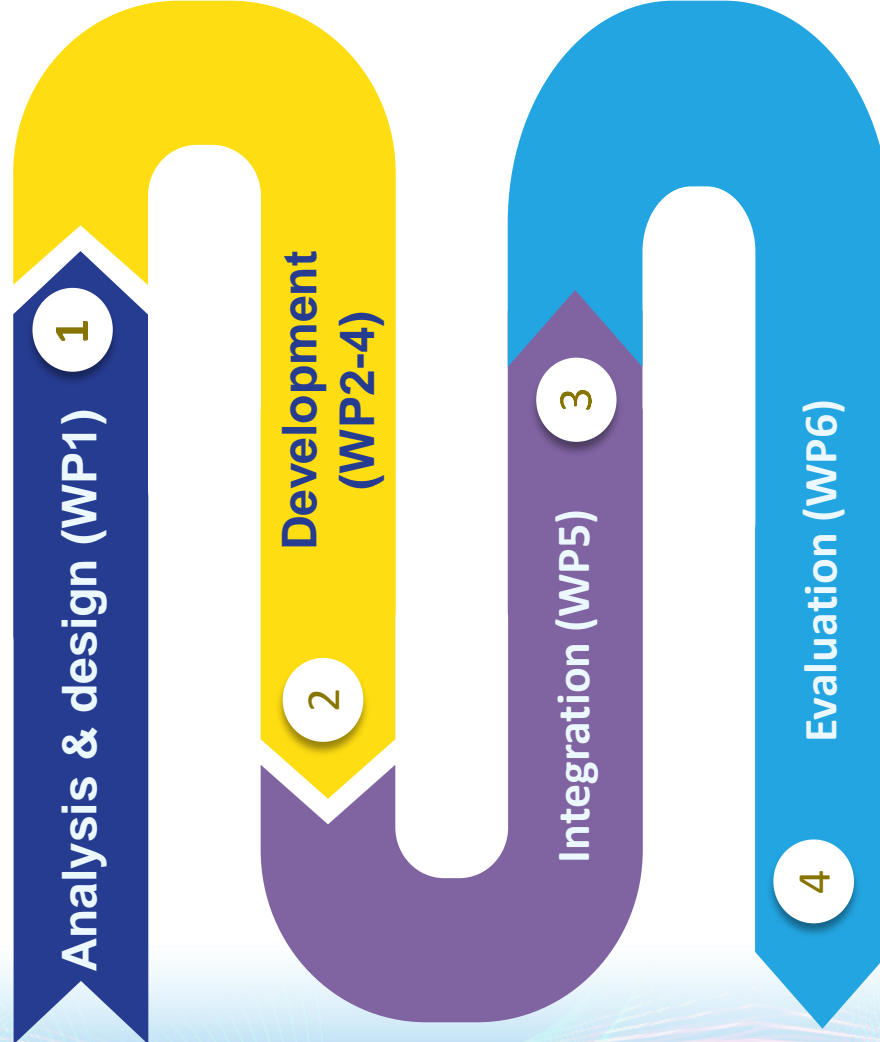
TECHNICAL ACTIVITIES TIMELINE



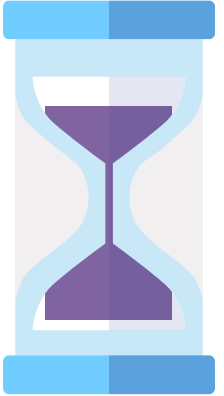
- Analysis
- Architecture
- Functional Requirements
- Non-Functional Requirements



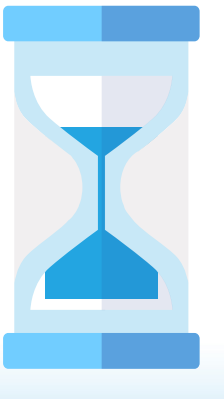
- Tools roadmap
- Tools release plan
- Demonstrators timeplan



- Integration plan
- Deployment plans
- Test plan
- Toolkit demo release timeline



- User needs
- Tools evaluation
- On-site deployment
- Piloting
- Evaluation





ENERGY SHIELD

PROJECT 2 POLICY



4/27/2022

11



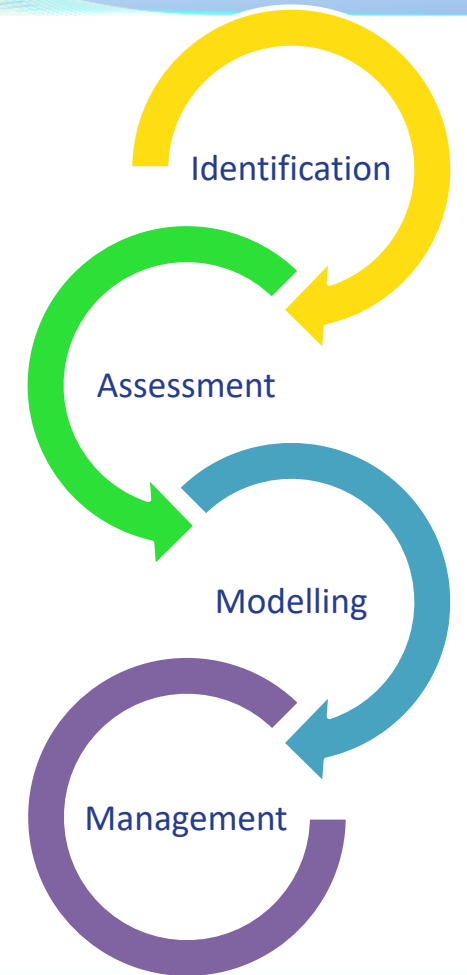
THE RELEVANCE OF A TOOLKIT FOR CI/EPEs

- Supply chains for components of critical infrastructure have gotten recently large attention of policy maker in the telecommunication, especially on 5G-driver regulation
 - This discussion is highly relevant for the energy sector as similar companies are also leading the sector of photovoltaic inverters.
- Software supply chain risks became additionally very visible after hackers inserted malware into the SolarWinds software, which was rolled-out to many customers from the government and critical infrastructure sector.
- Full flexibility systems are preferred .
 - monolith architecture is not feasible as limits the deployment possibilities, is difficult to scale and limits the adoption of new technologies.
 - **containerization** eases the deployment on a variety of system.
- The market and competition assessment confirmed that many tools are cross sectors tools (i.e., no specific offer to the energy sector).
 - There have been several recent incidents that provide good arguments for the exploitation of the EnergyShield toolkit (e.g. the global SolarWinds incident (software supply chain attack), vulnerabilities in Microsoft Exchange and recently the attack to the Colonial Pipeline (USA).)
 - on a high level, suppliers and customers agree that cybersecurity is important, but it is a completely different story to convince utilities to install new cybersecurity (not established) devices into their critical infrastructures



RISK ASSESSMENT

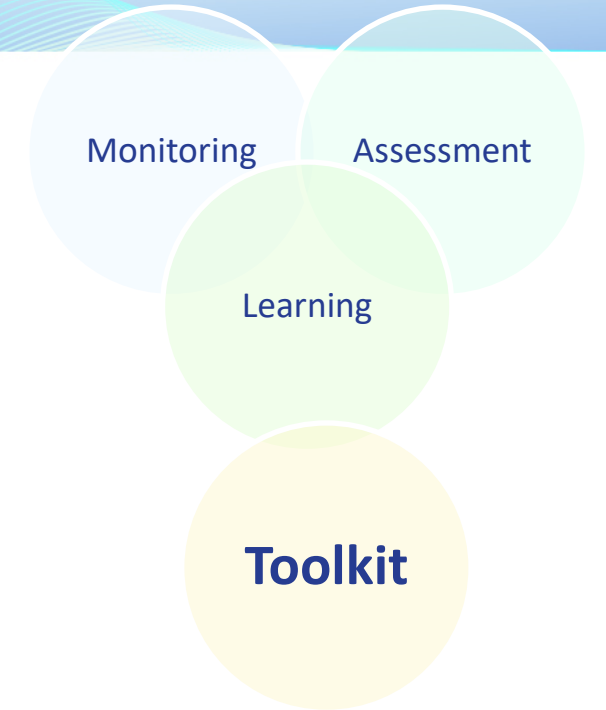
- Energy Shield assessment tools provide information on most critical attack vectors and probable paths.
 - The vulnerability assessment tool integrates a threat model (attack vectors and probabilities) and is built into securiCAD Enterprise; supports MAL based threat modelling languages that allows a more adequate representation of EPES systems. The **Risk Matrix** - Confidentiality, Integrity and Availability - scores are the sum of the probabilities for the attacker to have succeeded with compromising C, I and/or A related operations (like read, write and deny) for the selected high value assets. It is extended to inform other modules of the identified vulnerabilities and priorities in real time. Uses **CVSS** scoring of vulnerabilities. It is non-intrusive, meaning it will not interfere with the actual systems
 - The security behaviour analysis tool to assess evaluates the current security readiness of an organization's workforce. The identification of specific cyber-threats based on the achieved socio-cultural behaviour assessment results exploiting: a) a hybrid **MITRE ATT&CK** (Adversarial Tactics, Techniques, and Common Knowledge) Model for an OT Environment, consisted of a combination of the Enterprise and the ICS threat models and b) an enriched version of the **MERIT** (Management and Education of the Risk of Insider Threat) model. The tool is designed and implemented using a holistic approach to easily adapt and adjust to any business domain
 - Risk information should be linked with SIEM which will provide feedback on the proposed attack vectors by enabling real-time incident logging and analysis for immediate sharing throughout the industry (i.e. decision-support tools to coordinate cyber defender response across the EPES value chain). SIEM is also improved with two concept tools: automated forensic and homomorphic encryption tools.





SIEM TOOL

- The EnergyShield toolkit is organized in several “shelves” or “drawers” and contains hardware components, software components, and communication ports and includes the following components/modules:
 - ASSESSMENT tools add focus on the critical infrastructure components and leverages the security behaviour to improve the vulnerability analysis.
 - For SOCs/CSIRTs, the vulnerability assessment tool can continuously monitor an infrastructure, following and considering changes to the technical infrastructure, human users and IAM, vulnerabilities and cyber threat intelligence. Its usage extends from adversary emulation, red teaming, behavioural analytics development to a defensive gap and SOC (Security Operations Centre) maturity assessment
 - MONITORING & PROTECTION tools focus on allowing rapid attack response (e.g. heat maps of intrusion).
 - LEARNING & SHARING tools gradually automate the security information and event management process and integrate vulnerability assessment tools to create security metamodels.
 - EnergyShield deploys an open source SIEM tool compatible with the most widely used network security tools using the IDMEF (Intrusion Detection Message Exchange Format) standard format, making sure that incident reports can be shared seamlessly with EU CERTs and EPES operators.
- The components of EnergyShield toolkit
 - exposes a set of **REST API** that enables the interoperability between them and the possible integration with other tools.
 - offers **asynchronous message exchange** using queues, inter module asynchronous communication, and allowing external system to **subscribe to the topics**.
 - the toolkit is accessible via a Portal through an authentication mechanism



Continuous monitoring

Exposes REST APIs

Asynchronous message exchange

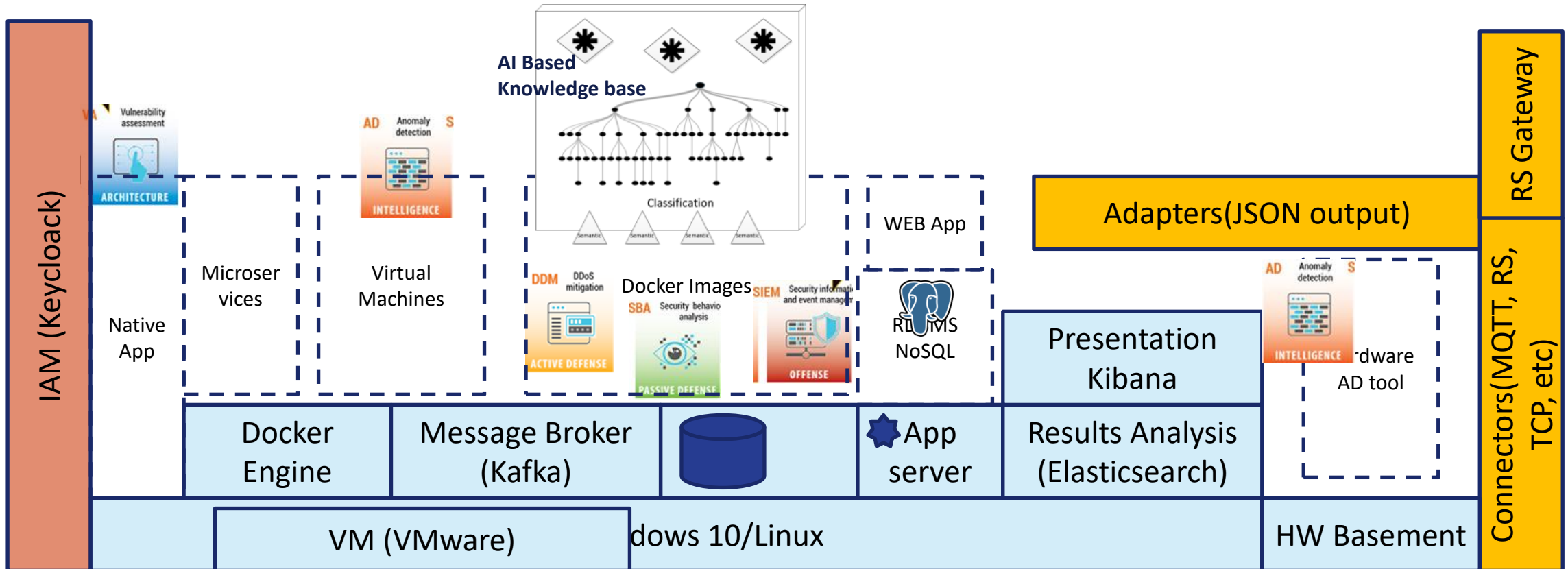


ENERGY SHIELD TOOLKIT

- EnergyShield project develops an integrated toolkit
 - covering the complete EPES value chain (generator, TSO, DSO, consumer).
 - A framework components are supporting components used by the whole deployment.
 - They include container engine (Docker), Authentication and Authorization (Keycloak), Communication system (Kafka), REST, and Process management (Kubernetes).
- The EnergyShield toolkit
 - combines the latest technologies for (automated threat vulnerability assessment modelling), (anomaly detection and DDoS mitigation) and monitoring & protection learning & sharing (security information and event management).
 - The global view of each tool results using a data fusion mechanism combined with a machine learning system able to continuously improve the outputs of the fused model.
 - The whole architecture is federated. There is a central federation Coordinator and there are locally deployed federation members.
 - The central component is responsible for maintaining the rules and standards, for common processing.
 - The federation members are responsible for local data collection and processing.



ENERGYSHIELD TOOLKIT ORGANIZATION





CONCEPT TOOLS

- Energy Shield has worked on a number of concept tools approaching:
 - Cybersecurity supply chain risk analysis (chain of software and hardware components that are part of tools such as control systems that are used to operate critical energy infrastructures.),
 - Automated forensic tool (enrich events identified by the embedded vulnerability detector module with information deriving from different security databases, such as CWE, CAPEC, OVAL, WASC, OWASP)
 - Searchable Encryption and Homomorphic Encryption (anonymise and search data in the encrypted domain using the state-of-the-art homomorphic encryption techniques)



ENERGY SHIELD

LESSONS LEARNED



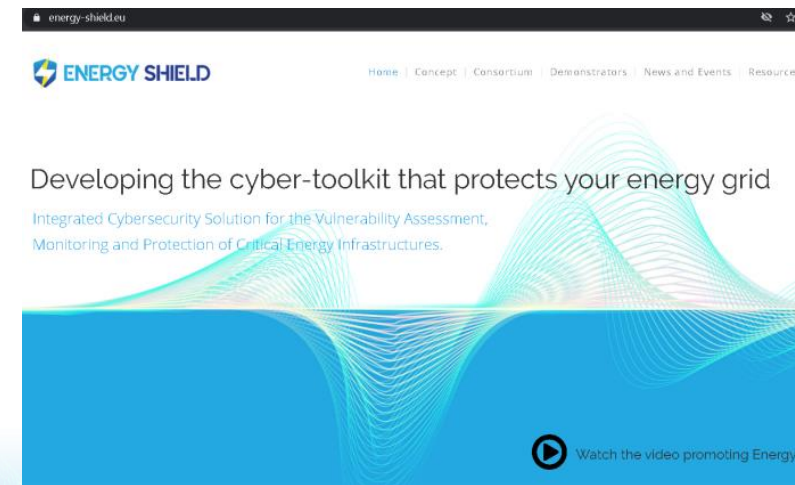
4/27/2022

18



BUILDING ONLINE IDENTITY IS ESSENTIAL

- Social media
 - Twitter
 - LinkedIn
- Project website
 - Articles on events participation
 - Newsletters
- 26 scientific articles published
- Foundation members in 2 clusters: CyberEPES and ESCI





COLLABORATION IMPROVES COMMUNICATION



flexitranstore



FARCROSS



SDN-μSense

CyberEPES
cluster

ESCI Cluster




FLEXIBILITY IS KEY

- Starting from a **plethora of technologies** and use case functionalities the EnergyShield system needs to provide full flexibility
- Adapting and integrating technologies
 - the **technology providers have improved and adapted the tools** making them ready for integration through the overall EnergyShield system and interacted with Practitioners to collect feedback (testing and evaluation of tools)
 - a **flexible integration concept was designed** and is being implemented to ease the accommodation of tools a Portal to securely access the toolkit.
 - technology providers have collaborated towards preparing and **accommodating** tools using different technologies in a common environment (EnergyShield toolkit) and using a data fusion mechanism combined machine learning to create a global view.
- **Challenges**
 - OT and IT integration and testing
 - Integration due to a wide area of technologies used to develop the components
 - Working with different business aspects of the functionality (from behaviour analysis to anomaly detection and monitoring)



REACH OUT THE PROJECT


- Find us: www.energy-shield.eu
- Subscribe for Newsletter
- Follow us: @EnergyShield_
- Join our LinkedIn group: EnergyShield
- Contact us: EnergyShield@siveco.ro
- Video presentation: <https://youtu.be/AtSUMkrp1Dw>
- Project Coordinator: SIMAVI
 - Otilia Bularca, Project Manager
 - E-mail: otilia.bularca@simavi.ro




ENERGY SHIELD
INTEGRATED CYBERSECURITY SOLUTION FOR THE
VULNERABILITY ASSESSMENT, MONITORING AND PROTECTION
OF CRITICAL ENERGY INFRASTRUCTURES

EnergyShield project aims at testing small-scale and large-scale disruption attack scenarios in a live cyber-defence exercise

- 01 ADAPT** available tools to support Electrical Power and Energy System (EPES) in fighting against cyber attacks
- INTEGRATE 02** the cybersecurity tools in a solution with assessment, monitoring protection and learning capabilities
- 03 VALIDATE** the practical value of the EnergyShield toolkit with EPES stakeholders
- DEPLOY 04** best practices, guidelines, methodologies and encourage the adoption of EnergyShield results

 This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement 852907

EnergyShield toolkit



DEVELOPING THE CYBER-TOOLKIT THAT PROTECTS YOUR ENERGY GRID

Italy - a small scale offline demonstrator focusing on DSO infrastructures.

Bulgaria - a city-level online demonstrator analyse cyber security risks related to the cyber supply chain.


EnergyShield in a nutshell

Grant Number: 832907
Type of action: Innovation Action
Grant: € 7,421,437.38

18 partners from 10 countries
Duration: 01/07/2019 - 30/06/2022

Find us: www.energy-shield.eu
Follow us: @EnergyShield_
Join our group: EnergyShield

Contact us: EnergyShield@siveco.ro





ENERGY SHIELD

THANK YOU!



This project has received funding from the European Union's H2020 research and innovation programme under the grant agreement No. 832907