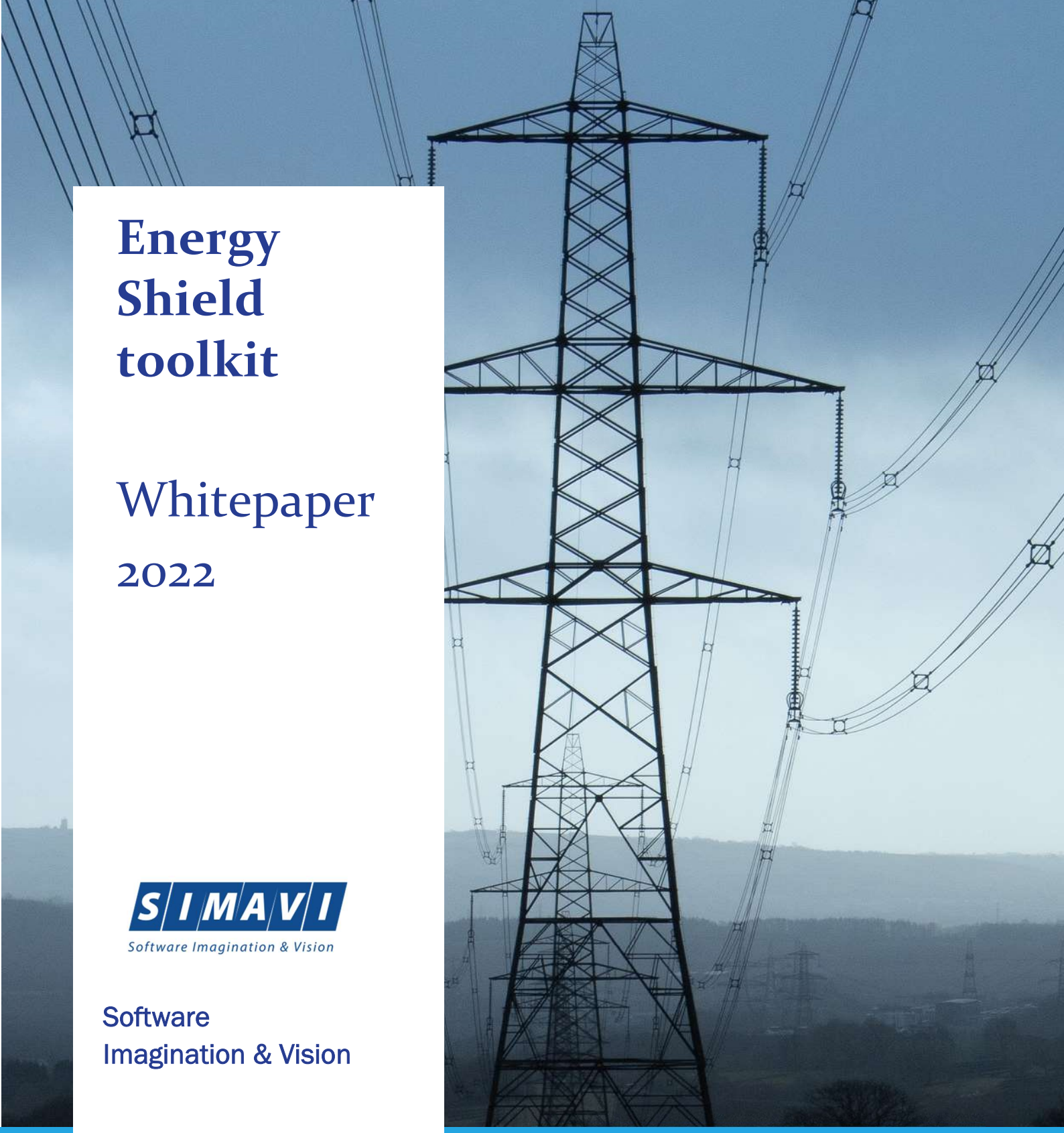


Energy Shield toolkit

Whitepaper 2022

SIMAVI
Software Imagination & Vision

Software
Imagination & Vision

Authored by:
Iacob Crucianu,
Lavinia Dincă,
Ana-Maria Dumitrescu

ENERGY SHIELD

EnergyShield toolkit

IN A NUTSHELL

The EnergyShield toolkit is defined as the common platform where different tools developed and adapted as part of the project are integrated.

The EnergyShield toolkit is organized in several "shelves" or "drawers" and contains: hardware components, software components, and communication ports. The toolkit is accessible through an authentication mechanism and is prepared to be placed in an OT environment with existing security mechanisms.

The toolkit aims at accommodating EnergyShield tools in a common environment in terms of component installation, deployment, and print screens from the integrated system, the data flow mechanism and message exchange.

"

Integration is a critical tool in our arsenal, that depicts different district tools working together.

Lavinia Dinca, SIMAVI

CONTEXT

Taking over the architectural design of the tools, the current paper demonstrates how the subsystems interact among themselves and/or with external actors (input providers, output receivers, and affected objects).

Designed as a prerequisite for the EnergyShield demonstrator, the toolkit integrates information from all technology providers and pilot leaders through the steps to be taken toward integration. The effort was focused mainly on the technical aspects of the toolkit, but it also identifies challenges and limitations on an operational and business levels, along with facing the upcoming activities. Each tool was assessed by considering the information that it could export, how data could be exchanged and what input information is used by each tool. Then, the focus was on the placement of components on the system platform, and on the way the components are exchanging information towards reaching the main goals of the EnergyShield

system. Details about the EnergyShield components installation, deployment, and print screens from the integrated portal are included in next sections.

The integration of tools via the common platform (EnergyShield toolkit) is detailed in the following together with the benefits of the toolkit. The toolkit is now able to use the individual component's outputs separately but is also placed in a common environment where they are collaborating to increase the value of the system and offer high levels of security when applied to the OT systems.

TECHNICAL DETAILS

The common software platform used by the EnergyShield demonstrator is the main output of the project. The common platform is implemented on a cloud environment hosted by SIMAVI, on a Linux machine that hosts two major groups of components:

- Standalone components like Kafka, and PostgreSQL.
- Docker containers (Keycloack, and all the other specific modules).

The common platform is developed according to the specifications outlined as part of the initial work and defines the proposed architecture.

The toolkit is organized in several "shelves" or "drawers" and contains hardware components, software components, and communication ports. The toolkit is accessible through an authentication mechanism.

The shelves are grouped in General common component and specific components.

The General common component refers to basement hardware shelf. Contains power supplies, cables, and measurement units.

The basement software shelf contains the Operating system, Java RunTime, and virtualization mechanism, serving all the software components. In this case, it is Linux running VMware system and running Java 1.8 and JEE.

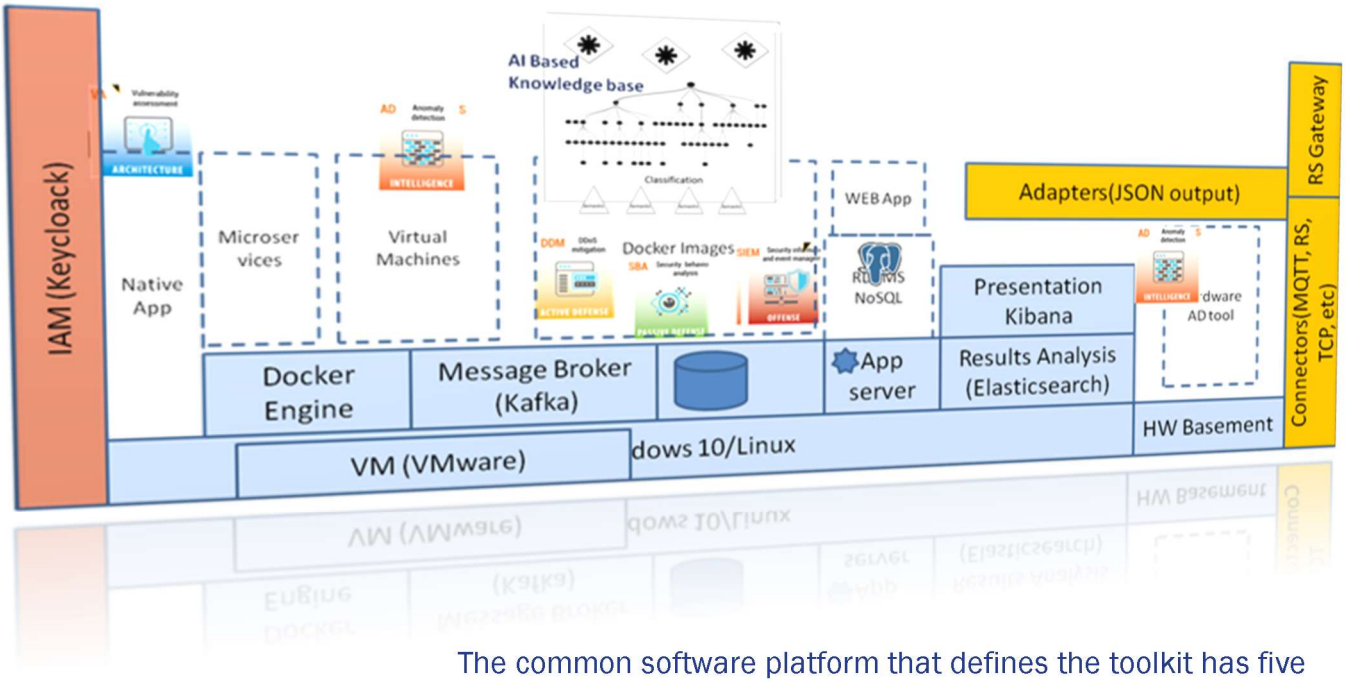
The container Manager is a software component. It runs a container engine (Docker), where all docker images can be run.

The communication HUB is a software component. It runs a message broker (Kafka) and communication bus for REST services.

The persistence is formed of software components used for data persistence. They can be RDBMS (Postgres) databases and NoSQL (Cassandra).

The application servers include software components (WEB App server like Apache Tomcat).

The presentation tools are software tools used to display data in a format required by end-users. Kibana is one example.



The common software platform that defines the toolkit has five different deployment areas:

- Assessment provides information on the most critical attack vectors. It includes Vulnerability Assessment (VA) modules and Security Behaviour Analysis (SBA) tools.
- Monitoring and protection provide early warning on incoming attacks and malware. It includes Anomaly Detection modules and Distributed Denial of Service mitigation modules.
- Learning and sharing collect information from all the other modules and create plans and instruction which refers to SIEM.
- Framework components are supporting components used by the whole deployment. They include container engine, Authentication and Authorization, Communication system, REST, and Process management.
- Deployment system. It implements a Continuous Integration/Continuous Deployment (CI/CD) mechanism based on GitLab
- The platform is prepared to be placed in an OT environment with existing security mechanisms. Information regarding the inclusion of existing security mechanisms will be included in forthcoming versions when the system will be tested in real environments.

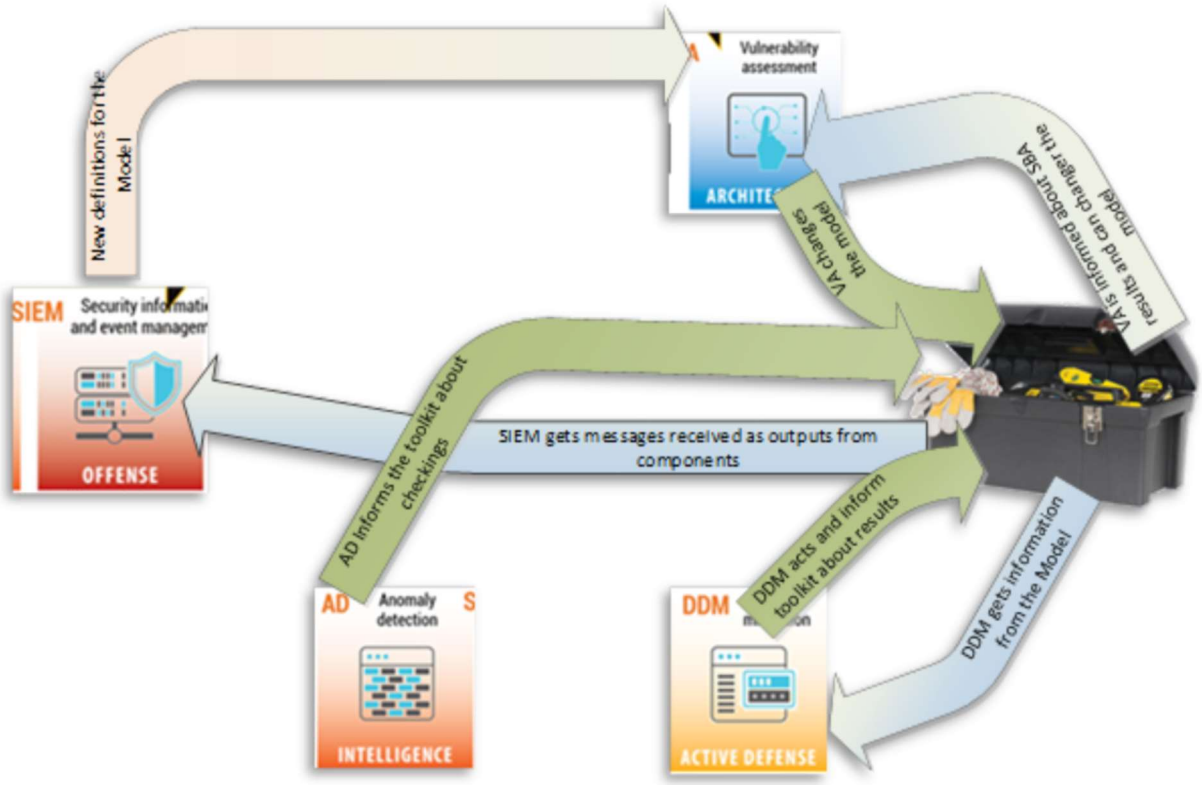
ENERGYSHIELD DEMONSTRATOR

The tools developed and used in the project were created to work separately, but also to cooperate and enrich their value. This is possible by defining a data exchange mechanism, composed of

data structures, and defined data flow in the system. Considering the architecture of the components, the most suitable way of data exchange is based on asynchronous message exchange. This is implemented by using Kafka broker.

Messages will be in a uniform JSON format. Each component will send data on a topic and will explore to read some other topics. This implementation follows the architectural pattern of "Choreography" with a very loose coupling of components, and with the possibility to dynamically increase the module data exchange.

Messages are exchanged asynchronously, in a publish-subscribe model. Each component publishes messages on specific topics. Also, each component subscribes to specific topics.



The flow of messages is as presented in the following. VA, SBA, AD, and DDoSM will produce messages based on the processing of data they refer to, and they prepare such data, especially for the SIEM tool. VA, AD, and DDoSM are subscribers of the SIEM tool, from where they collect feedback. SIEM tool reads data from VA, SBA, AD, and DDoSM and produces outputs for VA, AD, and DDoSM components. While some tools expect data from external sources or other tools in the toolkit, there are cases when data is coming directly from the user (e.g., SBA is mainly a user-driven tool and is not interacting directly with the rest of the tools). SBA only expects inputs from users.

EnergyShield Portal is the place where there is a single point of access to the toolkit. It displays the data available from individual components, considering that the components might be

deployed in the same place as the portal or they are deployed on pilot premises, from where information is offered via a secured line and according to the security policy implemented by a pilot. The Portal is enabled to take advantage of using the outputs of components running as services. There is no direct interaction between the common platform or the portal with the environment where the Operational System is working. There are communication links between the technical components of the toolkit deployed on-premises, and the common framework and the portal.

The portal is also the place where the results of the event fusion system are run and where the results are presented. The event fusion mechanism is the central added value for the integrated toolkit, as it offers a global view of the system as a whole. Only authenticated users have access, and the access is strictly monitored and is based on the security policy defined in each site (pilot site).

BEST PRACTICES & LESSONS LEARNED

The whole process of developing the EnergyShield toolkit presented several challenges we have addressed, through close cooperation between partners, and by the usage of the best suited available technologies. Both pilots have a very complex OT infrastructure. It is already protected by an important security mechanism, and the access was limited to specific areas. We have addressed the access to OT infrastructure by designing and implementing a federated architecture, with tools having the possibility to address specific areas of the system.

The OT infrastructure presented in the pilots defined what type of protocols and systems could be used. Each tool provider was focused of the best software components for the tools they have developed. Covering a wide area of business and functions, the tools were from very different areas, and finally, the integration process was a big issue. We have addressed this from the very beginning of the project when we have defined the software architecture. The establishment of standards and protocols, the usage of message broker with well-defined topics allow us to address these challenges.

The cybersecurity is a very dynamic area of IT. This aspect was addressed by using last version of software modules available, and by creating an open ecosystem, based on API, where new modules could be plugged in.

The integration process presented several challenges for the integrator and refer to: (i) An important number of modules were created for the system; (ii) A wide area of technologies used to develop the components; (iii) Different business aspects of the functionality (from behavior analysis to anomaly detection and monitoring); (iv) Component providers spread in several locations; (v) Cultural and language barriers.

DISSEMINATION & COMMUNICATION

Dissemination **events**:

- SU-DS04-2018-2020 – Workshop: “Bridging three H2020 EU projects, EnergyShield, PHOENIX and SDN-microSENSE, all funded under the SU-DS04-2018-2020 programme and, consequently, sharing the same goals and vision towards Cybersecurity in the Electrical Power and Energy System (EPES)”
- CyberWatching - Webinar: "EPES and Smart GRIDS: practical tools and methods to fight against cyber and privacy attacks" (https://cyberwatching.eu/epes-and-smart-grids-practical-tools-and-methods-fight-against-cyber-and-privacy-attacks)
- EnergyShield Workshop: “Trends, opportunities and choices in designing a cyber resilient EPES infrastructure”
- 2nd International Workshop on Cyber-Physical Security for Critical Infrastructure Protection (CPS4CIP 2021), collocated with the 26th European Symposium on Research in Computer Security (ESORICS) 2021
- 2nd ESCI-workshop CyberKit4SME Synergy was to create a collaborative environment across similar
- 2nd ECSCI Workshop on Critical Infrastructure Protection CIP. The focus of the presentation was on how stakeholders could shield the power grid from cyberattacks.
- “Trends in Managing Current Security and Predictive Maintenance Challenges in Smart Energy Grids in Romania”, arranged by the Bucharest Electrical Engineering Faculty.
- Critical Infrastructure Protection & Resilience Europe 2022 at the Parliament Palace in Bucharest.
- Final event “Building upon cyber resilience in energy sector” on the 23rd of June 2002.

ABOUT THE COMPANY

SOFTWARE IMAGINATION & VISION (SIMAVI) is an IT company established in 2019, following the division process of SIVECO Romania SA. Although the company was recently established, the team's experience is vast, taking over all software development activities in education, health, customs, nuclear, business, banking, utilities, production, etc.

An organization built on a European model, with unique competence centres and internationally competitive specialists, SOFTWARE IMAGINATION & VISION is the Romanian software company that provides IT services directly to European Commission organization.

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

Website: www.energy-shield.eu **Twitter**: @EnergyShield_
LinkedIn Group; https://www.linkedin.com/groups/8831159/
Youtube channel: https://www.youtube.com/channel/UCtNRIf0uXvDsxVCSo1NfF_Q
E-mail: EnergyShield@siveco.ro