ENERGY SHIELD

Integrated Cybersecurity Solution
for the Vulnerability Assessment, Monitoring and Protection of
Critical Energy Infrastructures

INNOVATION ACTION

H2020 Grant Agreement Number: 832907

W6 FIELD TRIALS

D6.3 – FIELD TRIAL EVALUATION SUMMARY REPORT

Document info	
Contractual delivery	**30/06/2022**
Actual delivery	**05/09/2022**
Responsible Beneficiary	**KTH**
Contributing beneficiaries	**all**
Version	**2.0**

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

DOCUMENT INFO

Document ID:	D6.3
Version date:	05/09/2022
Total number of pages:	81
Abstract:	This task evaluates the performance of the EnergyShield solution and provides feedback to improve it. • DESIGN phase: after analysing a system architecture, the vulnerability assessment tool will provide proactive redesign suggestions i.e., proactively suggest how to improve the architecture to get the most favourable cost-benefit ratio. Today this is analysis is done manually by the user. The task will create functionality as well as methodologies for automated design support i.e., provide suggestions for how to improve the architecture to improve security in the most cost-effective way. • OPERATION phase: the EPES end-users (practitioners) will assess the results of the pilots, verify the expected outcomes, and develop guidelines on how to optimize the use of the EnergyShield solution. The evaluation output should cover (among other areas) usability, flexibility and accuracy of expected results and will include a set of recommendations on how to improve further the EnergyShield solution, and a set of guidelines on how to maximize its usage. Detailed gap analyses intrinsic to specific infrastructure and assessments of current security systems, technologies and processes and other security solutions will be classified EU RESTRICTED (RES-EU), which is the case for the red team evaluation report. The read team report will describe how well each critical infrastructure can withstand a targeted attack and how well its critical assets are protected with the EnergyShield solution. The results yield will yield into how potential vulnerabilities can affect business continuity and how they can be effectively remedied.
Keywords	Bulgarian pilot, field trial, Italian pilot, offline, small-scale

AUTHORS

Name	Organisation	Role
İsmail Bütün	KTH	Overall Editor
Robert Lagerström	KTH	Manager Editor
José Eduardo Urrea Cabus	KTH	Section Editor
Serale Gianluca	IREN	Contributor
Magda Zafeiropoulou	SC	Contributor
Anna Georgiadou	NTUA	Contributor
Ariadni Michalitsi - Psarrou	NTUA	Contributor
Iosif Sklavidis	KT	Contributor
Christos Angelidis	KT	Contributor
Yisrael Gross	L7 Defense	Contributor

REVIEWERS

Name	Organisation	Role
Magda Zafeiropoulou	SC	Overall Reviewer
Anna Georgiadou	NTUA	Overall Reviewer
Ana Maria Dumitrescu	SMAVI	Overall Reviewer
Lavinia Dinca	SIMAVI	Overall Reviewer
Otilia Bularca	SIMAVI	QA Reviewer

VERSION HISTORY

0.1	13/05/2022	Table of Content release
0.2	17/06/2022	Including contributions from pilot leaders
0.3	17/06/2022	Overall review
0.4	28/06/2022	QA review
0.5	03/07/2022	QA review
1.0	06/07/2022	Final version released to EC
1.1 – 1.5	01/09/2022	Re-work
2.0	05/09/2022	version

EXECUTIVE SUMMARY

This report summarises the activities performed by the EnergyShield consortium partners to solution packages deployed to demonstrate the impact of the technologies developed during the project and evaluates the performance of the EnergyShield solution and provides feedback to improve it. The Pilot's goal was to assess the most effective solutions (hardware and software options, organisational approaches, changes in procedures, and staff qualification in this field) for dealing with malicious cyber-attacks on EPES Distribution System Operators (DSOs).

A two phase approach was followed to demonstrate the impact of technologies:

- **DESIGN phase**: after analysing a system architecture, the vulnerability assessment tool provides proactive redesign suggestions i.e., proactively suggest how to improve the architecture to get the most favourable cost-benefit ratio. The task created functionality as well as methodologies for automated design support i.e., provide suggestions for how to improve the architecture to improve security in the most cost-effective way.
- **OPERATION phase**: the EPES end-users (practitioners) assessed the results of the pilots, verified the expected outcomes, and developed guidelines on how to optimize the use of the EnergyShield solution. The evaluation output covers usability, flexibility and accuracy of expected results includea a set of recommendations on how to improve further the EnergyShield solution, and a set of guidelines on how to maximize its usage.

Also, the EnergyShield's D6.3explores the project results and developing an ecosystem of partners along the value chain to guarantee a sustainable impact of the project upon completion. All consortium partners of the EPES value chain validated the technology and disseminated the project results to their industry. The results yield will yield into how potential vulnerabilities can affect business continuity and how they can be effectively remedied.

The direct beneficiaries of the improvements proposed via the EnergyShield project are the European energy generators, transmission (TSO), and distribution (DSO) operators, as well as the final consumers. The results of the research and innovation activities performed as part of the EnergyShield project have been shared with stakeholders via 18 publicly available reports and 31 scientific articles during the project lifetime.

TABLE OF CONTENTS

EXECUTIVE SUMMARY 4
Table of Contents 5
List of figures 7
List of tables 8
Acronyms 9
1. Introduction 10
1.1. Scope and objectives 10
1.2. Structure of the report 10
1.3. Task dependencies 11
2. EnergyShield tools technical definitions 12
2.1. EnergyShield tools' Concepts and objectives 15
2.1.1. Italian pilot 15
2.1.2. Bulgarian pilot 15
3. Evaluation KPIs for the ToolKit and the Tools 17
3.1. Vulnerability Assessment Tool 17
3.1.1. VA tool technical details 17
3.1.2. VA tool demonstrator 18
3.1.3. VA tool best practices and lessons learned 24
3.2. Security Behaviour Analysis Tool 25
3.2.1. SBA tool technical details 25
3.2.2. SBA tool demonstrator 27
3.2.3. SBA tool best practices and lessons learned 40
3.3. Anomaly Detection Tool 41
3.3.1. AD tool technical details 42
3.3.2. AD tool demonstrator 43
3.3.3. AD tool best practices and lessons learned 48
3.4. Distributed Denial of Service Mitigation Tool 49
3.4.1. DDoSM tool technical details 49
3.4.2. DDoSM tool demostrator 50
3.4.3. DDoSM best practices and lessons learned 61
3.5. Security Information and Event Management Tool 61
3.5.1. SIEM technical details 62

3.5.2. SIEM tool demostrator 63
3.5.3. SIEM tool best practices and lessons learned 68
3.6. TOOLKIT 69
3.6.1. TOOLKIT technical details 69
3.6.2. TOOLKIT demostrator 70
3.6.3. TOOLKIT best practices and lessons learned 75
4. Conclusion 77
4.1. challenges and limitation 77
5. References 79

LIST OF FIGURES

Figure 1. Italian Pilot overview applications 15
Figure 2. Bulgarian Pilot overview applications 16
Figure 3. VA architecture 17
Figure 4. SBA tool architecture 26
Figure 5. SBA tool roadmap 27
Figure 6. AD tool overview 42
Figure 7. Proposed tiered model 53
Figure 8. Updated AMI simulator 54
Figure 9. Registrations behaviour on a PLC (2) in the simulator with no attacks 54
Figure 10. Registrations behaviour on a PLC (1) in the simulator with FET attack 55
Figure 11. Compromised populations from simulator outputs 55
Figure 12. Compromised populations estimated by model 56
Figure 13. Compromised populations from simulator outputs (close-up) 56
Figure 14. Compromised populations estimated by model 57
Figure 15. SIEM tool architecture 62
Figure 16. SIEM tool architecture in Pilot 63

LIST OF TABLES

Table 1. Tool Quality Model Categories 13
Table 2. VA Bulgarian Pilot KPIs results 19
Table 3. SBA Bulgarian Pilot KPIs results 28
Table 4. SBA Italian Pilot KPIs results 35
Table 5. AD Italian Pilot KPIs results 44
Table 6. Attack types overview 48
Table 7. DDoSM Bulgarion pilot KPI results 57
Table 8. SIEM Bulgarian pilot KPI results 64
Table 9. Toolkit Bulgarian pilot KPI results 71

ACRONYMS

ACRONYM	DESCRIPTION
AF	Automated Forensic
CEZ	CEZ Distribution Bulgaria
CITY	City University London
CoTTP	Cogen Zagore Ltd
CSC	Cyber Security Culture
D	Deliverable
DIL	D I L DIEL Ltd aka Goldline
DSO	Distribution System Operator
EPES	Electrical Power & Energy Systems
ESO	Bulgarian Electricity System Operator EAD
EUW	European Utility Week
FOR	foreseeti AB
HE	Homomorphic Encryption
IREN	IREN S.p.A.
KPI	Key Performance Indicator
KT	Konnekt-able Technologies
KTH	KTH Royal Institute of Technology
L7D	L7Defense
M	Month
MIG	MIG 23 Ltd
NTUA	National Technical University of Athens
PSI	PSI Software AG
R&D	Research and Development
SBA	Security Behaviour Analysis
SC	Software Company Limited
SIGA	Si-Ga Data Security Ltd
SIV	Software Imagination & Vision Romania
T	Task
TEC	Tech Inspire Limited
TSO	Transmission System Operator
VETS	VETS Lenishta OOD
WP	Work package

INTRODUCTION

1.1. SCOPE AND OBJECTIVES

The objective of this deliverable is to illustrate the outcomes of the EnergyShield solution packages deployed to demonstrate the impact of the technologies developed during the project on three different use cases. The Pilot's goal was to assess the most effective solutions (hardware and software options, organisational approaches, changes in procedures, and staff qualification) for dealing with malicious cyber-attacks on Distribution System Operators (DSOs) and the EPES sector. The purpose of the evaluation is to demonstrate how effective the EnergyShield solution is at fending off threats on next-generation power grids, also known as SmartGrids. The demonstrators (Pilots) made every effort to test and assess the created tools and the toolkit in settings that were as close to real-world implementations.

This task assesses the performance of the EnergyShield solution and provides suggestions for improvement. The report provides a summary of the EnergyShield solution package deployed to demonstrate the impact of the technologies developed during the project on three different use cases. The field trials began with a three-month pre-pilot (M15-M17) in which practitioners tested individual tools (with limited integration) to provide early feedback to tool developers and the system integrator. The full-scale pilots then completed a 3-month setup phase (M22-M24), a 9-month operational phase (M25-M33), and a final 3-month report production phase (M34-M36). The goals of this work package were to: implement the field trials (task 6.1); and evaluate the field trial results (task 6.2). The findings demonstrated how potential weaknesses can impact business continuity and how they can be effectively addressed.

1.2. STRUCTURE OF THE REPORT

The tasks of evaluating the performance of the EnergyShield solution and providing feedback to improve it are covered in the report's two main parts, which are structured into separate but related sections.

The first part, which also includes a list of the partners and pilots involved, covers the benchmarking phase. It also includes the list of the predetermined KPIs for EnergyShield Project tools and the toolkit architecture while also effectively enhancing security. It sets up the technical and economic key performance indicators (KPIs) that were used to evaluate and compare the chosen solutions.

The second part of the report includes the operation phase, which is where the EPES end-users (practitioners) evaluated the pilot results, confirmed the expected outcomes, and developed guidelines for optimising the use of the EnergyShield solution. A discussion about the KPIs that were used while the assessments were being conducted is provided.

Lastly, the report concludes with the outcomes of the EnergyShield solution packages deployment at the end of the reporting period.

1.3. TASK DEPENDENCIES

WP6 Field Trials focuses on the work package (tools and toolkit) that deploys the EnergyShield platform to demonstrate the impact of the technologies developed throughout the project on three distinct use cases. Summarizing the results of the field trial implementation **[ESH61]** (confidential) and evaluating the field trial results **[ESH62]** (EU-R).

ENERGYSHIELD TOOLS TECHNICAL DEFINITIONS

EnergyShield is a defensive toolkit that takes into account the requirements of operators of Electrical Power and Energy Systems (EPES) and combines the most recent advancements in technologies for vulnerability assessment, supervision, and protection. In this section, the technical and economic evaluation KPIs to evaluate and benchmark the identified solutions are defined. The practitioners validated the toolkit in specific use case scenarios (pilots) designed to replicate their operations. All modules were deployed on a test infrastructure representative of a production environment, and penetration testing experts were contracted to test the infrastructure in order to compare their vulnerability and resilience to attacks. The first evaluation is related to each tool and the combination of them. Then the framework is evaluated in two phases:

- **Phase 1**: Baseline includes assessing technical performance such as mitigation time (practitioners) and security architecture (practitioners). After analysing the system architecture, the vulnerability assessment tool offers proactive redesign recommendations, or suggestions for how to make the architecture better to achieve the best possible cost-benefit ratio. The user performs this analysis today manually. The task entails developing methodologies and functionality for automated design support, i.e., offering advice on how to upgrade the architecture in the most affordable manner to increase security.
- **Phase-2**: The end-users (practitioners) of EPES evaluate the pilot results, confirms the intended outcomes, and create guidelines for maximizing the application of the EnergyShield solution. The evaluation output includes a set of recommendations on how to further improve the EnergyShield solution, as well as a set of guidelines on how to maximize its use. It covers usability, flexibility, and accuracy of expected results. Evaluation by applying the tools and assessing technical performance such as security architecture improvement (practitioners), mitigation time (practitioners), detection performance (tool kit), flexibility (tool kit), accuracy (tool kit), as well as assessing the economic performance, e.g., usability (tool kit) and security (pentesting of toolkit).

The Evaluation Framework has been completed through the collaboration of KTH and NTUA, and all technology providers were requested to fill-in this list of KPIs. The criteria for evaluation place an emphasis on flexibility (F), usability (U), and accuracy (A). The foundation for the framework is settled out in the form of scientific recommendations drawn from a variety of sources. **[EDE06]** and **[TER00]** are just two examples of these recommendations. Then, there are nine primary categories, each of which is further subdivided into categories.

1. Functional suitability – flexibility (F)
2. Performance efficiency
3. Compatibility (F)

4. Usability (U)
5. Reliability
6. Security
7. Maintainability (F)
8. Portability (F)
9. Accuracy (A)

The end-users of EPES, also known as practitioners, evaluated the results of the pilots, verified that the expected outcomes occurred, and developed guidelines for how to make the most of the EnergyShield tools. The outcome of the evaluation covered (among other topics) usability, flexibility, and accuracy of expected results. Additionally, it included a set of recommendations on how to improve the EnergyShield solution as well as a set of guidelines on how to make the most of its utilisation. A list of the Tool Quality Model Categories KPIs for the EnergyShield Project tools and the toolkit is presented in Table 1.

Table 1. Tool Quality Model Categories

Sub-characteristics	Definition
Functional suitability	
Functional completeness	Degree to which the set of functions covers all the specified features and user objectives.
Functional correctness	System provides the correct results with the needed degree of precision.
Functional appropriateness	The functions facilitate the accomplishment of specified tasks and objectives.
Performance efficiency	
Time behaviour	Response, processing times and throughput rates of a system, when performing its functions, meet requirements.
Capacity	Degree to which the maximum limits of a product or system parameter meet requirements.
Compatibility	
Co-existence	Product can perform its functions efficiently while sharing environment and resources with other products.
Interoperability	A system can exchange information with other systems and use the information that has been exchanged.
Usability	
Appropriateness recognizability	Degree to which users can assess whether a product or system is appropriate for their needs.
Learnability	Degree to which a product or system can be used by specified users to achieve specified goals of learning to use the product or system with effectiveness, efficiency, freedom from risk and satisfaction in a specified context of use.
Operability	Degree to which a product or system has attributes that make it easy to operate and control.

User error protection	System protects users against making errors.
Accessibility	System can be used by people with the widest range of characteristics and capabilities.
Reliability	
Maturity	System meets needs for reliability under normal operation.
Availability	System is operational and accessible when required for use.
Fault tolerance	System operates as intended despite the presence of hardware or software faults.
Recoverability	Degree to which, in the event of an interruption or a failure, a product or system can recover the data directly affected and re-establish the desired state of the system.
Security	
Confidentiality	System ensures that data is accessible only to those authorised to have access.
Integrity	System prevents unauthorised access to, or modification of, computer programs or data.
Non-repudiation	Actions or events can be proven to have taken place, so that the events or actions cannot be repudiated later.
Accountability	Degree to which the actions of an entity can be traced uniquely to the entity.
Authenticity	The identity of a subject or resource can be proved to be the one claimed.
Maintainability	
Modularity	System is composed of components such that a change to one component has minimal impact on other components.
Reusability	An asset can be used in more than one system, or in building other assets.
Modifiability	Degree to which a product or system can be effectively and efficiently modified without introducing defects or degrading existing product quality.
Testability	Effectiveness and efficiency with which test criteria can be established for a system.
Portability	
Adaptability	Degree to which a product or system can effectively and efficiently be adapted for different or evolving hardware, software or other operational or usage environments.
Installability	Effectiveness and efficiency with which a system can be successfully installed and/or uninstalled.
Accuracy	
Sufficiency	Degree to which data collected by the product can constitute a representative data set.
Coverage	Effectiveness and efficiency with which the product handles the data set collected.
Validity	Degree to which results produced by the product results deviate from real-life.

1.4. ENERGYSHIELD TOOLS' CONCEPTS AND OBJECTIVES

The EnergyShield project addresses both **small-scale** and **large-scale** disruption attack scenarios with an integrated toolkit, which was intended to be validated in a live cyber-defense exercise.

For attacks on a smaller scale, the following can be mentioned:

- Targeting specific organization
- Meant to prevent them from conducting business normally. For example, distributed denial of service and ransomware

For attacks on a larger scale, the following can be mentioned:

- Targeting the entire EPES value chain
- Meant to take down the energy supply services at regional or country level. For example, malware distribution and man-in-the-middle attacks

1.4.1. ITALIAN PILOT

The purpose of the Italian Pilot is to evaluate the most effective solutions (hardware and software solutions, organizational approaches, changes in the procedures and qualified the staff in this field) to face malicious cyber-attacks, see Figure 1.The Italian Pilot scenarios are presented as follows: Testing the Security Behaviour Analysis tool; Perform a feasibility study on integration of the Anomaly detection tool on its specific SCADA system.

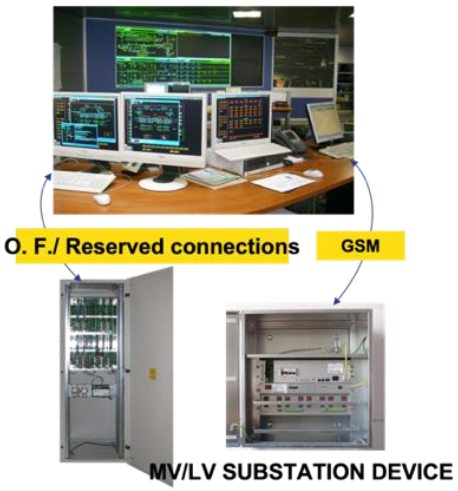

Figure 1. Italian Pilot overview applications

1.4.2. BULGARIAN PILOT

The purpose of the Bulgarian Pilot is to determine which methods are the most successful in preventing, detecting, and mitigating the effects of malicious cyber-attacks, see Figure 2. The Bulgarian Pilot scenarios are presented as follow: Attacks

on Substation Infrastructure; Attacks on Consumer / Prosumer networks points. Additional information regarding the pilot's description, scenario presentations, tool assessments, and results is presented in sections 0 and **Error! Reference source not found.**.

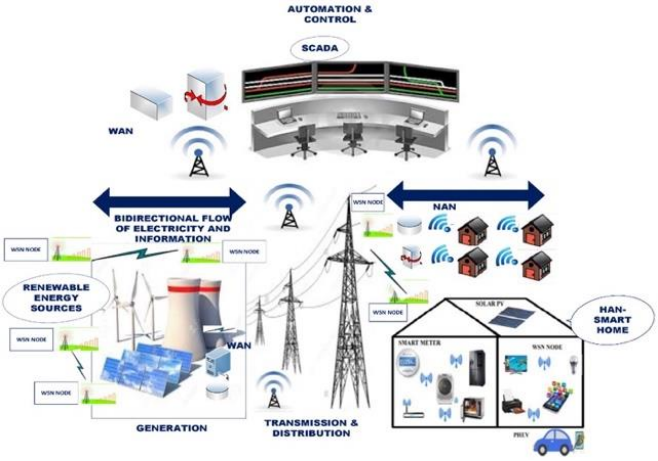

Figure 2. Bulgarian Pilot overview applications

EVALUATION KPIS FOR THE TOOLKIT AND THE TOOLS

This section provides an overview of the KPI results obtained from the EnergyShield tool applications that have been discussed in the preceding section.

1.5. VULNERABILITY ASSESSMENT TOOL

The Vulnerability Assessment (VA) module includes both software that integrates a vulnerability assessment tool based on Foreseeti's SecuriCAD tool as well as a threat model that includes attack vectors and probabilities. The threat modelling and attack simulation approach makes use of a model of an environment which is used to run attack simulations on. In other words, a digital twin or offline clone of the environment is created, allowing for attack simulations using a virtual attacker, which means that the method is non-intrusive by nature.

1.5.1. VA TOOL TECHNICAL DETAILS

The purpose of creating a model of an architecture or a live environment is to be able to run attack simulations on that model. The attacker is given a starting point, defining the initial attack vector, and the simulation engine then calculates and presents the expected path the attacker will follow within the model. This is possible since the modelling language/objects contain logic regarding which attacker operations are expected to lead to different achievements, which in turn make further operations possible. Some operations are a direct effect of previous achievements, while others require additional effort or are not guaranteed to be successful depending on the status of the objects in the model. In Figure 3, all blue and green boxes are components that are part of the VA tool, and the white and grey boxes symbolize other related tools such as the MAL compiler. The SDK boxes represent the possibility to create arbitrary integration and automation logic.

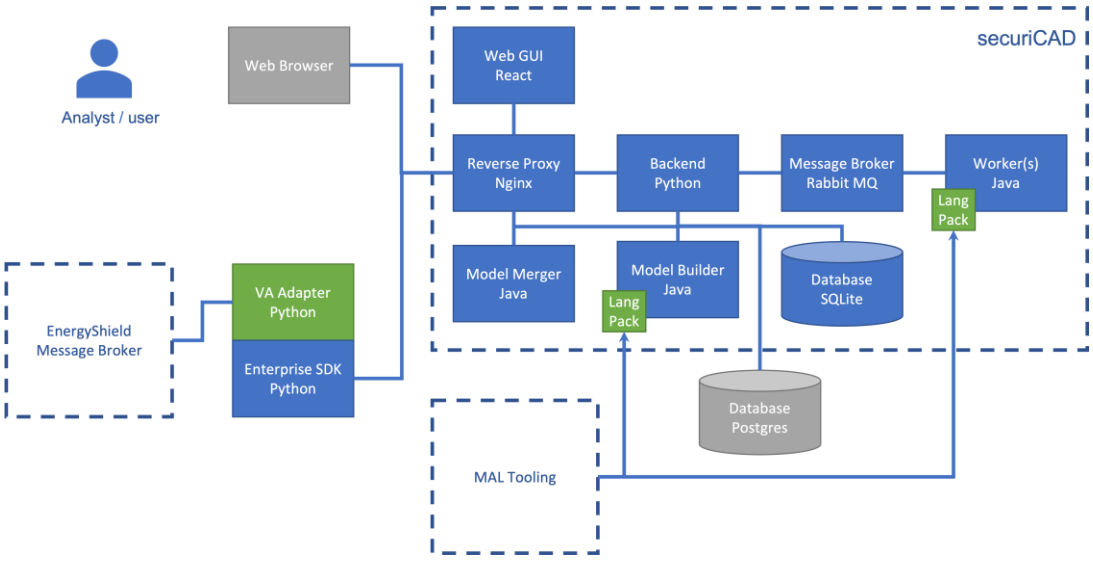

Figure 3. VA architecture

1.5.2. VA TOOL DEMONSTRATOR

Access to the VA tool is made possible by the Demonstrator, an online platform. The installation is a whole VA tool with a demonstrator model based on the cyberattack against Ukraine in 2015. This model, which was created using publicly available details from an attack, can be thought of as a condensed, smaller version of the EPES domain system. The utility can be accessed online and is hosted in the Sweden area of Amazon AWS. Given the cost associated with maintaining the demonstrator, foreseeti may choose to run it exclusively during central European business hours or, if usage is extremely low, only start it when requested in order to minimize costs. Furthermore, because the hardware configuration of the VA tool demonstrator system is constrained, only small to moderately sized models may be simulated. The VA tool is installed alongside the other EnergyShield tools in a stand-alone fashion. In the demonstrator set-up, the tools were installed on the same server. Communication between the tools, like VA, SBA, SIEM and the Dashboard, is carried out via different message queues based on the Kafka application. The approach is that once a tool has new information to share with other tools or publish on the Dashboard, it posts it in a related Kafka queue. The other tools who will use the information will then listen to new messages being posted on the relevant queues. One such example is that the SBA tool posts a message to a queue once a campaign is completed. The VA tool listens to that queue, fetches new campaign information using the VA tool's APIs, updates the model in the VA tool, runs a simulation, and posts the results to a different Kafka-queue which the Dashboard, in turn, is listening to, see Table 2 which contain the KPIs results from the VA tool application.

- **Demonstrator environment analysis**: A model was created to represent the demonstrator environment. This model was created with inspiration from high-level information provided by the Vets company combined with Foreseeti's experience from similar (SCADA/ICS) environments within the power distribution and generation industry. This model was then used for running attack simulations on.
    - The impact of updating security-related model parameters with collected values was inspected. For this purpose, the security awareness parameter of the user groups "regular users" and "administrators" in the model was used. When updating the model's default value for security awareness, with data collected by the SBA tool, the simulated risk levels were impacted as expected. The security awareness of the regular users' group had a 10% impact on the risk level of critical assets in the model. For the administrators' security awareness level, the impact was 30%.
    - The security awareness information is only one parameter that can be collected by the SBA tool. Additional data points from the SBA tool, as well as other tools in the EnergyShield toolkit, can also be used to enrich the model.

- **Early Results:** The workflow described above has been confirmed to work as expected; A message on "New campaign data available" is posted by the SBA tool, the VA tool picks that notification up, connects to the SBA to fetch the actual findings/data (For instance, a new value for the Security Awareness parameter for the group of users participating in the campaign/survey), updates the information in the model, triggers a simulation, and puts a notification message about the updated simulation results on a different queue where the Dashboard is picking it up.
- **Implementation process**: The implementation is based on using a wrapper application that is subscribing/listening to messages on Kafka-queues. When messages arrive, it uses the SBA APIs to fetch the new campaign data and then uses the VA APIs to update a predefined model with the new campaign data and run a simulation. When the simulation is complete and new data is available, this information is published on a different queue where the Dashboard application can pick it up. During the development of the wrapper, the essential sources of information were the API documentation of the SBA tool, the VA tool, and the Kafka solution.

Table 2. VA Bulgarian Pilot KPIs results

Characteristic	Definition	Necessity	(F)lexibility (U)sability (A)ccuracy	Will assess	VA Bulgarian Pilot KPI	Recommended KPI value	Actual KPI value	Comments
FUNCTIONAL SUITABILITY								
Functional completeness	Degree to which the set of functions covers all the specified features and user objectives.	N		Y	(Intended added functionality / Implemented functionality) x 100	100%	100%	
Functional appropriateness	The functions facilitate the accomplishment of specified tasks and objectives.	N		Y	(Provided data sources / Supported data sources) x 100	>90%	100%	
PERFORMANCE EFFICIENCY								
Time behaviour	Response, processing times and throughput rates of a system, when performing its functions, meet requirements.	N		Y	Simulation time. (Before / After) x 100	100%	1167 %	For a model of 1.000 modeling objects before the EnegryShield project, the simulation time was one minute. After the project, a model of 11.670 objects simulated in

								also one minute.
					Graph generation time. (Before / After) x 100	100%	800%	Generating an attack path (graph) of a model used for benchmarking before the EnergyShield project required 90 seconds and after, the same attack path was generated in 12 seconds.
Capacity	Degree to which the maximum limits of a product or system parameter meet requirements.	N		Y	Improvement in maximum feasible model size. (Max before / Max after(x 100	100%	1500 %	The maximum feasible model size before was 1.500 objects and after it was 22.000 objects.
COMPATIBILITY								
Co-existence	Product can perform its functions efficiently while sharing environment and resources with other products.	Y	F	Y	Can VA operate in a shared environment?	YES	YES	
Interoperability	A system can exchange information with other systems and use the information that has been exchanged.	Y	F	Y	Can VA exchange information with the rest of the EnergyShield components and other IT corporate tools?	YES	YES	
USABILITY								
Appropriateness recognizability	Degree to which users can recognize whether a product or system is appropriate for their needs.	Y	U	Y	Combining externally provided data points with existing models to put the data points into architectural context.	YES	YES	
Learnability	Degree to which a product or system can be used by	Y	U	Y	Learning hours (Concept, basic modeling and	<40	30	On average, a regular customer-education on the VA

	specified users to achieve specified goals of learning to use the product or system with effectiveness, efficiency, freedom from risk and satisfaction in a specified context of use.				basic analysis)			tool requires 5 working days, 6 hours each.
Operability	Degree to which a product or system has attributes that make it easy to operate and control.	Y	U	Y	Number of integration configuration parameters	<5	4	The configuration parameters for the Kafka toolbox integration are credentials, connection path, queue name for incoming messages and queue name for outgoing messages.
User error protection	System protects users against making errors.	Y	U	Y	Does the whole VA tool crash on user errors?	NO	NO	
Accessibility	System can be used by people with the widest range of characteristics and capabilities.	Y	U	Y	VA tool is accessible and operational through different platforms	YES	YES	
				Y	VA tool is accessible and operational through different browsers	YES	YES	
RELIABILITY								
Fault tolerance	System operates as intended despite the presence of hardware or software faults.	N		Y	No. of Non-Critical Software Errors	<10	0	
SECURITY								
Confidentiality	System ensures that data is accessible only to those	N		Y	No. of incidents recorded	0	0	

	authorised to have access.							
Integrity	System prevents unauthorised access to, or modification of, computer programs or data.	N		Y	No. of incidents recorded	0	0	
Non-repudiation	Actions or events can be proven to have taken place, so that the events or actions cannot be repudiated later.	N		Y	No. of incidents recorded	0	0	
Accountability	Degree to which the actions of an entity can be traced uniquely to the entity.	N		Y	No. of incidents recorded	0	0	
Authenticity	The identity of a subject or resource can be proved to be the one claimed.	N		Y	Can you identify whether a logged in user is the one it claims to be?	YES	YES	
				Y	Can you identify whether a resource is the one it claims to be?	YES	YES	
MAINTAINABILITY								
Modularity	System is composed of components such that a change to one component has minimal impact on other components.	Y	F	Y	Is VA designed so that changes to data import, model generation, simulation engine and attack path visualization and reporting can be changed independently ?	YES	YES	
Reusability	An asset can be used in more than one system, or in building other assets.	Y	F	Y	Can VA be utilized in different business domains and application areas?	YES	YES	
Modifiability	Degree to which a product or system can be effectively and efficiently modified without introducing defects or	Y	F	Y	(No. of updates preformed without noticing operational problems) / (No. of updates performed)	>75%	100%	

	degrading existing product quality.							
Testability	Effectiveness and efficiency with which test criteria can be established for a system.	N		Y	Can sample models and known test input data be used to verify simulation results?	YES	YES	
PORTABILITY								
Adaptability	Degree to which a product or system can effectively and efficiently be adapted for different or evolving hardware, software or other operational or usage environments.	Y	F	Y	(No. of Total Errors recorded during Installations) / (Total No. of Installation Environments)	<1	0	
Installability	Effectiveness and efficiency with which a system can be successfully installed and/or uninstalled.	N		Y	(No. of Total Errors recorded during Installations) / (Total No. of Installations)	<1	0	
ACCURACY*								
Coverage	Effectiveness and efficiency with which the product handles the data set collected.	Y	A	Y	(Number of data points delivered to the tool / Number of corresponding asset types supported) * 100 %	100%	100%	
Validity	Degree to which produced by the product results deviate from real-life.	Y	A	Y	Regular Employee Security Awareness Score (SBA metric) impact on High Value Assets in a test model	>5%	10%	The model created for the pilot was used. The risk level of selected critical assets in the model were compared. The comparison was made with the users' security awareness parameter set to default (producing the risk level

								reference value) and with the users' security awareness levels set to the values collected by the SBA tool. The impact on critical assets was found to be 10%.
				Y	Admin Employee Security Awareness Score (SBA metric) impact on High Value Assets in a test model	>10%	30%	Equal to the description for regular users' security awareness level, the impact of the system administrators' security awareness was found to be 30% compared to the default value.

* *Accuracy refers to the closeness between the estimated value and the (unknown) true value that the statistics were intended to measure.*

1.5.3. VA TOOL BEST PRACTICES AND LESSONS LEARNED

Enriching a model with information on users, which the SBA tool is providing, and combining that information with a model is a very powerful combination, since information on "soft" assets are usually more difficult to gather than information on networks, assets, communication, and related security status. As mentioned briefly above, the simulations run by the VA tool are executed on a model that represents the environment to be simulated. This model can be created in different ways, from fully automated to fully manual. Early in the project, the possibility of automatically gathering information on a running environment was explored. However, due to confidentiality constraints, this turned out not to be an option. Instead, a model based on a provided architecture diagram was created manually. This is also a common and realistic approach to modelling an environment, particularly when it comes to critical infrastructure. In a more production-oriented deployment, however, there are multiple information-collection options available for generating and updating a model.

In terms of evaluation KPIs, the Bulgarian Pilot reports that the VA tool has been evaluated to achieve all the recommended KPI values. This information can be found in Table 2.

1.6. SECURITY BEHAVIOUR ANALYSIS TOOL

The Security Behaviour Analysis (SBA) tool has its foundations on the Cyber-Security Culture Framework which was developed in the context of the EnergyShield project. It was officially introduced in 2020 **[GEO20],** presenting an evaluation and assessment methodology of both individuals' and organisations' security culture readiness.

The specific framework is based on a combination of organisational and individual security factors structured into dimensions and domains. Its main goal is to examine organisational security policies and procedures in conjunction with employees' individual characteristics, behaviour, attitude, and skills. Each security metric introduced by the framework is assessed using a variety of evaluation techniques, such as surveys, tests, simulations, and serious games.

The assessment results are exploited in identifying cyber-security threats the organisation is vulnerable against. The framework has been correlated both with the hybrid MITRE ATT&CK Model for an OT Environment, consisting of a combination of the Enterprise and the ICS threat model **[GEA21]**, and with an enriched version of the Management and Education of the Risk of Insider Threat (MERIT) model **[GEO21]**, developed by the Secret Service and the Software Engineering Institute CERT Program at Carnegie Mellon University.

Based on the evaluation results and identified threats, several targeted recommendations, awareness training programs, seminars and free online games are introduced to both the decision-makers of the organisation as well as the individual employees and contractors.

A detailed presentation of the SBA tool, its objectives, scientific foundations, development iterations, architecture, implementation approach and application scenarios in a variety of different domains is contained in *D2.2 - Updated Security Culture Framework and Tool* [**ESH22**] and *D2.6 - Updated Security Culture Framework and Tool – Final Version* Error! Reference source not found.

1.6.1. SBA TOOL TECHNICAL DETAILS

The SBA tool has been designed, developed and implemented as a web application using a number of cut-edge technologies as presented in an overall architecture design in Figure 4. More specifically:

- ***Django***: a high-level open-source Python Web framework that encourages rapid development while offering the ability to quickly and flexibly scale. Its security features enforce applications' protection against common security issues, such as SQL injection, cross-site scripting, cross-site request forgery and clickjacking.
- ***PostgreSQL***: a powerful, open-source object-relational database system with a strong reputation for reliability, feature robustness, and performance. It is used to host the logical data structure behind the entire application, including

the security culture model and the representation of the evaluation methodology, along with its results and statistics.

- ***Web interface***: implemented using a combination of HTML, Bootstrap, CSS and JavaScript files to provide a user-friendly interface for all interacting actors of the tool.
- ***REST API***: a web interface allowing interaction of the SBA tool with the rest of the EnergyShield toolkit or with any other corporate operational system.
- ***Kafka Producer***: a Kafka client publishing messages to specific Kafka topics to inform listening parties (Kafka consumers) that new evaluation data have become available (e.g. at the end of an assessment campaign).

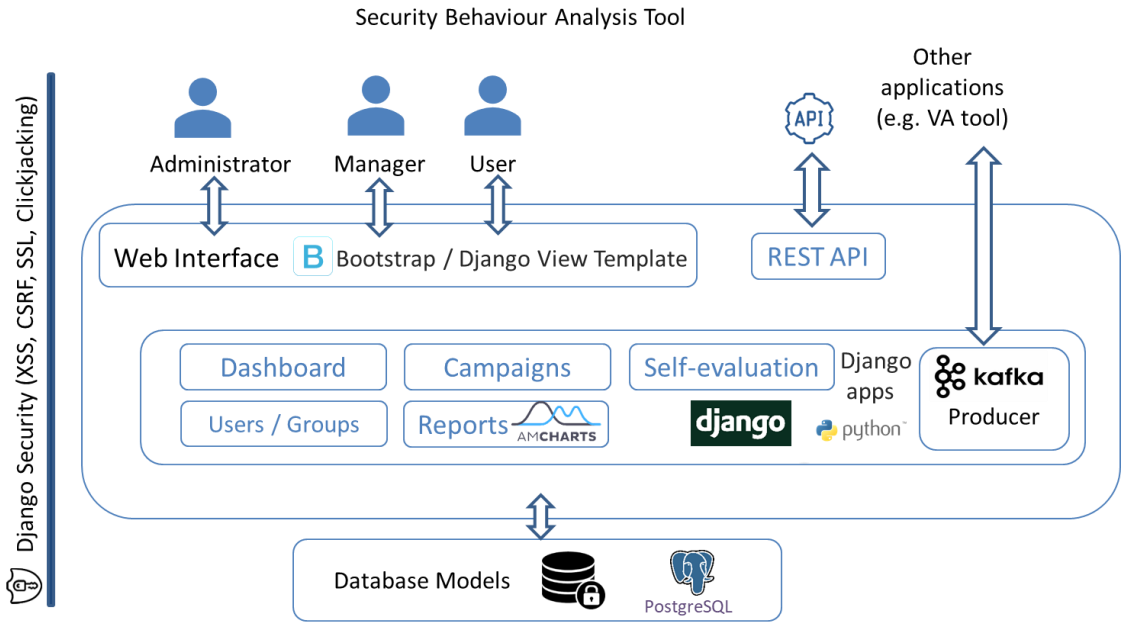

Figure 4. SBA tool architecture

SBA was designed, developed, tested and validated in 3 iterations, as with the rest of the EnergyShield toolkit components. Each iteration aimed to address specific functional and non-functional requirements, as described in T1.1 (technical requirements), T1.2 (commercial requirements), T1.3 (regulatory requirements) and all the reports related to the landscape of EnergyShield requirements. Moreover, SBA was finetuned to also address the EnergyShield guidelines as documented in *D1.5 System architecture-final update* [**ESH15**]. Figure 5 presents the main features of the SBA tool as developed during each one of its iterations.

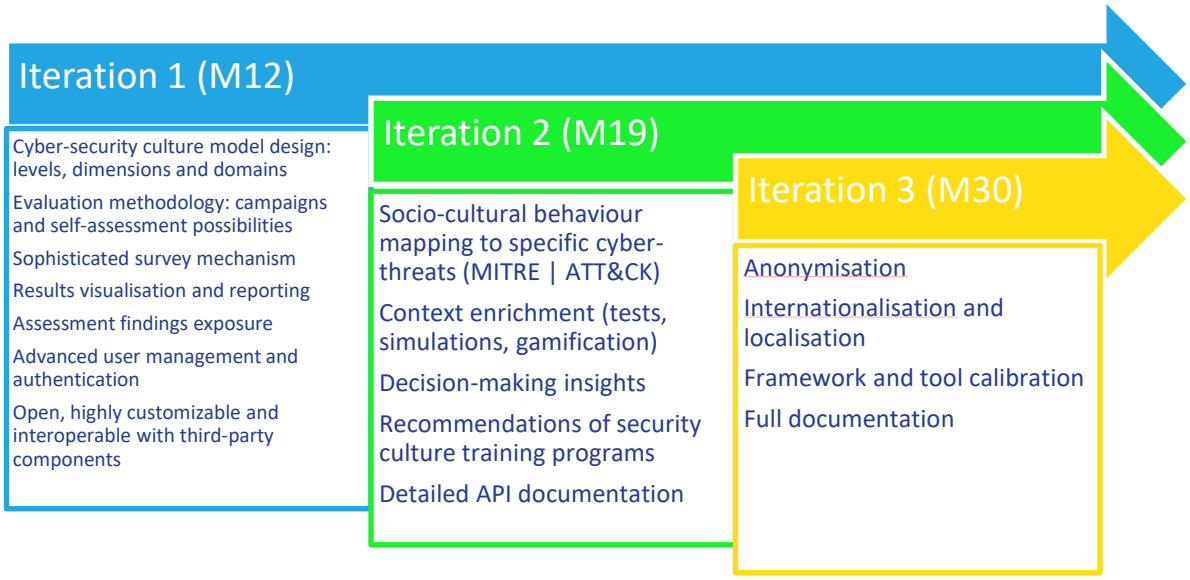

Figure 5. SBA tool roadmap

1.6.2. SBA TOOL DEMONSTRATOR

The SBA tool was tested by both the Italian and Bulgarian pilots in the context of the EnergyShield project. Additionally, extensive applications of the tool targeting alternative business domains have taken place with their results being presented in a number of scientific journals and conferences.

Bulgarian Pilot: Based on the initial task description of *T6.2* **[ESH62]**, the Bulgarian pilot was not expected to use the SBA tool in one of its use case scenarios. Yet, during the project lifecycle, the SBA tool was demonstrated to representatives of the Bulgarian pilot who expressed their interest in the functionality of the tool and subscribed to the SaaS version to familiarise themselves with and explore the capabilities of the tool.

In a second phase, various actors in the Bulgarian energy value chain (TSO, DSO, generation plants, prosumer, etc.) were involved in more detailed testing of the applicability and usability of the tool. During this phase, specific roles were assigned to different partners to analyse in detail the possibilities offered via the assessment mechanism of the tool.

Having adjusted and improved the tool based on the Bulgarian pilot's feedback, NTUA proceeded in translating all available questionnaires, thus fulfilling SBA localization and internationalization goals.

During the COVID-19 pandemic and the Ukrainian war, a cyber-security culture assessment campaign was carefully sketched out and adjusted to the Bulgarian pilot's needs. It was designed to be brief, lasting only for two weeks, while targeting employees from different organizational departments, of various expertise and professional backgrounds. The assessment campaign focused mainly on the **individual dimensions** aiming to evaluate the security skills, awareness, and behaviour of the participating organizations' workforce. Specifically, the campaign was aimed at the examination of the **Competency** and **Awareness** of the participants

in conjunction with their actual **Behaviour** and under the prism of existing security policies and procedures related to the **Assets** and the **Security Governance** of the participating organizations. Towards that end, **11 questionnaires and 1 simulation** were selected from a variety of assessment surveys, tests, games and simulations available within the SBA tool.

Following, specific employees from the entire power supply chain (producer, TSO, DSO, etc.) were selected for participation in the evaluation campaign. Table 3 presents the SBA tool evaluation results along with comments deriving from the practitioners' experience during the piloting.

Table 3. SBA Bulgarian Pilot KPIs results

Characteristic	Definition	Necessity	(F)lexibility (U)sability (A)ccuracy	Will assess	Bulgarian Pilot KPI	Bulgarian Pilot Recommended KPI value	Bulgarian Pilot Actual KPI value	Bulgarian Pilot Explanation
FUNCTIONAL SUITABILITY								
Functional completeness	Percentage of completed Use Cases / Usage Scenarios.	N		Y	(Completed Use Cases / Defined Use Cases) * 100 %	100 %	100%	
Functional correctness	Percentage of Use Cases without reported bugs, after tests.	N		Y	(Completed Use Cases without bugs / Defined Use Cases) * 100 %	>90%	100%	
Functional appropriateness	Percentage of tasks accomplished / Tasks Defined.	N		Y	(Accomplished Tasks / Tasks Defined) * 100%	>90%	92.24%	
PERFORMANCE EFFICIENCY								
Time behaviour	Average Latency.	N		Y	(Total Response Time) / (No. of Requests)	<= 1 sec	<=1 sec	
	Result Calculation.	N		Y	Total Time Interval from the completion of a task to the achievement score presentation	<= 2 sec	<=2 sec	
Capacity	Number of simultaneous transaction requests that can be served by the tool.	N		Y	Number of simultaneous transaction requests	>100	<29	In our campaign we had 29 participants

Compatibility								
Co-existence	Ability to host in a single environment.	Y	F	Y	Can SBA operate in a shared environment?	YES	YES	
Interoperability	Ability to exchange information with other systems.	Y	F	Y	Can SBA exchange information with the rest of the EnergyShield components and other IT corporate tools?	YES	YES	
Usability								
Appropriateness recognizability	Percentage of business goals (related with security behaviour, awareness, evaluation, etc.) addressed by the tool	Y	U	Y	(Addressed Business Goals / Defined Business Goals) * 100 %	>90%	100%	
Learnability	Hours required by a user to familiarise with the tool and use it efficiently, effectively and securely.	Y	U	Y	Learning Hours	< 1 hour	<1hour	
Operability	Number of clicks required to reach requested information.	Y	U	Y	Number of clicks required to reach required information	<3	1	
User error protection	Tool crash on user errors.	Y	U	Y	Does the whole SBA tool crash on user errors?	NO	NO	
Accessibility	Cross-Platform Accessibility.	Y	U	Y	SBA tool is accessible and operational through different platforms	YES	YES	
	Cross-Browser Accessibility.	Y	U	Y	SBA tool is accessible and operational through different browsers	YES	YES	

	Cross-Device Accessibility.	Y	U	Y	SBA tool is accessible and operational through different devices	YES	YES	
Reliability								
Maturity	Max. Concurrent Users Supported.	N		Y	No. of Max. Concurrent Users Recorded	>100 users	29 participants	
Availability	% Monthly Availability.	N		Y	1 - ((Downtown Time Minutes) / (Month Days*24*60))	>90%	Did not experience downtown time	
	Error Rate.	**N**		Y	(No. of Problematic Requests) / (Total Number of Requests)	<10%	None	
Fault tolerance	Number of software problems identified without affecting the platform.	N		Y	No. of Non-Critical Software Errors	<10	None	
Recoverability	Percentage of cases that system auto-recovered after an exception, error or a crash without any data loss.	N		Y	(No. of Auto-recovered Cases) / (Total Number of Erroneous Cases)	>90%	None	
Security								
Confidentiality	Incidents of ownership changes and accessing prohibited information.	N		Y	No. of incidents recorded	0	0	
Integrity	Incidents of authentication mechanism breaches.	N		Y	No. of incidents recorded	0	0	
Non-repudiation	Incidents of repudiable actions or events.	N		Y	No. of incidents recorded	0	0	
Accountability	Incidents of actions whose source	N		Y	No. of incidents recorded	0	0	

	cannot be identified.							
Authenticity N/A	Level of User Authenticity.	N		Y	Can you identify whether a subject is the one it claims to be?	YES	YES	
	Level of Data Resource Authenticity.	**N**		Y	Can you identify whether a resource is the one it claims to be?	YES	YES	
Maintainability								
Modularity	Tool is composed of sub-components such that a change to one component has no impact on other components.	Y	F	Y	Is SBA developed in a modular way so that sub-components (tests, games, etc.) function independently?	YES	YES	
Reusability	Ability to be used in more than one application scenarios and business domains.	Y	F	Y	Can SBA be utilized in different business domains and application areas?	YES	YES	
Modifiability	% of Update Effectiveness.	Y	F	Y	(No. of updates preformed without noticing operational problems) / (No. of updates performed)	>75%	100%	
Testability	Level of Testing.	N		Y	Are tests able to probe the tool behaviour?	YES	YES	
Portability								
Adaptability	Mean No. of Errors per different installation environment.	Y	F	Y	(No. of Total Errors recorded during Installations) / (Total No. of Installation Environments)	<1	0	

Installability	Mean No. of Errors per Installation.	N		Y	(No. of Total Errors recorded during Installations) / (Total No. of Installations)	<1	0	
Accuracy*								
Sufficiency	Percentage of organisation members (employees, external contractors, etc.) subscribed to the tool.	Y	A	Y	(Number of tool users / Number of organisation members) * 100 %	>90%	20.7%	
	Percentage of fulfilment of the tool evaluation processes.	Y	A	Y	(Number of completed assignments / Number of total assignments) * 100 %	>90%	100%	
Coverage	Percentage of security culture framework evaluated by the tool (i.e. with available assessment context and implemented evaluation techniques).	Y	A	Y	(Number of Domains evaluated by the tool / Number of Security Culture Framework Domains) * 100 %	100%	77%	
	Percentage of security culture framework evaluated within the organisation.	Y	A	Y	(Number of Evaluated Domains within the organisation / Number of Security Culture Framework Domains) * 100 %	>90%	13%	Targeted campaign on specific domains.
Validity	Deviation of phishing simulation results per user from phishing attack rate per user (as reported by security infrastructure solutions).	Y	A	Y	(Phishing Simulation Percentage Score – Phishing Attack Percentage Rate)	>5%	For security reasons, we want to keep this data confidential.	

	Deviation of user security awareness based on SBA evaluations and on organisation security awareness training program.	Y	A	Y	(Employee Security Awareness Score (SBA metric) - Employee Security Awareness Training Program Achievement Score)	>5%	>5%	
	Deviation of the Employee Individual dimensions (SBA metric) of the user from the corresponding Security Incident Profile (reported / identified security incidents).	Y	A	Y	(Employee Individual Score (SBA metric) - Security Incident Profile)	>5%	>5%	

* *Accuracy refers to the closeness between the estimated value and the (unknown) true value that the statistics were intended to measure.*

Italian Pilot: As described in detail in the ***D6.1 Offline field trial report*** **[ESH61]**, the SBA tool was piloted as part of the ***Use Case IT_01*** which focused on SCADA AMI systems operators and people involved in sensitive roles within IRETI organizational structure. The application scenario targeted employees operating in the following units: Substation O&M, Operations, Remote control, and SCADA, Technical and administrative of both IREN and IRETI.

Towards that end, the SBA tool was submitted to a significant cluster of beta-testers and early adopters who were selected to assess the business value and applicability of the questionnaires and games implemented. Each questionnaire filled for the SBA tool was analysed to evaluate if it was directly applicable to the IRETI test case or not, or if minor modifications were needed (e.g., regulatory adjustments to the Italian framework). In a second phase, the same analysis was carried out at a single-question level.

Initially, the interested business units and employee roles were individuated within the company focusing on the Advanced Meter Management (AMM) personnel, managers and operators, remote control system responsible personnel, IT referents, cybersecurity team, DSO top management, and DSO technical and OT staff. Secondly, questionnaires were characterized by setting the relation among units, roles, and groups of questions.

In a second stage, tests and questionnaires were submitted to “early adopters” (e.g., one person per significant unit individuated in the previous phase) to gather valuable feedback regarding both SBA’s content, applicability, and usability.

Once questions were categorized and modified according to IRETI requirements, all SBA questionnaires were translated into Italian since the vast majority of IRETI staff are native Italian speakers and lifting the language barrier was expected to assist in the overall security assessment.

Having concluded this testing phase with the assistance of the Italian pilot, SBA was ready to be submitted to a broader sample of users and practitioners to assess the overall company's cyber and physical security culture. For this reason, the test was submitted to all the employees of the company working on electrical energy distribution. A population of approximately 250 people was reached.

The SBA tool evaluation at the Italian pilot took place during the COVID-19 pandemic and the Ukrainian war. Due to the intensive cyber-security criminality of the period and in conjunction with the rather demanding work circumstances, certain criteria needed to be met:

1. **Life-cycle**: Since the assessment campaign was targeting a significant portion of the workforce of the participating organisations, deriving from different departments and sectors, a sufficient life-cycle needed to be defined and in accordance with the operations life-cycle. Individuals were invited to participate in the campaign given a rather loose deadline of almost a month allowing them to overcome professional obligations (e.g., projects), personal leaves, official holidays, and so on.
2. **Duration**: Due to the special living and working circumstances along with the well-known defensive approach towards surveys, the time required for its completion needed to remain short. As a result, 4 questionnaires were created by carefully combining and trimming existing assessment reports (in the SBA tool) adjusting them to the specific evaluation needs of the campaign. Thus, ensuring a mean participation time equal to less than 10 minutes.
3. **Plainness**: The campaign was targeting employees from various positions and expertise not necessarily familiar with technological and information security terms. Consequently, questions were carefully phrased aiming to ensure an increased difficulty in properly assessing participants' familiarity with the cyber-security reality. Furthermore, a localised version of the SBA tool was used to lift the language barrier from the evaluation process.

Additionally, certain organisational needs had to be addressed by this cyber-security culture evaluation. These needs dictated the dimensions and domains which needed to be addressed underlying the security factors of interest. Since organisation-related security factors were persistent for all participants, the survey focused on the individual dimensions and domains. Specifically, the campaign was aimed at the examination of the security Attitude of the participants in contrast with their Awareness and Competency.

Table 3 presents the SBA tool evaluation results along with comments deriving from the practitioners' experience during the piloting.

Table 4. SBA Italian Pilot KPIs results

Characteristic	Definition	Necessity	(F)lexibility (U)sability (A)ccuracy	Will assess	KPI	Italian Pilot Recommended KPI value	Italian Pilot Actual KPI value	Explanation
FUNCTIONAL SUITABILITY								
Functional completeness	Percentage of completed Use Cases / Usage Scenarios.	N		Y	(Completed Use Cases / Defined Use Cases) * 100 %	100 %	100%	
Functional correctness	Percentage of Use Cases without reported bugs, after tests.	N		Y	(Completed Use Cases without bugs / Defined Use Cases) * 100 %	>90 %	100%	
Functional appropriateness	Percentage of tasks accomplished / Tasks Defined.	N		Y	(Accomplished Tasks / Tasks Defined) * 100%	>90 %	100%	
PERFORMANCE EFFICIENCY								
Time behaviour	Average Latency.	N		Y	(Total Response Time) / (No. of Requests)	<=1 sec	0,35 sec	
	Result calculation.	**N**		Y	Total Time Interval from the completion of a task to the achievement score presentation	<=2 sec	0,57 sec	
Capacity	Number of simultaneous transaction requests that can be served by the tool.	N		Y	Number of simultaneous transaction requests	>100	23	This metric is important for assessing how many users might be handled by the SBA tool simultaneously. The peak usage in the Italian pilot was 23 users simultaneously, and it was successfully managed by the Energy Shield platform. Additional stress tests might be performed in a simulation environment.
COMPATIBILITY								
Co-existence	Ability to host in a single environment .	Y	F	Y	Can SBA operate in a shared environment?	YES	YES	

Interoperability	Ability to exchange information with other systems.	Y	F	Y	Can SBA exchange information with the rest of the EnergyShield components and other IT corporate tools?	YES	YES	The SBA tool was able to co-operate with Iren IT systems, allowing for simpler usage by end users..
USABILITY								
Appropriateness recognizability	Percentage of business goals (related with security behaviour, awareness, evaluation, etc.) addressed by the tool.	Y	U	Y	(Addressed Business Goals / Defined Business Goals) * 100 %	>90 %	100%	
Learnability	Hours required by a user to familiarise with the tool and use it efficiently, effectively, and securely.	Y	U	Y	Learning Hours	<1 hour	1 hour	The system is pretty simple to use and this creates a fast learning curve that allows a large employee population to be reached.
Operability	Number of clicks required to reach requested information.	Y	U	Y	Number of clicks required to reach required information	<3	2	The lower the number, the simpler the tool. It means that employees do not waste time on additional clicking and are able to navigate easily through the platform.
User error protection	Tool crash on user errors.	Y	U	Y	Does the whole SBA tool crash on user errors?	NO	NO	The system operated properly.
Accessibility	Cross-Platform Accessibility.	Y	U	Y	SBA tool is accessible and operational through different platforms	YES	YES	The system operated properly.
	Cross-Platform Accessibility.	**Y**	**U**	Y	SBA tool is accessible and operational through different browsers	YES	YES	The system operated properly.
	Cross-Platform Accessibility.	**Y**	**U**	Y	SBA tool is accessible and operational through different devices	YES	YES but	Few people (<1% respondents, <2% total pool of users) experienced issues in using the SBA from a tablet within the company network (covered by firewalls).
RELIABILITY								
Maturity	Max. Concurrent Users Supported.	N		Y	No. of Max. Concurrent Users Recorded	>100 users	23	

Availability N/A	% Monthly Availability.	N		Y	1 - ((Downtown Time Minutes) / (Month Days*24*60))	>90%	100%	
	Error rate.	**N**		Y	(No. of Problematic Requests) / (Total Number of Requests)	<10%	0	
Fault tolerance	Number of software problems identified without affecting the platform.	N		Y	No. of Non-Critical Software Errors	<10	0	
Recoverability	Percentage of cases that system auto recovered after an exception, error or a crash without any data loss.	N		Y	(No. of Auto-recovered Cases) / (Total Number of Erroneous Cases)	>90%	100%	
SECURITY								
Confidentiality	Incidents of ownership changes and accessing prohibited information.	N		Y	No. of incidents recorded	0	0	The system operated properly.
Integrity	Incidents of authentication mechanism breaches.	N		Y	No. of incidents recorded	0	0	The system operated properly.
Non-repudiation	Incidents of repudiable actions or events.	N		Y	No. of incidents recorded	0	0	The system operated properly.
Accountability	Incidents of actions whose source cannot be identified.	N		Y	No. of incidents recorded	0	0	The system operated properly.
Authenticity N/A	Level of User Authenticity.	N		Y	Can you identify whether a subject is the one it claims to be?	YES	YES	
	Level of Data Resource Authenticity.	**N**		Y	Can you identify whether a resource is the one it claims to be?	YES	YES	
MAINTAINABILITY								
Modularity	Tool is composed of sub-components such that a change to one component	Y	F	Y	Is SBA developed in a modular way so that sub-components (tests, games, etc.) function independently?	YES	YES	

	has no impact on other components.							
Reusability	Ability to be used in more than one application scenarios and business domains.	Y	F	Y	Can SBA be utilized in different business domains and application areas?	YES	YES	
Modifiability	% of Update Effectiveness.	Y	F	Y	(No. of updates preformed without noticing operational problems) / (No. of updates performed)	>75%	100%	
Testability	Level of Testing.	N		Y	Are tests able to probe the tool behaviour?	YES	YES	
PORTABILITY								
Adaptability	Mean No. of Errors per different installation environment.	Y	F	Y	(No. of Total Errors recorded during Installations) / (Total No. of Installation Environments)	<1	0	
Installability	Mean No. of Errors per Installation.	N		Y	(No. of Total Errors recorded during Installations) / (Total No. of Installations)	<1	0	
Accuracy*								
Sufficiency N/A	Percentage of organisation members (employees, external contractors, etc.) subscribed to the tool.	Y	A	Y	(Number of tool users / Number of organisation members) * 100 %	>90%	48.6%	This is the number of respondents over the total number of people involved (approx. 250). 90% was a very high target: the internal metric is 30-40% to be considered a successful campaign of investigation.
	Percentage of fulfilment of the tool evaluation processes.	**Y**	**A**	Y	(Number of completed assignments / Number of total assignments) * 100 %	>90%	95%	Almost all the people who started an assignment finished it.
Coverage N/A	Percentage of security culture framework evaluated by the tool (i.e. with available assessment	Y	A	Y	(Number of Domains evaluated by the tool / Number of Security Culture Framework	100%	100%	

	context and implemented evaluation.				Domains) * 100 %			
	Percentage of security culture framework evaluated within the organisation .	**Y**	**A**	Y	(Number of Evaluated Domains within the organisation / Number of Security Culture Framework Domains) * 100 %	>90%	5.8%	3 individual domains (employee profiling, security behaviour, and security skills evaluation) out of 52 domains (organizational and individual) of the CSC framework. As a result, a targeted campaign with a specific focus was designed and used to evaluate special security aspects. Moreover, each aspect requires a lot of time. We submitted the entire questionnaire to a restricted number of people (around 10) that cover crucial roles in OT cybersec. With those people, we decided which area to investigate over the entire sensible population (90% would require more than one day per employee and it is too high an effort.
Validity	Deviation of phishing simulation results per user from phishing attack rate per user (as reported by security infrastructure solutions).	Y	A	Y	(Phishing Simulation Percentage Score – Phishing Attack Percentage Rate)	>5%	-	For security reasons, we want to keep this data confidential.
	Deviation of user security awareness based on SBA evaluations and on organisation security awareness training program.	Y	A	Y	(Employee Security Awareness Score (SBA metric) - Employee Security Awareness Training Program Achievement Score)	>5%	-	For security reasons, we want to keep this data confidential.
	Deviation of the Employee Individual dimensions (SBA metric) of the user from the	Y	A	Y	(Employee Individual Score (SBA metric) - Security Incident Profile)	>5%	-	For security reasons, we want to keep this data confidential.

	corresponding Security Incident Profile (reported / identified security incidents).							

* *Accuracy refers to the closeness between the estimated value and the (unknown) true value that the statistics were intended to measure.*

1.6.3. SBA TOOL BEST PRACTICES AND LESSONS LEARNED

The SBA tool has been designed and implemented to facilitate the assessment, cultivation, and improvement of the cyber-security culture status of an organisation via a holistic approach. Numerous security elements and factors have been identified, listed, and grouped into different levels, dimensions, and domains, offering a hierarchical representation of the cyber-security readiness and overall reality of an organisation. Role segregation, key assessment concepts, and a specific evaluation methodology have been presented in detail, providing a useful guide through this rather demanding business procedure. Specific cyber-threats along with mitigation strategies, recommendations, and targeted security awareness training programs are identified based on the assessment results achieved via the SBA tool.

As presented in Table 3 and Table 4, both based on the witnessed KPIs' values and the ones provided by the practitioners feedback, the SBA tool managed to meet and surpass the KPI objectives, especially the ones related with:

- Functional suitability
- Performance efficiency
- Compatibility
- Reliability
- Security
- Maintainability
- Portability

but most importantly gained favourable remarks related to ***Usability*** proving its clear orientation towards the human factor in the cyber-security landscape.

Deviations noticed in ***Accuracy*** KPIs of both pilots are mainly due to the limited exploitation of the SBA tool within the evaluated organisations. An extended and assessment of the entire Cyber-Security Culture Framework implemented by the SBA tool requires numerous iterations (campaigns) carefully scheduled based on the operations lifecycle of each organisation and, most importantly, addressing the entire workforce.

During the COVID-19 crisis, the CSC framework was used to design a cyber-security culture assessment campaign targeting critical infrastructures [**GES20**, **GEA20**]. Its revealing findings [**GED20**] provided significant feedback to the participating EU

organizations. Insights and recommendations towards enforcing their cyber-security resilience were offered, further contributing to this research domain.

This scientific effort inspired SPHINX, an EU project aiming to enhance the cyber protection of the Health and Care IT Ecosystem [**SPH19**] and triggered a collaboration activity with EnergyShield. More specifically, the Cyber Security Culture framework assisted SPHINX security specialists in the design of a two-phase security awareness campaign targeting health sector personnel.

Finally, the SBA tool was used to assess the cyber-security culture readiness in Academia during the COVID-19 crisis and the Ukrainian war [**GEO22**].

The CSC and its implementation tool, SBA, were evaluated and exploited in wide application scenarios while gaining recognition by IT and security specialists in different business domains. The feedback provided throughout the process assisted in improving its methodology and approach toward end-users of different business domains and industries.

1.7. ANOMALY DETECTION TOOL

The Anomaly detection (AD) tool is a complex software and hardware tool that uses Machine Learning (ML) to enable the real-time detection of anomalies covering the monitoring part. The AD tool is a comprehensive process anomaly detection system that monitors critical assets, using ICS/SCADA electrical signal-based advanced analytics, Artificial Intelligence and Machine Learning.

On the EnergyShield solution architecture, this tool monitors and analyses the OT level 0 part of the different EPES assets (e.g., turbine, substation, etc.) that will be connected to the EnergyShield solution. The tool is duplicating unidirectionally the asset's ICS/SCADA electrical signals, which runs be-tween sensors and actuators to the PLC and is performing real-time pro-cess-oriented anomaly detection by using ML models on this data to detect and alert on abnormal behaviour of the process, indicating on a potential on-going cyber-attack on the OT and physical systems of the asset.

The anomalies are associated with the properties of the electrical signal, such as amplitude, phase, and frequency of the voltage and current being measured. The AD tool is based on the SigaGuard solution and technology developed by SIGA OT Solutions. SigaGuard safeguards industrial assets by monitoring its SCADA's raw electrical signals (using advanced ML on level 0 data) — as opposed to data packets, which can be hacked. SigaGuard brings new and unmatched operational reliability into physical processes, to provide real-time anomaly detection and to support intelligent, real-time, business-critical decision making, See Figure 6.

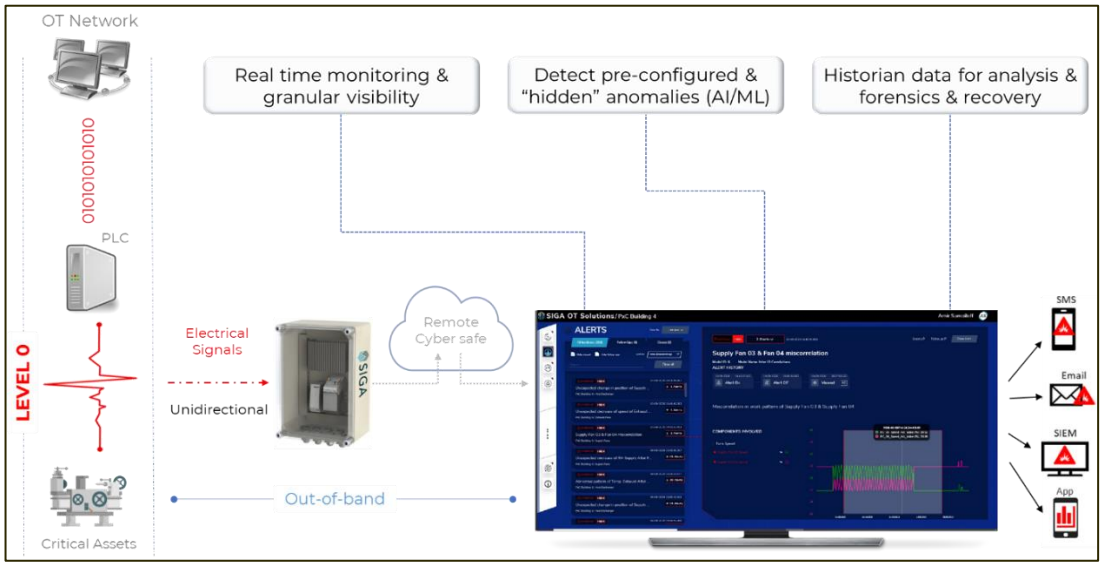

Figure 6. AD tool overview

1.7.1. AD TOOL TECHNICAL DETAILS

The tool is applying real-time ML models on live process data, which is generated by the tool's physical hardware platform, which is duplicating and acquiring the electrical signals. The tool architecture is composed of four layers:

1. Data Acquisition: A hardware layer that combines off-the-shelf industrial standard electronic components that are assembled into a platform, which is designed for duplicating and acquiring the ICS/SCADA electrical signals and using these signals as data for the anomaly detection engine and for GUI visualization.
2. Software framework: On the hardware layer runs the tool's software framework, ML engine, and GUI. From there, it can be connected to the internet, allowing for remote access to the Graphical User Interface (GUI) and sending alerts and reports in multiple ways (e.g., e-mail, SMS, etc.) and to interface with multiple platforms (e.g., SIEM, SOC, etc.). The tool's software framework, ML engine, and GUI can also run on a remote server. The software framework layer is responsible for collection of real time raw handling it and utilize it to be used by the ML engine layer and the GUI Layer. Another feature of this layer is clustering and aggregation of alerts, to reduce the number of alerts the system will send to the users and to frame specific process anomalies into one event.
3. ML engine: This layer preprocesses the data received from the database and then applies multiple ML models to the data for training (in the learning period) and to detect anomalies in real-time (while in operation). Once the anomaly has been detected, the ML algorithm engine sends the alert information to the database. It also provides the user with access to the Anomaly ML Analysis tool.
4. Graphical User Interface (GUI): The tool's graphical user interface is called SigaSight, and it provides the user with asset visualization, alerts, and analysis.

SIGA developed the AD tool based on SIGA's technology to have 3 new main capabilities for detecting abnormalities in EPES assets' operational processes:

- Improved anomaly detection capabilities and extended users' understanding of anomalies by developing new ML models:
  - Coupled Dependencies Boundary Analysis (CDBA) ML model for the detection of abnormal behaviour of analogue IO pairs in multi-dimensional time-series data of the operational process;
  - Coupled Dependencies Boundary Analysis (CDBA) with States ML model for detection of abnormal behaviour of analogue IO pairs combined with discrete IOs conditions in multi-dimensional time-series data of the operational process;
  - Time Series Parallel Neural-Network Detection ML model for creating multiple parallel prediction, using a neural network (NN) architecture on time-series data of the operational process
- Improved explainability of alerts, allowing the user more understanding and actionable insights from each alert.
- Added sources of EPES operational process data for analytics.

1.7.2. AD TOOL DEMONSTRATOR

The AD tool was deployed at two pilot sites: in Iren's Martinetto HV/MV substation in Turin, Italy; and in HPP Lenishta hydro power plant in Bulgaria. The deployment included the installation of the SIGA hardware platform in the substation, with the SIGA software and ML engine running on the platform computing device. The SIGA hardware platform is packaged in a small cabinet, called SigaBox, and was connected and wired to the sub-station and hydro power plant's sensors, circuit breakers, and actuators. The hardware platform acquires the data to be used by the tool software and its ML engine to detect anomalies. The users are provided with SIGA's GUI with secure remote access for visualization and analytics.

At the Italian pilot site, the AD tool is monitoring the operation of 5 different lines of the sub-station (circuit breaker and current measurement in each line) and the main bus bar (voltage measurements). At the Bulgarian pilot site, the AD tool is monitoring the operation of the hydropower (temperature, power, flow, and pressure sensors). First, after the installation, the AD tool has learned the normal behaviour of the sub-station/power plant process. Once the learning period is completed, the AD tool now detects anomalies in real-time. The anomalies the tool detects are caused by abnormal behaviour of the substation/power plant operational process. These anomalies can potentially be caused by a cyber-attack performed on the SCADA in which the attacker is trying to manipulate the substation process operation and harm the machinery, causing a breakdown of the substation/power plant. This can stop the electricity transfer out of the sub-station or the power generation of the power plant, and in some cases, endanger the safety of the machinery and even risk human life. The AD tool GUI in the pilots enables the users to have full visualisation of the process, receive alerts on anomalies, perform analysis and forensics etc.

Table 5. AD Italian Pilot KPIs results

Characteristic	Definition	Necessity	(F)lexibility (U)sability (A)ccuracy	Will assess	AD	Recommended KPI value	Actual KPI value
FUNCTIONAL SUITABILITY							
Functional completeness	Degree to which the set of functions covers all the specified features and user objectives.	N		Y	(Completed Use Cases / Defined Use Cases) * 100 %	100 %	100%
Functional correctness	System provides the correct results with the needed degree of precision.	N		Y	(Completed Use Cases without bugs / Defined Use Cases) * 100 %	>90%	100%
Functional appropriateness	The functions facilitate the accomplishment of specified tasks and objectives.	N		Y	(Accomplished Tasks / Tasks Defined) * 100%	>90%	100%
PERFORMANCE EFFICIENCY							
Time behaviour	Response, processing times and throughput rates of a system, when performing its functions, meet requirements.	N		Y	Response time to alert when anomaly occures in the process	<5 sec	1 sec
Capacity	Degree to which the maximum limits of a product or system parameter meet requirements.	N		Y	Number of anomalies detected simultaneously	>10	15
COMPATIBILITY							
Co-existence	Product can perform its functions efficiently while sharing environment and resources with other products.	Y	F	Y	Can AD operate in a shared environment?	Yes	Yes
Interoperability	A system can exchange information with other systems and use the information that has been exchanged.	Y	F	Y	AD able to send alerts to users by e-mail and users can use the e-mail message to see the alert on the tool GUI	Yes	Yes
USABILITY							

Appropriateness recognizability	Degree to which users can recognize whether a product or system is appropriate for their needs.	Y	U	Y	(Addressed Business Goals / Defined Business Goals) * 100 %	>90%	100%
Learnability	Degree to which a product or system can be used by specified users to achieve specified goals of learning to use the product or system with effectiveness, efficiency, freedom from risk and satisfaction in a specified context of use.	Y	U	Y	Learning Hours	< 2 hours	1 hour
Operability	Degree to which a product or system has attributes that make it easy to operate and control.	Y	U	Y	Number of clicks required to reach required information	< 5	3 clicks
User error protection	System protects users against making errors.	Y	U	Y	Is there a pop-up / verification message to the user when clicking an action button before taking the action?	Yes	Yes
User interface aesthetics		Y	U	Y	Pilot user's review on the aesthetics of GUI in the scale of 1-10	≥7	9
Accessibility	System can be used by people with the widest range of characteristics and capabilities.	Y	U	Y	There is a function in which the user can increase and decrease the fonts size in the dashboard	Yes	Yes
RELIABILITY							
Maturity	System meets needs for reliability under normal operation.	N		Y	System is operational 24/7 without manual interferance	Yes	Yes
Availability	System is operational and accessible when required for use.	N		Y	1 - ((Downtime Minutes) / (Month Days*24*60)) * 100%	>90%	99%
Fault tolerance	System operates as	N		Y	System is fully operational	Yes	Yes

	intended despite the presence of hardware or software faults.				also without internet connection		
Recoverability	Degree to which, in the event of an interruption or a failure, a product or system can recover the data directly affected and re-establish the desired state of the system.	N		Y	System is automatically restarting after power outage	Yes	Yes
SECURITY							
Confidentiality	System ensures that data is accessible only to those authorised to have access.	N		Y	No. of incidents recorded	0	0
Integrity	System prevents unauthorised access to, or modification of, computer programs or data.	N		Y	Personal user name and password are required to access the dashboard	Yes	Yes
Non-repudiation	Actions or events can be proven to have taken place, so that the events or actions cannot be repudiated later.	N		Y	All actions performed in the dasboard are being logged and recorded (with user and time of the action)	Yes	Yes
Accountability	Degree to which the actions of an entity can be traced uniquely to the entity.	N		Y	All actions performed in the dasboard are being logged and recorded (with user and time of the action)	Yes	Yes
Authenticity	The identity of a subject or resource can be proved to be the one claimed.	N		Y	2FA mechanism is implemented and used in the dasboard	Yes	Yes
MAINTAINABILITY							
Modularity	System is composed of components such that a change to one component has minimal impact on other components.	Y	F	Y	Is AD developed in a modular way so that sub-components (database, dashboard, ML models) function independently ?	Yes	Yes

Reusability	An asset can be used in more than one system, or in building other assets.	Y	F		Can AD be utilized in different business domains and application areas?	Yes	Yes
Modifiability	Degree to which a product or system can be effectively and efficiently modified without introducing defects or degrading existing product quality.	Y	F	Y	(No. of updates preformed without noticing operational problems) / (No. of updates performed)	>90%	100%
Testability	Effectiveness and efficiency with which test criteria can be established for a system.	N		Y	Are tests able to probe the tool behaviour?	Yes	Yes
PORTABILITY							
Adaptability	Degree to which a product or system can effectively and efficiently be adapted for different or evolving hardware, software or other operational or usage environments.	Y	F	Y	Can the AD tool operate with different sources of data or different vendors of HW components?	Yes	Yes
Installability	Effectiveness and efficiency with which a system can be successfully installed and/or uninstalled.	N		Y	Net. duration of installation (in days)	≤3	2
Accuracy*							
Sufficiency	Degree to which data collected by the product can constitute a representative data set.	Y	A	Y	The learning period of the AD tool's ML models	<10 weeks	8 weeks
Coverage	Effectiveness and efficiency with which the product handles the data set collected.	Y	A	Y	The graphs representing the process data in the dasboard can be zoomed in to the same resolution as the measurements in the database	Yes	Yes
Validity	Degree to which	Y	A	Y	(Number of anomalies	>90%	100%

	produced by the product results deviate from real-life.				detected by the tool in 1 day / Number of anomalies occurred in the physical process in 1 day) *100%		

* *Accuracy refers to the closeness between the estimated value and the (unknown) true value that the statistics were intended to measure.*

1.7.3. AD TOOL BEST PRACTICES AND LESSONS LEARNED

A cyber-attack simulation test was conducted at the Italian site as part of the evaluation of the AD tool performance and functionalities. In June 2022, Iren's team performed physical manipulation of the physical process of the sub-station to simulate cyber-attacks and test the tool's capabilities to detect anomalies and alerts. There were a number of different attacks that were simulated, each of which had a number of different variants. Some of the attacks were carried out physically within the substation systems, while others were carried out from the control room using the main control system. The following Table 6 provides an overview of the various primary attack types.

Table 6. Attack types overview

Attack Description	Attack Potential Damage	Test Result
Attacker changes the voltage on the main bus bar	Power outages in all lines	Anomaly detected immediately and alert was fired
Line circuit breaker protection mechanism is manipulated by attacker	Equipment damage and safety issues	Anomaly detected immediately and alert was fired
Attacker is Increasing the load on a line to abnormal values	Interruptions in the grid, damage to the equipment	Anomaly detected immediately and alert was fired
Circuit breakers sequence is changed by attacker	Power outages in some areas of the city	Anomaly detected immediately and alert was fired

To illustrate how the AD tool operates, the following is an illustration of an anomaly detection of one type of attack in which the attacker increases the Potenza line's load until it reaches abnormal values:

- The attacker suddenly increases the load on the Potenza line, using the control system, from 4 A to 93 A, at 14:09:50.
- The AD tool detects this process anomaly at 14:09:50 (immediately) with various ML models (TCM and TCM with states models). An alert is fired in the GUI and sent by e-mail to Iren's team.
- The users can now see the alert details and a visualisation of the attack on the sub-station process.
- The user enters the ML visualisation tool in the GUI to investigate the alert and understand where, how, and when the attack took place in the process.

This example demonstrates the importance and advantages of detecting anomalies in the process from level 0. SIGA's AD tool is the only solution that provides the operator with complete visibility into its operations and machinery by performing the analysis of electrical signals directly from the OT/ICS Level 0. The process signals-oriented ML models deliver the most elaborated insights to allow the operators to really feel their machinery pulse, and act upon potential threats quickly and effectively, so that downtime is avoided or reduced to the minimum.

In terms of evaluation KPIs, the Italian Pilot reports that the AD tool has been evaluated to achieve all of the recommended KPI values. This information can be found in Table 5.

1.8. DISTRIBUTED DENIAL OF SERVICE MITIGATION TOOL

The Distributed Denial of Service Mitigation (DDoSM) tool is a Software as a Service that uses L7Defense's Ammune technology ("Innate Immune Theory") to detect advance attack patterns (such as multi-vector attacks) together with City analytical modelling approach (epidemiological modelling) to predict and protect against cascading effects. This means that, apart from detection, it takes care of the protection level as well. The application is focused on:

- Applying an advanced unsupervised learning model
- Detecting automatically unknown automated threats
- Highly controlled and precise mitigation process KPIs

1.8.1. DDOSM TOOL TECHNICAL DETAILS

Methodology used: City, University of London, based its analytical modelling approach on epidemiological principles. This methodology was used to model the smart grid components' activities alongside applied DDoS attack dynamics. These models provide insight into the impact of timings, durations, and many more. It also looks at the influence of simulated DDoS attacks on the settings, deployment, and analysis capabilities of the Ammune tool.

Features: L7 Defense's Ammune™ API security solution is an advanced unsupervised AI/ML technology. It protects APIs from advanced attack types, with a minimal impact on legitimate traffic. It continuously and automatically discovers and protects each API separately. It builds a specific profile (AI/ML set of baselines) for each API endpoint, which is used to spot and stop emerging threats that otherwise go unnoticed, in real-time, and without any prior knowledge or signatures of the attack characteristics. It is inspired by the natural "innate immune" model, designed for accuracy and to minimise the damage from both erroneous detections (false positives) and from incoming attack penetration (false negatives).

Ammune contains the following functional modules:

- API-WAF protects from content injection threats targeting remote command execution, data exfiltration, denial of service, and more.
- API-BOT protects from advanced automated threats that implement data exfiltration, fraud actions, account takeover, functionality abuse, and more.
- API-DDoS protects from DDoS attacks on API business logic that attempt to overload the computation and memory resources of the application servers.
- API-BL protects APIs from business-level exploits, such as authorization and authentication bypasses.

The Ammune™ architecture consists of a real-time traffic enforcement unit and an analytics unit that provides near real- time analytics of the traffic flows. Ammune™ supports various embedding architectures, including:

- Network test access point (TAP)-Copy of the traffic is received by the Ammune Real-Time module directly from the network TAP without reverse proxy). The module blocks commands that could be sent to other enforcing devices.
- Log feed - Copy of traffic that could be received from other sources, such as log feeds in the SIEM and security information.
- Integration with Kubernetes ingress Ammune integrates with ingress (reverse proxy-based) instead of a standard reverse proxy.
- Inline integration - Ammune™ integrates in front of the customer's application architecture or between two hops in the flow.

As far as integration goes, alerts and security incidents generated by Ammune can be forwarded to other tools such as SIEM, security orchestration, automation, and response (SOAR), or ticketing systems. Furthermore, a special integration pattern was added to support the Energy Shield project. Ammune™ can be integrated with API gateways to receive traffic log feeds for analysis. Log feeds could also be fetched from other sources such as SIEM or weblogs. Ammune can also integrate with packet brokers as a traffic feed source, where a special adapter module will extract logs and forward them to Ammune's main engine. Ammune also contains a rich UI interface to control network flow, configurations, and enforcement policies by the user.

1.8.2. DDOSM TOOL DEMOSTRATOR

For the project, Ammune algorithms were retrained and recalibrated to handle smart grid scenarios. For instance, Ammune DDoS detection was adjusted to better handle extra heavy-duty calls. It can now detect DDoS attacks successfully at rates above one request per second. Also, a significant weight to calls returning error was added to increase the sensitivity for capturing attacks that overload the system with calls to non- existent objects to bypass cache. The Ammune analysis time slot was reduced from 5 to 1 second to reduce the attack mitigation time to under 1 minute.

DDoS attacks were initiated and generated by sending API calls via randomly selected proxies at a relatively short timeout to maximise the attack rate at around 400 requests per second. Three types of attack scenarios were conducted. The first one was aimed at the “meter update” API endpoints where the smart meter id and meter reading parameters were randomly selected to add extra load on the server. The second one consisted of attacks aimed at the “read region power consumption” API endpoints. The third one combined the two scenarios.

A simulated botnet was launched to mimic a DDoS attack. When the server is overwhelmed, aggregators are impacted, and subsequently, smart meters are impacted. The simulation environment was used for testing and validation activities. The IA-DDoS model was deployed to capture population fluctuations in a DDoS-enabled botnet. The IA-DDoS model successfully passed testing and validation against L7 Defense’s simulations.

Also, the Secured Authentication Communication (SAC) model was deployed to test the possibility of using population-level observation of the smart grid and its component networks and/or systems in the context of DDoS impact propagation. Unlike IA-DDoS, the SAC model also splits the overall smart grid into subpopulations to check the impact that one subpopulation could have on another, given any dependencies existing between them. The SAC model was successfully validated using parametric testing and numerical simulation.

The FC-DDoS model was analysed using numerical simulations and tested under varying conditions. For the DDoS module, it was observed that the malicious stream consumed a rising number of resources as the arrival rate increased. Also, the duration of the attack increased the period of disruption. For later attack end times, a downward recovery slope indicated that more damage occurred. The arrival rate was mitigated by blocking the attack as soon as possible.

The Ammune DDoS attack discovery was made by analysing the “distance” of incoming request flow from the generic and business logic (BL) profiles. Both profiles are implemented at a single API endpoint, entity, and multi-entity (campaign) levels. For distance regarding the general profile, the API-based anomaly detection consisted of weighing the anomaly of the specific API endpoint call rate by its reply complexity. For the API-based anomaly detection, anomalies in the context of the API endpoint calls, such as time intervals between calls and unexpected call sequences, were detected.

Ammune™ identify DDoS attacks based on OOD calculation of incoming request flow charateristics from normal distribution. The calculation is implemented at a single API endpoint, entity, and multi-entity (campaign) levels. The anomaly results weight the OOD with the resource consumption related to the specific API endpoint.

Results:

- Regarding attack scenario 1, flooding the server with bogus smart meter update requests, where smart meter ID and reading are selected randomly, Ammune was able to perform efficient mitigation in 30 seconds from the attack initiation. As the botnet sources were rotating, Ammune was able to update its mitigation policy on-the-fly without any further degradation of service.
- Regarding attack scenario 2, flooding the server with read region power consumption (heavy requests), Ammune started its efficient mitigation within 30 seconds from the start of the attack. As the botnet sources were rotating, Ammune was able to update its mitigation policy on-the-fly, without any further degradation of service.
- Regarding attack scenario 3, the combination of attack scenarios 1 and 2, Ammune started to mitigate the attack after 30 seconds from its initiation, which is the experience “set-up time” for a visible impact of the attack on an API activity under the simulation conditions. As the botnet sources were rotating, Ammune was able to update its mitigation policy on-the-fly without any further degradation of service.

Using generic Ammune capabilities and the novel Smart Meter business logic implementation model, an efficient anti-DDoS solution against realistic DDoS attack simulation was provided. Ammune’s response restored the service activity within 30 seconds from the start of the attack, thus preventing long-term damage. The applied IP rotation attacking tactics did not affect the results, as Ammune captured new source IPs and blocked them almost immediately. Apart from a few short service degradations, normal traffic was not affected, with false positives (false blocks) kept at zero in these simulations. Although a few “fresh” bots were not immediately identified during the simulation, this would not happen in reality, where new bots accumulate incriminatory evidence much faster.

The total node population is divided into ‘tiers’, which refers to a grouping of devices that operate at the same logical level in terms of the dependencies between devices and networks. The status of each node is a binary choice between ‘operational’ or ‘failed’, such that at any point in time, the state of system can be summarised by the current number of operational and unavailable nodes. Based on attack rates and node-to-node dependencies, nodes change status stochastically as they are either directly attacked or they suffer from the loss of a node that they are dependent on. This is illustrated in Figure 7.

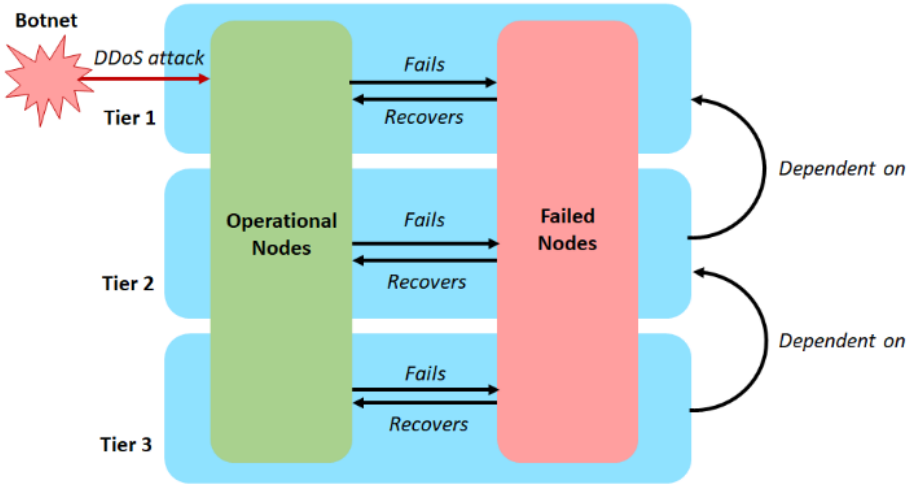

Figure 7. Proposed tiered model

The attack rates are generated by the dynamic attack component, which takes some DDoS parameters (schedule, size, frequency) to deterministically predict the consumption of the target's resources. It is based on server traffic patterns and designed to be generic so that 'resources' may represent different commodities (e.g., processing capacity, memory, bandwidth). As a result of this flexibility, a parallel instance of this component can be created to represent legitimate traffic alongside attack traffic, so that total load on the target may be assessed.

The *SAC* model assumed that all nodes will receive the attack in the same way and are equally likely to become compromised. In reality, the external-facing, remotely-accessible nodes will be the predominant targets. Furthermore, a single DDoS instance will typically be focused on only a few critical devices at a time. To remediate this assumption, the new model extracts potential targets (i.e., nodes with external IT interfaces) into a separate tier. The attack hits the target nodes, and the impact of their diminished service is felt in the rest of the network. The *SAC* model was also deterministic, whilst the new one adds event stochasticity to account for randomness in node failures and recoveries.

New Simulator Overview: The simulator scripts have been updated with a new backend, consisting of a utility server to run REST APIs and business logic, and an SQL database to record client information and energy readings. Alongside this, an intermediary layer between the backend and clients has been added, consisting of 3 PLC aggregators. Each aggregator serves a set of regions and receives data from clients within those regions. This data is then accumulated and periodically forwarded to the backend in bulk. These additions to the simulation environment were designed to better emulate the complexity of the AMI, as well as to add distinct layers (or tiers) that interact with each other. An overview is given in Figure 8.

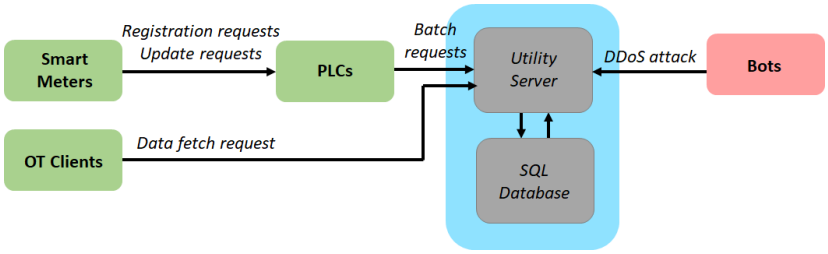

Figure 8. Updated AMI simulator

Figure 9 demonstrates the behaviours of an aggregating PLC in the simulator. A PLC receives a streams of registration requests (*reg_received*). On the PLC, these are aggregated for a period (*reg_pending*), before being pushed to the server. This causes the zig-zag pattern in pending registrations in the chart. Requests are then either valid (*reg_fwd_valid*), blocked (*reg_fwd_blocked*), or timed out (*reg_fwd_timeout*). As there is no attack in this example, *reg_fwd_valid* mirrors (in steps) the peaks and drops of *reg_pending*, steadily increasing as more registration requests are successfully processed. Similar patterns can be observed for update requests, but with larger steps due to the longer intervals for periodic update batches.

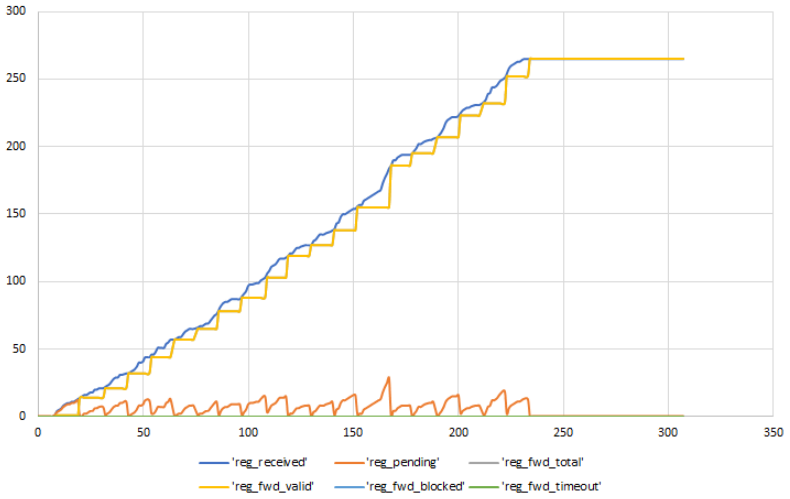

Figure 9. Registrations behaviour on a PLC (2) in the simulator with no attacks

For comparison, Figure 10 shows the logs of an aggregating PLC during a fetch DDoS attack on the server. The PLC still receives registration requests from the clients, but due to the pressure placed on the server, the forwarded requests are now timing out, so that the number of valid (i.e., successfully forwarded) requests is much lower.

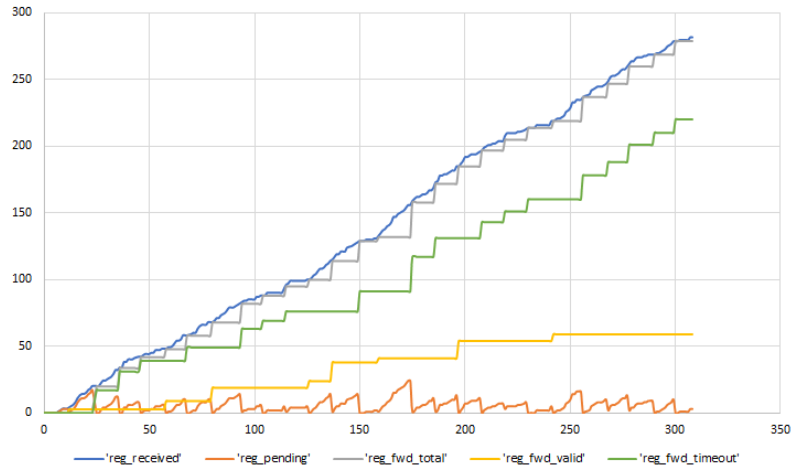

Figure 10. Registrations behaviour on a PLC (1) in the simulator with FET attack

Testing & Validation: A case scenario was created to align the model and the simulator. For this, the model was setup with 3 tiers (labelled *T*, *X*, and *Y*) to represent the backend, the aggregator layer, and the clients. During a fetch attack, the backend server is directly targeted. Therefore, the *T* tier is where the attack lands, and has a population of 1. The PLCs experience failures when the server is compromised, and so the *X* tier is assessed on the basis of these failures, and has a population of 3. Finally, the clients cannot be registered if the PLCs cannot contact the server, and so the total requests that fail to be forwarded by the PLCs is used to assess the *Y* tier. Figure 11 shows some simulator-generated outputs, focused on the compromised populations, and Figure 12 shows the estimates generated by the proposed model.

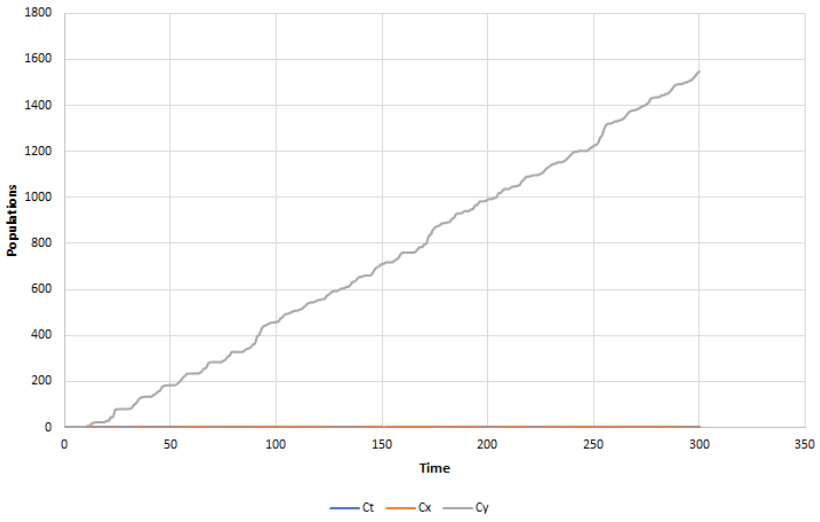

Figure 11. Compromised populations from simulator outputs

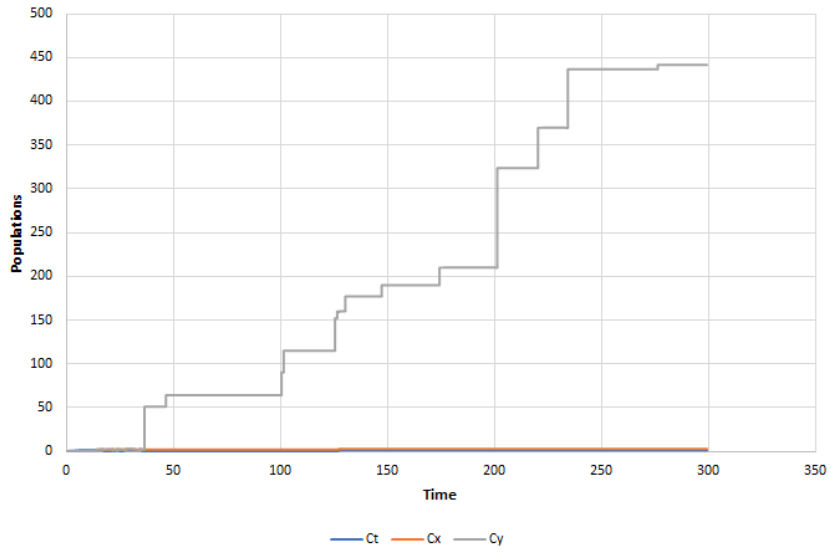

Figure 12. Compromised populations estimated by model

For the *Y* tier, the model's counts are lower due to conservative estimations of meters added per time. This was to keep the model population from growing too rapidly. Also, the line is more stepped because the model randomly adds multiple meters at once, whereas the simulator has a steadier stream of additions over time. Nonetheless, the model is able to approximate the increase trajectory of the *Y* population (as smart meters join the network and try to register via the PLCs). Similarly, a close-up of the *T* and *X* tiers' compromised populations show that the model bluntly approximates that the T and X tiers will be mostly compromised for the duration of the attack, after some initial fluctuation.

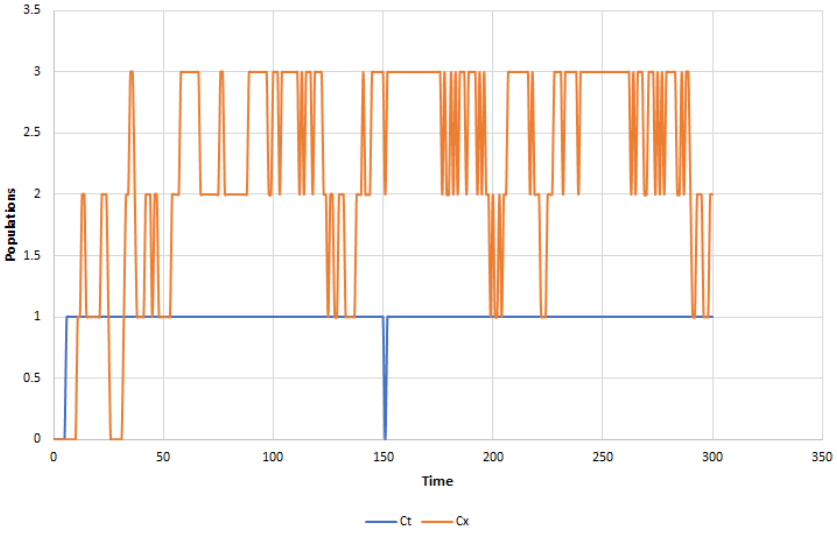

Figure 13. Compromised populations from simulator outputs (close-up)

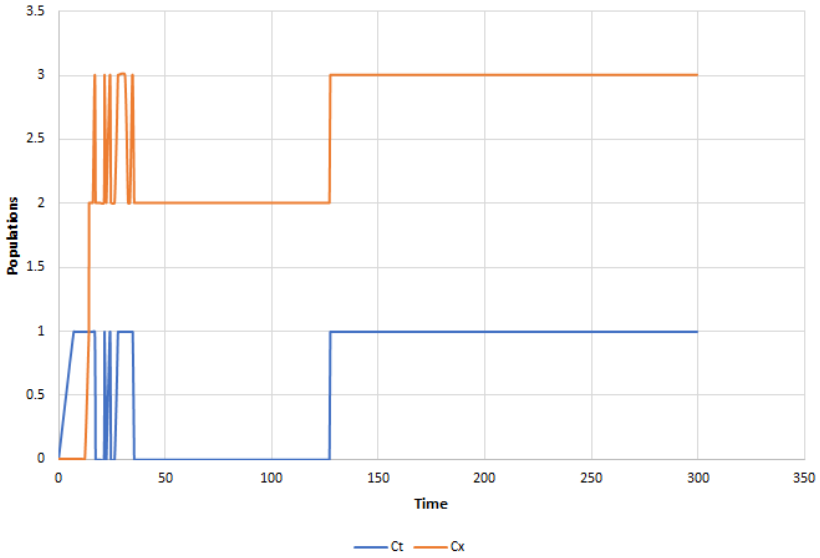

Figure 14. Compromised populations estimated by model

At the time of writing, the work described here has been fully documented as a journal paper for Elsevier Computers & Security, as so full details will be provided therein **[ACM21]**.

Table 7. DDoSM Bulgarion pilot KPI results

Characteristic	Definition	Necesity	F)lexibility (U)sability (A)ccuracy	Will asses s	DDoS	Recommended KPI value	Actual KPI value	Comments
Functional suitability								
Functional completeness	Degree to which the set of functions covers all the specified features and user objectives.	N		n	(Completed Use Cases / Defined Use Cases) * 100 %	100 %	100%	
Functional correctness	System provides the correct results with the needed degree of precision.	N		n	(Completed Use Cases without bugs / Defined Use Cases) * 100 %	>90%	100%	
Functional appropriateness	The functions facilitate the accomplishment of specified tasks and objectives.	N		n	(Accomplished Tasks / Tasks Defined) * 100%	>90%	100%	
Performance efficiency								
Time behaviour	Response, processing times and throughput rates of a system, when performing its functions, meet requirements.	N		Y	(Total Response Time) / (No. of Requests)	<= 1 sec	<= 5 sec	
				n	Total Time Interval from the completion of a task to the achievement score presentation	<= 2 sec	<= 5 sec	
Capacity	Degree to which the maximum limits of a product or	N		n	Number of simultaneous transaction requests	>100	300	

	system parameter meet requirements.							
Compatibility								
Co-existence	Product can perform its functions efficiently while sharing environment and resources with other products.	Y	F	Y	Can DDoS operate in a shared environment?	YES	Yes	
Interoperability	A system can exchange information with other systems and use the information that has been exchanged.	Y	F	Y	Can DDoS exchange information with the rest of the EnergyShield components and other IT corporate tools?	YES	Yes	
Usability								
Appropriateness recognizability	Degree to which users can recognize whether a product or system is appropriate for their needs.	Y	U	Y	(Addressed Business Goals / Defined Business Goals) * 100 %	>90%	100%	
Learnability	Degree to which a product or system can be used by specified users to achieve specified goals of learning to use the product or system with effectiveness, efficiency, freedom from risk and satisfaction in a specified context of use.	Y	U	Y	Learning Hours	< 1 day	< 1 hour	
Operability	Degree to which a product or system has attributes that make it easy to operate and control.	Y	U	Y	Number of clicks required to reach required information	<4	2-3	
User error protection	System protects users against making errors.	Y	U	Y	Does the whole DDoS tool crash on user errors?	NO	NO	
Accessibility	System can be used by people with the widest range of characteristics and capabilities.	Y	U	Y	DDoS tool is accessible and operational through different browsers	YES	Yes	
Reliability								
Maturity	System meets needs for reliability under normal operation.	N		n	No. of Max. Concurrent Users Recorded	>100 users	300	
Availability	System is operational and accessible when required for use.	N		n	1 - ((Downtown Time Minutes) / (Month Days*24*60))	>90%	99%	

				n	(No. of Problematic Requests) / (Total Number of Requests)	<10%	2-3%	
Fault tolerance	System operates as intended despite the presence of hardware or software faults.	N		n	No. of Non-Critical Software Errors	<10	0-1	
Recoverability	Degree to which, in the event of an interruption or a failure, a product or system can recover the data directly affected and re-establish the desired state of the system.	N		n	(No. of Auto-recovered Cases) / (Total Number of Erroneous Cases)	>90%	99.99 %	
Security No. of incidents recorded: 0								
Confidentiality	System ensures that data is accessible only to those authorised to have access.	N		Y	No. of incidents recorded	0	0	
Integrity	System prevents unauthorised access to, or modification of, computer programs or data.	N		Y	No. of incidents recorded	0	0	
Non-repudiation	Actions or events can be proven to have taken place, so that the events or actions cannot be repudiated later.	N		Y	No. of incidents recorded	0	0	
Accountability	Degree to which the actions of an entity can be traced uniquely to the entity.	N		Y	No. of incidents recorded	0	0	
Authenticity	The identity of a subject or resource can be proved to be the one claimed.	N		Y	Can you identify whether a subject is the one it claims to be?	YES	Yes	
					Can you identify whether a resource is the one it claims to be?	YES	Yes	
Maintainability								
Modularity	System is composed of components such that a change to one component has minimal impact on other components.	Y	F	Y	Is DDoS developed in a modular way so that sub-components (tests, games, etc.) function independently?	YES	Yes	
Reusability	An asset can be used in more than one system,	Y	F	Y	Can DDoS be utilized in different business	YES	Yes	

	or in building other assets.				domains and application areas?			
Modifiability	Degree to which a product or system can be effectively and efficiently modified without introducing defects or degrading existing product quality.	Y	F	Y	(No. of updates preformed without noticing operational problems) / (No. of updates performed)	>75%	100%	
Testability	Effectiveness and efficiency with which test criteria can be established for a system.	N		Y	Are tests able to probe the tool behaviour?	YES	Yes	
Portability								
Adaptability	Degree to which a product or system can effectively and efficiently be adapted for different or evolving hardware, software or other operational or usage environments.	Y	F	Y	(No. of Total Errors recorded during Installations) / (Total No. of Installation Environments)	<0.5	0	
Installability	Effectiveness and efficiency with which a system can be successfully installed and/or uninstalled.	N		Y	(No. of Total Errors recorded during Installations) / (Total No. of Installations)	<1	0	
Accuracy*								
Sufficiency	Degree to which data collected by the product can constitute a representative data set.	Y	A	Y	(Number of api domains with full baseline learned / Number of api domains used) * 100 %	>90%	100%	
Coverage	Effectiveness and efficiency with which the product handles the data set collected.	Y	A	Y	Amount of traffic till 90% convergence	<1000*API_Endpoints_tracked	300	
Validity	Degree to which produced by the product results deviate from real-life.	Y	A	Y	(Falsely blocked request portion)	<0.01%	0	
				Y	(Portion of attack blocked after 2mins)	90% in 90% of the benchmark cases	100%	
				Y	(Portion of attack blocked after 5mins)	90% in 99% of the benchmark cases	100%	

* *Accuracy refers to the closeness between the estimated value and the (unknown) true value that the statistics were intended to measure.*

1.8.3. DDOSM BEST PRACTICES AND LESSONS LEARNED

DDoS remains an effective attack vector for threat actors that smart grid networks are susceptible to. Disruptions triggered by successful DDoS attacks can disturb smart grid processes that can subsequently cause imbalance and desynchronization and where the impact is allowed to accumulate and develop. This is because of the tight interconnection of both IT and operational devices, which function in tandem to achieve common goals. To protect the smart grid, incoming DDoS attacks must be blocked or mitigated within the shortest amount of time. The DDoSM tool achieves this through Ammune's immediate dynamic response, which adapts itself to the attack dynamic, which is highly stochastic in nature. The Ammune AI engine was shown to be powerful in adapting itself to these attack conditions, even at very low traffic rates, while protecting sensitive API endpoints without causing damage to normal traffic during the attack mitigation or the learning period. DDoSM is informed by the FC-DDoS model, which captures the dynamics of population compromise given behavioural assessments of a DDoS attack. This is achieved by combining epidemiological modelling methods with dynamic modelling to analyse the grid networks and the attack itself. This contributes a novel approach alongside traditional graph-based approaches and provides validation for enhancements made to Ammune to fit the smart grid context.

1.9. SECURITY INFORMATION AND EVENT MANAGEMENT TOOL

EnergyShield SIEM tool aims to combine the security information management (SIM) with the security event management (SEM), forming a single collaborative security management system.

This system collects critical information from multiple sources and endpoints. These endpoints can be:

- Servers
- Virtual Machines
- Personal computers (laptops, desktops)

from the critical infrastructure that SIEM is assigned to monitor. In the current project, the infrastructure is going to be the EPES sector and the assets from the SCADA system that are connected to one of the endpoints.

The customized and adapted features of SIEM are the following:

- Event Logging
- Distributed Data Storage
- Secure Authorization
- Monitoring
- Incident Response (Countermeasures)
- Alerting
- Visualization
- System Diagnostics

- Learning & Sharing

The initial deployment and the testing of the SIEM solution were developed inside an internal infrastructure of KT. This simple infrastructure, consisting of a server for the SIEM solution, two personal computers and one server for monitoring endpoints, represents part of the SCADA system that is connected to critical assets of the EPES sector, such as RTUs, PMUs, Hydro-plants, among others. Please see D4.4 Final SIEM Solution, released in December 2021.

Furthermore, the SIEM solution was installed in SIMAVI's VPN, to be part of the toolkit. Finally, for the fulfilment of iteration 3, the SIEM solution, was tested In the Bulgarian Pilot, SPEAR Project mirror workstation.

The architecture of the SIEM solution is demonstrated in the figure below, alongside with the rest tools that are connected, as well as the required monitoring endpoints, that it can protect.

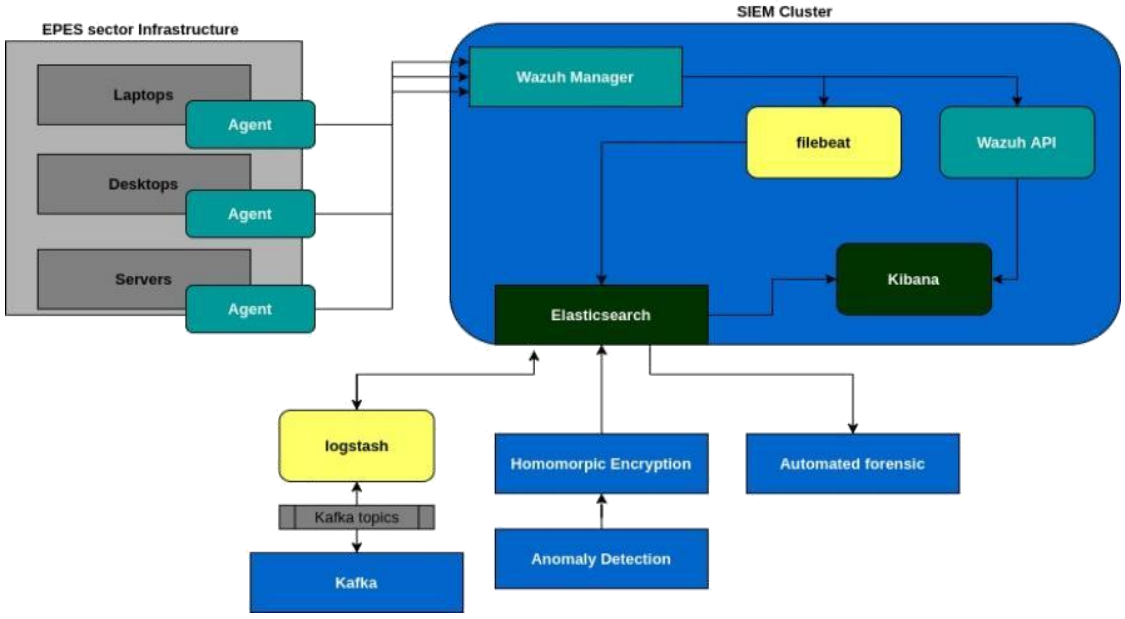

Figure 15. SIEM tool architecture

As it is shown in the above Figure 15, SIEM tool is also adapting two new concept tools: an automated forensic tool by NTUA and a tool for homomorphic encryption by TEC. Both tools are analysed in the following sub-chapters.

1.9.1. SIEM TECHNICAL DETAILS

SIEM consists of the following components:

- Wazuh agents 4.0.4 version
- Wazuh 4.0.4 version
- Elasticsearch 7.9.1 version
- Filebeat 7.9.1 version
- Logstash 7.9.1 version

- Suricata
- SMTP Server (for sharing)
- X-Pack
- Python

The above components are customized to enable the following mechanisms:

- Real-time incidents and events
- Active Response (Countermeasures on attacks)
- Learning and Sharing
- Compliance with other frameworks (MITRE ATTACK, GPDR, NIST)

For more information on the technical details and SIEM Capabilities, please se D4.4 Final SIEM Solution.

1.9.2. SIEM TOOL DEMOSTRATOR

SIEM solution and its concept tools (AF and HE) were tested on the Bulgarian Pilot.

SIEM Solution: A Wazuh agent was installed to a desktop provided in the Bulgarian Pilot, to monitor this endpoint and test SIEM capabilities

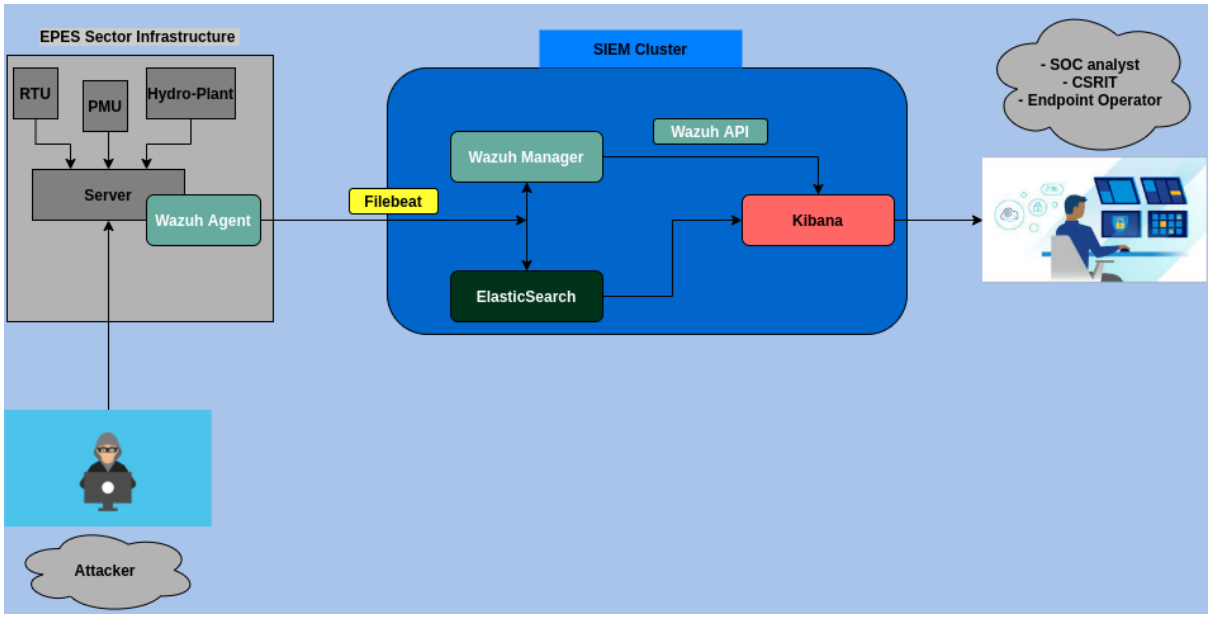

Figure 16. SIEM tool architecture in Pilot

As it is shown in the above Figure 16, the agent sends system logs to the SIEM Cluster, to detect any malicious activity. Moreover, KT enabled the file integrity monitoring, among the capabilities from the previous chapter.

Dummy attacks were made by KT, such as Brute Force Attack, Shellshock Attack, and SQL Injection, for the end-users to have the ability of testing the active response and the learning & sharing mechanism.

As a result, SIEM "caught" malicious activity, as well as system logs, and blocked the attacker IP (deny-host capability for instance). Moreover, the end-user had the ability of "learning" about the attack via correlated SIEM Indices with alerts, as well as they receive alerts notification emails, to protect their infrastructure.

In addition, SIEM also shared the detected vulnerabilities (by SIEM's vulnerability detector) with the automated forensic tool, DDoS for the system logs and retrieved valuable information from the SBA tool via Apache Kafka Topics. Finally, SIEM generated all the alerts to a dedicated Apache Kafka Topic, to be shared on the front-end of the main EnergyShield Toolkit Dashboard.

Due to the sensitive nature and special business needs the specific tool addresses, no further information can be publicly disclosed.

Table 8. SIEM Bulgarian pilot KPI results

Characteristic	Definition	Necessity	(F)lexibility (U)sability (A)ccuracy	Will assess	SIEM	Recommended KPI value	Actual KPIs	Comments
Functional suitability								
Functional completeness	Degree to which the set of functions covers all the specified features and user objectives.	N		Y	(Completed Use Cases / Defined Use Cases) * 100 %	100%	100%	
nFunctional correctness	System provides the correct results with the needed degree of precision.	N		Y	(Completed Use Cases without bugs / Defined Use Cases) * 100 %	>85%	100%	
Functional appropriateness	The functions facilitate the accomplishment of specified tasks and objectives.	N		Y	(Accomplished Tasks / Tasks Defined) * 100%	>85%	90%	
Performance efficiency								
Time behaviour	Response, processing times and throughput rates of a system, when performing its functions, meet requirements.	N		Y	(Total Response Time) / (No. of Requests)	<= 2 sec	<=1 sec	
				Y	Total Time interval to create an alert for a security incident	<= 5 sec	<= 2 sec	
Compatibility								
Co-existence	Product can perform its functions efficiently while sharing environment and resources with other products.	Y	F	Y	Can SIEM operate in a shared environment?	Yes	Yes	

Interoperability	A system can exchange information with other systems and use the information that has been exchanged.	Y	F	Y	Can SIEM exchange information with the rest of EnergyShield components and Pilots?	Yes	Yes	
Usability								
Appropriateness recognizability	Degree to which users can recognize whether a product or system is appropriate for their needs.	Y	U	Y	(Addressed Business Goals / Defined Business Goals) * 100 %	>90%	>90%	
Learnability	Degree to which a product or system can be used by specified users to achieve specified goals of learning to use the product or system with effectiveness, efficiency, freedom from risk and satisfaction in a specified context of use.	Y	U	Y	Learning Hours	< 1 day	2< days <4	
Operability	Degree to which a product or system has attributes that make it easy to operate and control.	Y	U	Y	Number of clicks required to reach required information	<5	<4	
User error protection	System protects users against making errors.	Y	U	Y	Does the whole SIEM tool crash on user errors?	No	No	
Accessibility	System can be used by people with the widest range of characteristics and capabilities.	Y	U	Y	SIEM tool is accessible and operational through different browsers	Yes	Yes	
Reliability								
Maturity	System meets needs for reliability under normal operation.	N		N	No. of Max. Concurrent Users Recorded	> 100 users	Yes	
Availability	System is operational and accessible	N		N	1 - ((Downtown Time Minutes) /	> 85%	100%	

	when required for use.				(Month Days*24*60))			
				N	(No. of Problematic Requests) / (Total Number of Requests)	<10%	<5%	
Fault tolerance	System operates as intended despite the presence of hardware or software faults.	N		N	No. of Non-Critical Software Errors	< 10	No	
Recoverability	Degree to which, in the event of an interruption or a failure, a product or system can recover the data directly affected and re-establish the desired state of the system.	N		N	(Total Recovering Time due to Software Issues) / (Total Software Issues resulting to recovery)	>85%	>90%	
Security: No. of incidents recorded: 215								
Confidentiality	System ensures that data is accessible only to those authorised to have access.	N		Y	No. of incidents recorded	86	86	
Integrity	System prevents unauthorised access to, or modification of, computer programs or data.	N		Y	No. of incidents recorded	13	13	
Non-repudiation	Actions or events can be proven to have taken place, so that the events or actions cannot be repudiated later.	N		Y	No. of incidents recorded	0	0	
Accountability	Degree to which the actions of an entity can be traced uniquely to the entity.	N		Y	No. of incidents recorded	10	10	
Authenticity	The identity of a subject or resource can be proved to be the one claimed.	N		Y	Can you identify whether a subject is the one it claims to be?	YES	YES	
				Y	Can you identify	YES	YES	

					whether a resource is the one it claims to be?			
Maintainability								
Modularity	System is composed of components such that a change to one component has minimal impact on other components.	Y	F	Y	Is SIEM developed in a modular way so that sub-components (tests, games, etc.) function independently?	YES	NO	
Reusability	An asset can be used in more than one system, or in building other assets.	Y	F	Y	Can SIEM be utilized in different business domains and application areas?	YES	YES	
Modifiability	Degree to which a product or system can be effectively and efficiently modified without introducing defects or degrading existing product quality.	Y	F	Y	(No. of updates preformed without noticing operational problems) / (No. of updates performed)	>75%	70%	
Testability	Effectiveness and efficiency with which test criteria can be established for a system.	N		Y	Are tests able to probe the tool behaviour?	YES	YES	
Portability								
Adaptability	Degree to which a product or system can effectively and efficiently be adapted for different or evolving hardware, software or other operational or usage environments.	Y	F	Y	(No. of Total Errors recorded during Installations) / (Total No. of Installation Environments)	<0.7	0	
Installability	Effectiveness and efficiency with which a system can be successfully installed and/or uninstalled.	N		Y	(No. of Total Errors recorded during Installations) / (Total No. of Installations)	<1	0	

Accuracy*								
Sufficiency	Degree to which data collected by the product can constitute a representative data set.	Y	A	Y	(Number of true alarms / Number of alarms used) * 100 %	>85%	3 from the attacks provided by KT for testisting pusrposes	
Coverage	Effectiveness and efficiency with which the product handles the data set collected.	Y	A	Y	(Percentage of assets modelled= All assets and the assets being tracked by the SIEM/Percentage of assets being tracked by the SIEM.)*100%	>85%	100%	Only one desktop was provided by the pilot
Validity	Degree to which produced by the product results deviate from real-life.	Y	A	Y	(Falsely Alerting)	<0.15 %	0	

* *Accuracy refers to the closeness between the estimated value and the (unknown) true value that the statistics were intended to measure.*

1.9.3. SIEM TOOL BEST PRACTICES AND LESSONS LEARNED

SIEM solution helped the end-users to quickly detect abnormal behaviours on the monitoring system. This system was immediately protected via the Active Response mechanism and the whole infrastructure had the ability to learn and get shared the alert notifications. Alerts, actions (countermeasures), emails to specific users, visualizations were provided to better inform the situation inside the infrastructure.

SIEM would have also the ability to retrieve operational data by the integration platform of the Project, however the Bulgarian Pilot was not able to share them due to the high sensitivity of them.

If in future work, these data are shared, then SIEM can raise alerts by investigating the data and given the required threshold from the end-user, to raise operational alerts and provide actions to the end-users, to defend their infrastructure.

By combining information from different data sources and publicly available knowledge bases, the **AF tool** identifies potential attacks and correlates them with vulnerabilities, detects attack patterns, and gathers evidence for adversary techniques. Similar security events noticed within the monitored network that might indicate an ongoing attack are also pinpointed, thus, supporting the forensic investigation and analysis. Most importantly, the AF tool assists in the extraction of

digital evidence and the interpretation of the recovered data while putting them in a logical and useful format. Thus, it leads to the preparation of a written report of findings which can, later on, be used for legal purposes.

Two challenges were faced during the implementation of the **HE tools** which are 1) encrypting the database tables for storing the encrypted data and 2) producing the analytical graph from the encrypted result.

- Firstly, none of the database software provide standard method to convert the plain database structure to encrypted database structures including table name and fields. We have devised an algorithm and implemented a function to take the table name as a parameter along with other database connection parameters and to go through every column and encrypt them to create a new table with the encrypted table name. Every field needs to store 310-character string data, because the searchable encrypted data can fit within 310 characters. By doing this way, the table names and fields will not be vulnerable to hackers.
- The second problem was overcome by devising an algorithm to collect the decrypted result and to form arrays of plain data suitable for passing to a graph function. This tool can be integrated and used not only for energy sector, but also for any sector with little modification of the data model and rewriting respective modules of the tool.

All the traditional encryption schemes such as AES, RC4, DES, 3DES, RC5, RC6, and the Searchable Encryption schemes use either public and private keys or private key only for asymmetric and symmetric encryption respectively. The major problems in encryption are 1) protecting the keys and managing the keys 2) Hackers generate keys randomly to match the actual key. These problems can be overcome by not using the key external to the software or tool which encrypts files or data. In this case, the user does not handle the key at all and not necessary to manage the key as well. Furthermore, the hackers have no opportunity to get hold of the keys to decrypt the files or data and there is no way that a randomly generated key can be applied with the software.

1.10. TOOLKIT

The components for the hardware, software, and communication ports are all contained within the toolkit, which is laid out in a manner resembling a series of shelves or drawers. A portal and an authentication mechanism provide access to the toolkit. Authentication is required. The approach to integration taken by EnergyShield is one that is built upon technology-oriented pillars that support the architectural layers. The common platform is implemented on a Linux machine that is hosted by SIMAVI in a cloud environment.

1.10.1. TOOLKIT 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.

1.10.2. TOOLKIT DEMOSTRATOR

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 produced 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. 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).

Table 9. Toolkit Bulgarian pilot KPI results

Characteristic	Definition	Necessity	(F)lexibility (U)sability (A)ccuracy	Will assess	KPI	Recommended KPI value	Actual KPI value
FUNCTIONAL SUITABILITY							
Functional completeness	Degree to which the set of functions covers all the specified	N		Y	(Completed Use Cases / Defined Use Cases) * 100 %	100%	100%

	features and user objectives.						
Functional correctness	System provides the correct results with the needed degree of precision.	N		Y	(Completed Use Cases without bugs / Defined Use Cases) * 100 %	>85%	1
Functional appropriateness	The functions facilitate the accomplishment of specified tasks and objectives.	N		Y	(Accomplished Tasks / Tasks Defined) * 100%	>85%	1
PERFORMANCE EFFICIENCY							
Time behaviour	Response, processing times and throughput rates of a system, when performing its functions, meet requirements.	N		Y	(Total Response Time) / (No. of Requests)	<= 2 sec	<1sec
Resource utilization		N		Y	No. of max Megabytes of RAM Memory recorded	<1GB	600MB
Capacity	Degree to which the maximum limits of a product or system parameter meet requirements.	N		Y	Max % CPU utilisation recorded	<40%	10%
COMPATIBILITY							
Co-existence	Product can perform its functions efficiently while sharing environment and resources with other products.	Y	F	Y	Can toolkit operate in a shared environment?	YES	YES
Interoperability	A system can exchange information with other systems and use the information that has been exchanged.	Y	F	Y	Can toolkit exchange information with the rest of EnergyShield components and Pilots?	YES	YES
USABILITY							
Appropriateness recognizability	Degree to which users can recognize whether a product or system is appropriate for their needs.	Y	U	Y	(Addressed Business Goals / Defined Business Goals) * 100 %	>90%	99%
Learnability	Degree to which a product or system can be used by specified users to achieve specified goals	Y	U	Y	Learning Hours	<1 day	20h

	of learning to use the product or system with effectiveness, efficiency, freedom from risk and satisfaction in a specified context of use.						
Operability	Degree to which a product or system has attributes that make it easy to operate and control.	Y	U	Y	Number of clicks required to reach required information	<5	4
User error protection	System protects users against making errors.	Y	U	Y	Does the whole toolkit tool crash on user errors?	No	No
User interface aesthetics	N/A	Y	U	Y	Clean user interface?	Yes	Yes
Accessibility	System can be used by people with the widest range of characteristics and capabilities.	Y	U	Y	SIEM tool is accessible and operational through different browsers	Yes	Yes
RELIABILITY							
Maturity	System meets needs for reliability under normal operation.	N		N	No. of Max. Concurrent Users Recorded	> 100 users	200 (In tests with JMETER)
Availability	System is operational and accessible when required for use.	N		N	1 - ((Downtown Time Minutes) / (Month Days*24*60))	> 85%	Not recorded
				N	(No. of Problematic Requests) / (Total Number of Requests)	<10%	7%
Fault tolerance	System operates as intended despite the presence of hardware or software faults.	N		N	No. of Non-Critical Software Errors	< 10	3
Recoverability	Degree to which, in the event of an interruption or a failure, a product or system can recover the data directly affected and re-establish the desired state of the system.	N		N	(Total Recovering Time due to Software Issues) / (Total Software Issues resulting to recovery)	>85%	Not recorded
SECURITY							
Confidentiality	System ensures that data is accessible only to those	N		Y	No. of incidents recorded	0	0

	authorised to have access.						
Integrity	System prevents unauthorised access to, or modification of, computer programs or data.	N		Y	No. of incidents recorded	0	0
Non-repudiation	Actions or events can be proven to have taken place, so that the events or actions cannot be repudiated later.	N		Y	No. of incidents recorded	0	0
Accountability	Degree to which the actions of an entity can be traced uniquely to the entity.	N		Y	No. of incidents recorded	0	0
Authenticity	The identity of a subject or resource can be proved to be the one claimed.	N		Y	Can you identify whether a subject is the one it claims to be?	YES	YES
				Y	Can you identify whether a resource is the one it claims to be?	YES	YES
MAINTAINABILITY							
Modularity	System is composed of components such that a change to one component has minimal impact on other components.	Y	F	Y	Is toolkit developed in a modular way so that sub-components (tests, games, etc.) function independently ?	YES	YES
Reusability	An asset can be used in more than one system, or in building other assets.	Y	F	Y	Can toolkit be utilized in different business domains and application areas?	YES	YES
Modifiability	Degree to which a product or system can be effectively and efficiently modified without introducing defects or degrading existing product quality.	Y	F	Y	(No. of updates preformed without noticing operational problems) / (No. of updates performed)	>75%	Not recorded

Testability	Effectiveness and efficiency with which test criteria can be established for a system.	N		Y	Are tests able to probe the toolkit behaviour?	YES	YES
PORTABILITY							
Adaptability	Degree to which a product or system can effectively and efficiently be adapted for different or evolving hardware, software or other operational or usage environments.	Y	F	Y	(No. of Total Errors recorded during Installations) / (Total No. of Installation Environments)	<0.5	0.3
Installability	Effectiveness and efficiency with which a system can be successfully installed and/or uninstalled.	N		Y	(No. of Total Errors recorded during Installations) / (Total No. of Installations)	<1	0.3
ACCURACY:							
Sufficiency	Degree to which data collected by the product can constitute a representative data set.	Y	A	Y	(Total number in the federation of tools / Number of active tools in tookit) * 100 %	>90%	100%
Coverage	Effectiveness and efficiency with which the product handles the data set collected.	Y	A		Same KPI as above	100%	100%
Validity	Degree to which produced by the product results deviate from real-life.	Y	A	Y	incorect data received from federation member	>5%	1%

* *Accuracy refers to the closeness between the estimated value and the (unknown) true value that the statistics were intended to measure.*

1.10.3. TOOLKIT BEST PRACTICES AND 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 operational technology (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 information technology (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 behaviour analysis to anomaly detection and monitoring); (iv) Component providers spread in several locations; (v) Cultural and language barriers.

Regarding evaluation KPIs, as shown in Table 9, the Bulgarian Pilot report stated that the toolkit was evaluated to meet the majority of the recommended KPI values and that it would not be evaluated for certain KPIs, including availability, recoverability, and modifiability.

CONCLUSION

This task evaluated the effectiveness of the EnergyShield solution and offers recommendations for security upgrades. The report gives an overview of the EnergyShield solution set that was used to show how the technologies made for the project worked. The results showed how potential flaws could affect business continuity and how to effectively address them. Practitioners, or end-users of EPES, assessed pilot results, confirmed anticipated results, and created instructions for employing EnergyShield. We assessed usability, adaptability, and anticipated outcomes. It also contained usage instructions and suggestions for how to make EnergyShield better. Practitioners used replicated use case scenarios to validate the toolkit (pilots). The penetration testing experts tested the infrastructure's susceptibility to attacks and tested all the modules' deployments on a test infrastructure modeled after a production environment. Each tool and its combination are first assessed. The evaluation process is then divided into two phases: design and operation.

To testing the AD and SBA tools created for the project, IREN provided a case study. The electrical distribution system in Turin, which includes the grid operators (who work for the company IRETI, which is controlled by IREN) and the primary high-to-medium voltage substation, is the focus of the case study. The outcomes improved the business's comprehensive cybersecurity strategy. Grid digitalization increases risks and threats, so cybersecurity plays a bigger role. The SBA campaign's findings were used to develop a cybersecurity-focused educational campaign and enhance corporate culture. The cybersecurity team also worked to minimize any potential risk affecting those areas if a critical weakness is found there. The AD detection tool test provided IREN and IRETI with a fantastic opportunity to examine their substations' level of cybersecurity. In fact, the enormous amount of data produced by the field could be both a great opportunity for the development of a smart grid and a potential risk of cyber intrusion. The RTU, PLC, and smart meters used in EnergyShield field testing in Bulgaria, where all participants in the energy value chain took part in an SBA demonstration campaign, were provided to the consortium by the Bulgarian partners. The Siga Box was additionally delivered to the Lenisthta hydroelectric facility to gather operational data, train models, and deploy the AD tool to safeguard the generating infrastructure. To avoid interfering with the network's uninterruptible power supply, the EnergyShield toolbox was installed on a hydropower plant workstation, which was connected in parallel with the plant's regular operation. Utilizing all operational data from a plant, the EnergyShield toolbox can assess its security measures without jeopardizing supply security. The toolkit and the tools were found to be able to meet the majority of the pre-evaluation KPIs based on the results of the Pilots' evaluations.

1.11. CHALLENGES AND LIMITATION

Regarding the Bulgarian Pilot there is a necessity of not to disrupt the uninterruptible generation of electricity to the network. Therefore, a dedicated workstation has been installed in the hydro power plant to host the EnergyShield toolkit. This workstation is connected in parallel with the normal operation of the plant. In that way, the

EnergyShield toolkit can leverage all the operational data of the plant and implement its security mechanisms in a testing environment without jeopardizing security of supply.

REFERENCES

[ESH15] EnergyShield Consortium, leader SIMAVI (2021), D1.5 System architecture (final update), Report, Confidential

[ESH22] EnergyShield Consortium, leader NTUA (2019) D2.2 Security culture framework and tool, Demonstrator, Public

[ESH26] EnergyShield Consortium, leader NTUA (2021) D2.6 Updated security culture framework and tool - final version, Demonstrator, Public

[ESH61] EnergyShield Consortium (2021), D6.1 Offline field trial report

[ESH62] EnergyShield Consortium (2022), D6.2 Online field trial report

[EDE06] Eden, Amnon H., and Tom Mens. "Measuring software flexibility." IEE Proceedings-Software 153.3 (2006): 113-125.

[TER00] Terry Anthony Byrd, Douglas E. Turner. "Measuring the flexibility of information technology infrastructure: Exploratory analysis of a construct." Journal of management information systems 17.1 (2000): 167-208.

[GEO20] Anna Georgiadou, Spiros Mouzakitis, Kanaris Bounas & Dimitrios Askounis (2020) A Cyber-Security Culture Framework for Assessing Organisation Readiness, Journal of Computer Information Systems, DOI: 10.1080/08874417.2020.1845583

[GEO21] Anna Georgiadou, Spiros Mouzakitis & Dimitris Askounis (2021) Detecting Insider Threat via a Cyber-Security Culture Framework, Journal of Computer Information Systems, DOI: 10.1080/08874417.2021.1903367

[GEA21] Georgiadou, A.; Mouzakitis, S.; Askounis, D. Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework. Sensors 2021, 21, 3267. https://doi.org/10.3390/s21093267

[GES20] Georgiadou, Anna, Spiros Mouzakitis and Dimitrios Askounis. “Towards Assessing Critical Infrastructures Cyber-Security Culture During Covid-19 Crisis: A Tailor-Made Survey.” ArXiv abs/2012.13718 (2020): n. pag.

[GEA20] Georgiadou, Anna, Spiros Mouzakitis and Dimitris Askounis. “Designing a Cyber-security Culture Assessment Survey Targeting Critical Infrastructures During Covid-19 Crisis.” ArXiv abs/2102.03000 (2021): n. pag.

[GED20] Georgiadou, A., Mouzakitis, S. & Askounis, D. Working from home during COVID-19 crisis: a cyber security culture assessment survey. Security Journal (2021). https://doi.org/10.1057/s41284-021-00286-2

[SPH19] SPHINX Project EU. SPHINX Project EU. SPHINX.,1 January 2019, Available online: https://sphinx-project.eu/. (Accessed on 19 June 2021).

[GEO22] Georgiadou, A., Michalitsi-Psarrou, A. and Askounis, D. Cyber-Security Culture Assessment in Academia: A COVID-19 Study, DOI: 10.1145/3538969.3544467

[TOY21] Touloumis, K.; Michalitsi-Psarrou, A.; Kapsalis, P.; Georgiadou, A.; Askounis, D. Vulnerabilities Manager, a platform for linking vulnerability data sources (under publication).

[ACM21] Acarali, D., Rao, K.R., Rajarajan, M., Chema, D. and Ginzburg, M.,2021. Modelling Smart Grid IT-OT Dependencies for DDoS ImpactPropagation. In Computers & Security, p.102528.

DEVELOPING THE CYBER-TOOLKIT THAT PROTECTS YOUR ENERGY GRID

www.energy-shield.eu