



# ENERGY SHIELD

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

INNOVATION ACTION

H2020 Grant Agreement Number: 832907

## WP2 - VULNERABILITY ASSESSMENT & SECURITY BEHAVIOUR ANALYSIS

### D2.6 – UPDATED SECURITY CULTURE FRAMEWORK AND TOOL – FINAL VERSION

#### Document info

<b>Contractual delivery</b>	<b>31/12/2021</b>
<b>Actual delivery</b>	<b>31/12/2021</b>
<b>Responsible Beneficiary</b>	<b>NTUA</b>
<b>Contributing beneficiaries</b>	<b>FOR, KTH, SC, IREN</b>
<b>Version</b>	<b>1.0</b>



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



## DOCUMENT INFO

<b>Document ID:</b>	<b>D2.6</b>
<b>Version date:</b>	31/12/2021
<b>Total number of pages:</b>	75
<b>Abstract:</b>	The aim of this deliverable is to present the Security Culture Framework and the corresponding Security Behaviour Analysis tool which shall allow automated planning and implementation of security culture assessment campaigns and training programmes.
<b>Keywords</b>	cyber-security culture, assessment, awareness, security behaviour

## AUTHORS

Name	Organisation	Role
<b>Anna Georgiadou</b>	NTUA	Overall Editor
<b>Ariadni Michalitsi - Psarrou</b>	NTUA	Overall Editor
<b>Dimitris Dimitrakopoulos</b>	NTUA	Editor

## REVIEWERS

Name	Organisation	Role
<b>Per Eliasson</b>	FOR	Overall Reviewer
<b>Lavinia Dinca</b>	SIMAVI	QA Reviewer

## VERSION HISTORY

<b>0.1</b>	04/10/2021	ToC
<b>0.2</b>	02/11/2021	Updated document structure
<b>0.3</b>	10/11/2021	First draft version
<b>0.4</b>	16/11/2021	Updated draft version
<b>0.5</b>	30/11/2021	Version ready for internal review
<b>1.0</b>	17/12/2021	Final version

## EXECUTIVE SUMMARY

The aim of this deliverable (D2.6) is to present the Cyber-Security Culture Framework and the corresponding Security Behaviour Analysis tool that aims to assess and map the socio-cultural behaviour of an organisation's workforce to cyberthreats. The tool is designed and implemented using a holistic approach to easily adapt and adjust to any business domain and, within the context of the project, it was adapted to and is being validated by the EPES sector.

The main purpose of the cyber-security culture framework is to assess and evaluate the current security readiness of an organisation's workforce. It 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.

Both the assessment methodology and the underlying model are thereafter materialised via the development of the Security Behaviour Analysis tool. The respective tool focuses both on user friendliness and business effectiveness while clearly differentiating among the three (3) distinctive security roles implemented: **administrator**, **manager** and **user**.

This deliverable presents:

- The Cyber-Security Culture framework along with its main concepts: levels, dimensions, and domains.
- The evaluation methodology developed based on the suggested security culture model.
- The identification of specific cyber-threats based on the achieved socio-cultural behaviour assessment results exploiting:
  - a hybrid **MITRE ATT&CK** (Adversarial Tactics, Techniques, and Common Knowledge) **Model** for an OT Environment, consisted of a combination of the Enterprise and the ICS threat models,
  - an enriched version of the **MERIT** (Management and Education of the Risk of Insider Threat) model.
- The recommendations and insights based on the findings of our assessment tool and on the threat models used.
- The architecture of the implementation tool and its underlying technologies.
- The structure of the security evaluation tool in accordance with the corresponding assessment methodology.
- The enriched evaluation techniques used to assess the socio-cultural behaviour with the addition of new questionnaires, tests (e.g., password strength test), simulations and games.

- The updated presentation of our tool interfaces allowing its interconnection with both the EnergyShield tools and various others corporate solutions.
- The internationalisation and localisation features of the tool.

## TABLE OF CONTENTS

EXECUTIVE SUMMARY .....	3
Table of Contents .....	5
List of figures .....	7
List of tables .....	9
Acronyms .....	10
1. Introduction .....	11
1.1. Scope and objectives .....	11
1.2. Structure of the report .....	11
1.3. Task dependencies .....	12
2. SBA Tool – Design concept and methodology .....	13
2.1. Cyber-Security Culture Framework .....	13
2.1.1. Model .....	13
2.1.2. Methodology .....	15
2.2. Assessment Results .....	17
2.2.1. Cyber-threats .....	17
2.2.2. Recommendations .....	27
2.3. Application .....	27
3. SBA Tool - Features & Capabilities .....	30
3.1 Tool Architecture .....	30
3.2 Tool Roadmap .....	31
3.3 Interfaces .....	31
3.1.1. REST API .....	32
1.1.1. Kafka Producer .....	37
3.4 Additional Features .....	40
1.1.1. Internationalisation & localisation .....	40
1.1.2. Anonymisation .....	41
4. Proposed innovation & market perspectives .....	42
5. Conclusion and Next Steps .....	46
References .....	47
ANNEX – Security Behaviour Analysis Tool – User Manual .....	49
1. Cyber-Security Culture Framework .....	49
2. Main Concepts .....	49

3. Structure.....	50
1.1. Dashboard .....	53
1.2. Users.....	54
1.3. Groups .....	58
1.4. Reports.....	61
1.5. Self Evaluation .....	63
1.6. Campaigns.....	64
1.7. Assignments .....	68
1.8. Questionnaires.....	69
1.9. Threats .....	71
1.10. Recommendations.....	71
1.11. Tests/Quiz.....	72

## LIST OF FIGURES

Figure 1. Cyber-Security Culture Framework: Main Concepts.....	13
Figure 2. The Cyber-Security Culture Model.....	14
Figure 3. Security culture evaluation methodology.....	15
Figure 4. CERT Insider Threat Types .....	22
Figure 5. SBA validation and integration pillars .....	28
Figure 6. SBA tool performance KPIs.....	29
Figure 7. SBA tool architecture .....	30
Figure 8. SBA tool roadmap .....	31
Figure 9. Exemplary mappings from SBA over MITRE ATT&CK to icsLang. ....	32
Figure 10. Questionnaire localisation .....	40
Figure 11. Competitive comparison of the SBA tool.....	45
Figure 12. Sign-in view .....	51
Figure 13. Console layout .....	52
Figure 14. Dashboard view.....	54
Figure 15. Users view .....	55
Figure 16. User profile view .....	56
Figure 17. Sign-up view .....	57
Figure 18. Create new user wizard .....	58
Figure 19. Groups view .....	59
Figure 20. Group details view.....	60
Figure 21. Create new group wizard .....	61
Figure 22. Reports view .....	62
Figure 23. Self-evaluations view.....	63
Figure 24. Execute new assessment view .....	63
Figure 25. Campaigns view .....	64
Figure 26. Campaign details' view .....	65
Figure 27. Create new campaign view .....	66
Figure 28. Questionnaire assignment execution .....	67
Figure 29. Test assignment execution .....	68
Figure 30. Assignments view .....	69
Figure 31. Questionnaires view .....	70
Figure 32. Questionnaire details view .....	70

Figure 33. Threats view .....	71
Figure 34. Recommendations view .....	72
Figure 35. Test/Quiz views .....	73



## LIST OF TABLES

Table 1. Cyber-Security Culture model relation to MITRE ATT&CK for Enterprise and ICS Mitigations. ....	18
Table 2. Insider Threat Types and Contributing Security Factors .....	23
Table 3. Cyber-Security Culture model relation to Insider Threat factors .....	25
Table 4. Kafka Message Fields .....	38

## ACRONYMS

ACRONYM	DESCRIPTION
DoA	Description of Action
SBA	Security Behaviour Analysis
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
MERIT	Management and Education of the Risk of Insider Threat
UIT	Unintentional Insider Threat
IPT	Intellectual Property Theft
ITS	Information Technology Sabotage
ICS	Industrial Control Systems
CSC	Cyber-Security Culture
IT	Information Technology
OT	Operational Technology
IP	Intellectual Property
USP	Unique Selling Proposition

## 1. INTRODUCTION

### 1.1. SCOPE AND OBJECTIVES

The scope of this deliverable (D2.6) is to present the EnergyShield Cyber-Security Culture Framework and the corresponding Security Behaviour Analysis Tool that aims to assess and map the socio-cultural behaviour of an organisation's workforce to cyberthreats (Task 2.2). More specifically, the objectives of this tool are to:

- perform the assessment of the security culture of an organisation at different levels (organisation, department units, and employees),
- map the socio-cultural behaviour of end-users to specific cyber-threats,
- provide insights for decision-making regarding improving the security culture of the company,
- assist in planning and implementation of security culture training programs.

The results of the SBA tool assessments are further communicated to the EnergyShield Vulnerability Assessment tool via Kafka messages and the REST API, showing the effect of user's cyber awareness and skill in a holistic security context. The Security Behaviour Analysis tool has been integrated with the overall EnergyShield toolkit and is currently validated by the pilot users in the EPES sector.

This deliverable (D2.6) constitutes an updated version of *D2.2 Updated security culture framework and tool*, submitted on M12 of the EnergyShield project, aiming to demonstrate the updates and progress of the tool during its second and third iteration.

### 1.2. STRUCTURE OF THE REPORT

This deliverable presents a cyber-security culture framework for evaluating the readiness of an organisation with an emphasis on the aspects of the human factor. The aforementioned framework, along with its implementation, the Security Behaviour Analysis tool, are being presented in dedicated chapters divided into three sections:

- The first section presents a holistic Cyber-Security Culture framework and assessment methodology built upon security standards and frameworks, as well as a wide and diverse range of scientific studies related to cyber-security behavioural analysis. This section concludes by correlating the framework's evaluation results with specific cyber-threat models leading to targeted recommendations aiming to advance the security readiness and status.
- The second section focuses on the Security Behaviour Analysis tool, implementing the Cyber-Security Culture framework, detailing its architecture, main concepts, interfaces, features and capabilities.
- The third section analyses the market perspectives of the SBA tool while unrevealing its innovative assets.

### 1.3. TASK DEPENDENCIES

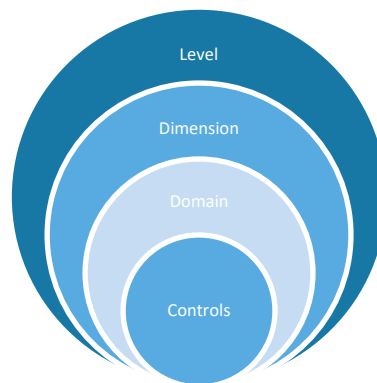
This report presents the Cyber-Security Culture framework as described in Task 2.2: *Map socio-cultural behaviour to cyberthreats and update the SBA tool to provide input to the vulnerability tool*, which is an essential module that interoperates with the Vulnerability Assessment tool (Task 2.1: *Develop a threat model suitable to the EPES sector*). Moreover, it is aligned with the T1.1 (technical requirements) rolled-out in parallel with T1.2 (commercial requirements), T1.3 (regulatory requirements) and all the reports related to the landscape of EnergyShield requirements. Lastly, this report is in alignment with the detailed architecture and technical specifications of the EnergyShield toolkit as documented in *D1.4 System architecture v1* and *D1.5 System architecture-final update* (Task 1.4: *Design the overall system architecture*). The Security Behaviour Analysis tool has been integrated into the EnergyShield Toolkit in the context of Tasks 5.1 - 5.4, as presented in D5.1 – D5.6, and is currently being validated by the pilot users in the context of Tasks 6.1 – 6.3.

## 2. SBA TOOL – DESIGN CONCEPT AND METHODOLOGY

### 2.1. CYBER-SECURITY CULTURE FRAMEWORK

The Cyber-Security Culture Framework was developed in the context of the EnergyShield project and was originally presented in the scientific community in 2020 [GEO20]. Its model constitutes a foundation of **organisational** and **individual** security factors organised into **dimensions** and **domains**, as depicted in Figure 1.

Its elements derive from a thorough and multi-dimensional literature review and research analysis of the current cyber-security reality. It was originally designed to examine organisational security infrastructure, policies and procedures jointly with employees' individual characteristics, behaviour, attitude and skills. Thus, bridging the professional with the scientific approach, the external with the internal indicators directly or indirectly related with cyber-security culture. However, most importantly, a framework co-examining all these security facets with their many interactions and under a complicated business fabric.



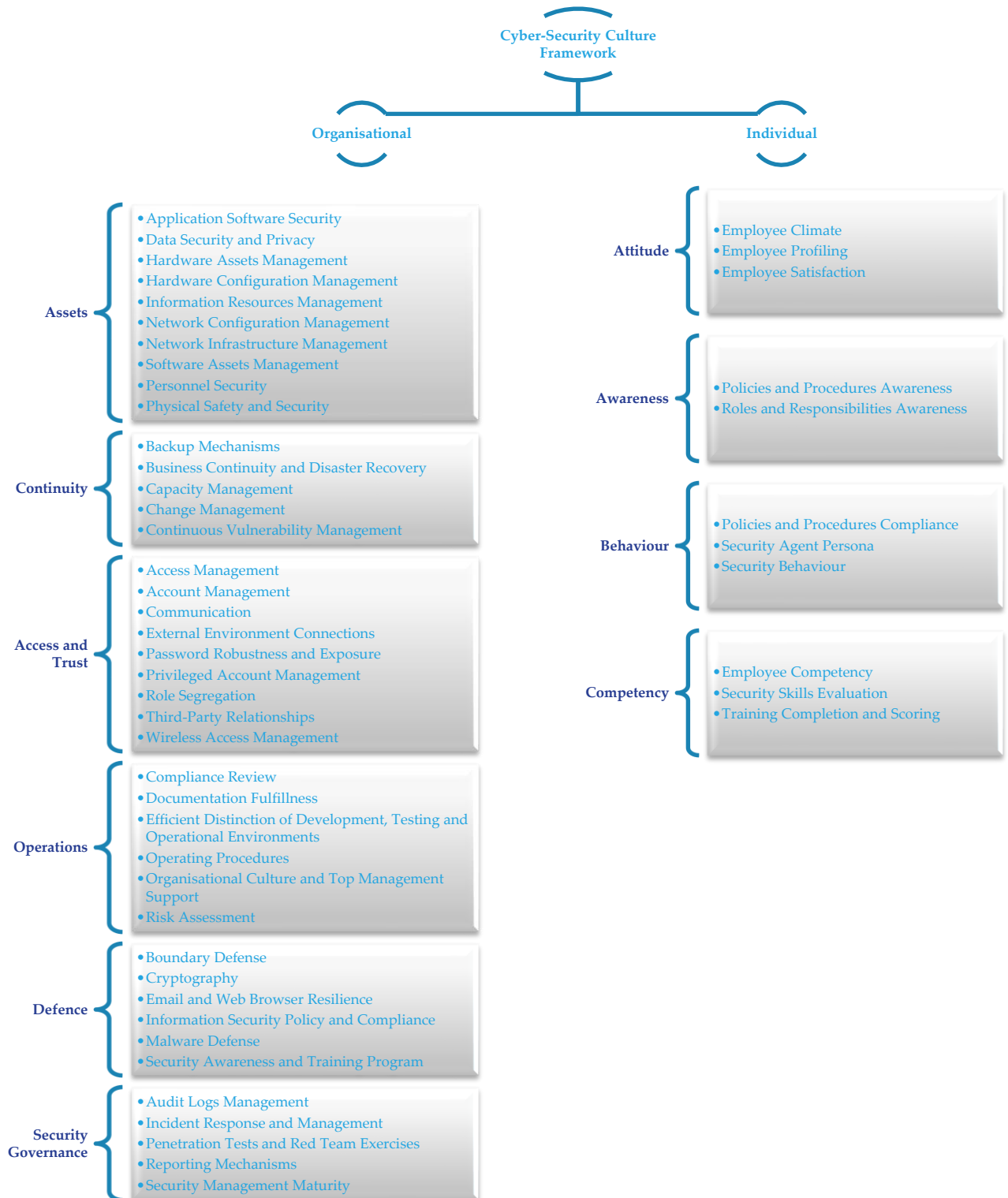
**Figure 1. Cyber-Security Culture Framework: Main Concepts**

#### 2.1.1. MODEL

The Cyber-Security Culture Framework organises security culture indicators into two levels: **organisational** and **individual**, as depicted in Figure 2. Each dimension of the 1st level corresponds to a security facet that each organisation is meant to address using a combination of IT solutions and security countermeasures. On the other hand, dimensions of the 2<sup>nd</sup> level are meant to address individual attributes directly affecting the overall security readiness of a business environment [GEA21].

Dimensions are further split into domains analysing the different aspects of each security facet. For example, dimension “Assets” refers to security policies that enforce several levels of confidentiality, availability and integrity controls on the organisation’s assets (including people, buildings, machines, systems and information assets) [GEO20]. Its domains are meant to organise these controls into the different asset categories and security management facets related to them. Therefore, some of the domains met into this dimension are “Hardware Assets Management” and “Hardware Configuration Management,” “Network Infrastructure

Management” and “Network Configuration Management,” “Software Assets Management” and “Information Resources Management.” Similarly, each security dimension of this framework presents, in a structured way, the distinctive security application areas of an organisation reaching down to quantifiable indicators.



**Figure 2. The Cyber-Security Culture Model**

A detailed presentation of the Cyber-Security Culture Model, clearly defining each one of its levels, dimensions, and domains, has been introduced in *D2.2 Updated security culture framework and tool*, submitted on M12 of the EnergyShield project.

Each domain is then attributed to a number of metrics that can be properly assessed and measured using a variety of evaluation techniques varying from simple surveys and observation techniques and reaching up to more sophisticated methods, such as simulations and serious games.

### 2.1.2. METHODOLOGY

The Cyber-Security Culture Model represents the key security metrics to be measured along with their dependencies, influences and varieties. The next step was to define an evaluation methodology that not only enables an organisation to illustrate a uniform representation of its everyday reality but also assists in identifying its vulnerabilities and weaknesses [GEO20].



**Figure 3. Security culture evaluation methodology**

As depicted in Figure 3, the evaluation methodology consists of clearly defined and easily comprehensible steps. Starting from the decision of performing a security assessment process either due to an organisation board's initiative (which is usually the case) or driven by the need to defend against the numerous cyberthreats of current reality (possibly after an unexpected real-life incident). The decision-making group, bearing in mind the real reasons behind this endeavour, need to set the initial goals and provide proper business requirements. Depending on their expectations, the entire methodology shall be respectively targeted in means of groups and security domains.

In the next step, evaluation iterations, so-called assessment **campaigns**, are being planned by managers and team leaders with proper variations among the different user groups, teams or even organisation sections and departments. Bearing in mind the targeting results of the previous step, they calibrate and carefully and collaboratively design the evaluation procedure which takes place in the next step. Using proven techniques, such as testing, examination, interviewing, simulation,

gamification and many others, gather as much information as possible from its participants.

Reaching to the most demanding step of the methodology, results are being gathered and analysed via a series of sophisticated weighting algorithms and statistical computations generating a number of graphical representations and reports at an individual as well as organisational level. Using the score generated by the evaluation procedure for each targeted individual (analysed into the different dimensions and domains), the methodology proceeds in appropriately aggregating them along with the organisational related ones producing corresponding scores for sections, departments, units and ultimately for the organisation as a whole.

Finally, the acquired results pinpoint the existing security weaknesses and gaps, allowing security training programs' personalisation and adaptation to user-specific needs. Suggestions and recommendations are being provided both to individuals and directors while the decision-making board is armed with the knowledge of their security culture status along with its pain points.

An indicative simplified scenario to serve as an example of all of the above would be as follows. The security officers of company X have been alerted by the security operation centre (SOC) solution at hand that an excessive number of fraud emails are reaching their marketing department. After further investigating, they have also verified a misuse of social channels from its employees. Consequently, they have reached the decision to run an assessment campaign targeting this specific department. Since their focus lies on email, web and social media usage, they include to their campaign a number of relative questionnaires, phishing simulation tests, social engineering games and email and password exposure checks. After the expiration date of the campaign, the security officers gather the results and, via a graphical representation, are able to understand both the security vulnerabilities they are up against as well as their magnitude. Would the users accept and activate a virus received as an attachment via an email? Would someone reply to a phishing email providing important personal or corporate information? Do they understand the dangers they are up against by the exposure they have as members of the marketing department (email addresses available to the public)? Do they conform with the password policies of the company? Knowing where more employees failed to live up to the expectations, they can proceed in building their defence and calibrating existing technological assets to protect them and, more importantly, educate them and arm them against the cyber-threats they face. Not to mention that, via the evaluation process, they have already triggered them and initiated a security cultural zymosis.



## 2.2. ASSESSMENT RESULTS

### 2.2.1. CYBER-THREATS

#### 2.2.1.1. HYBRID MITRE ATT&CK ENTERPRISE AND ICS MODEL

The **MITRE ATT&CK** (Adversarial Tactics, Techniques, and Common Knowledge) Framework provides a rich and actionable repository of adversarial tactics, techniques, and procedures. Its innovative approach has been broadly welcomed by both vendors and enterprise customers in the industry. Its usage extends from adversary emulation, red teaming, behavioural analytics development to a defensive gap and SOC (Security Operations Centre) maturity assessment. While extensive research has been done on analysing specific attacks or specific organisational culture and human behaviour factors leading to such attacks, a holistic view on the association of both was missing.

Therefore, during the 2<sup>nd</sup> year of the EnergyShield project, we have conducted scientific research aiming to associate our Cyber-Security Culture (CSC) framework with security vulnerabilities mapped to specific adversary behaviour and patterns utilising the MITRE ATT&CK framework. Thus, we have exploited MITRE ATT&CK's possibilities towards a scientific direction that had not yet been explored: security assessment and defensive design, a step prior to its current application domain.

The CSC framework was designed to aim at critical infrastructures and, more specifically, the energy sector. Organisations of these domains exhibit a co-existence and strong interaction of the IT (Information Technology) and OT (Operational Technology) networks. As a result, we emphasised our scientific effort on the **hybrid MITRE ATT&CK for Enterprise and ICS** (Industrial Control Systems) model as a broader and more holistic approach. The results of our research can be utilised in an extensive set of applications, including the efficient organisation of security procedures as well as enhancing security readiness evaluation results by providing more insights into imminent threats and security risks. Our research has been introduced to the scientific community via a journal article published in early 2021 [[GEA21](#)].

Table 1 presents a many-to-many relationship between the Cyber-Security Culture model and the hybrid MITRE ATT&CK for Enterprise and ICS mitigation list. Seemingly, the assessment results of many different security domains need to be jointly examined to evaluate the fulfilment of a number of mitigations along with the risk of numerous possible ATT&CK TTPs (Tactics, Techniques and Procedures).

**Table 1. Cyber-Security Culture model relation to MITRE ATT&CK for Enterprise and ICS Mitigations.**

Level	Dimension	Domain	MITRE ATT&CK Mitigation
<b>Organisational</b>	<b>Assets</b>	Application Software Security	M0813
			M0815
			M1013
			M1040
			M1042
			M1045
		Data Security and Privacy	M0803
		Hardware Assets Management	M0813
			M1034
		Hardware Configuration Management	M0815
			M1024
			M1028
			M1039
			M1046
		Network Configuration Management	M0814
			M1037
		Network Infrastructure Management	M1037
		Software Assets Management	M0815
			M1033
			M1038
			M1040
			M1042
			M1044
			M1045
			M1048
			M1054
		Personnel Security	M0804
		Physical Safety and Security	M0805
			M0812
	<b>Continuity</b>	Backup Mechanisms	M1029
			M1053
		Business Continuity & Disaster Recovery	M0810
			M0811
		Continuous Vulnerability Management	M1053
			M1016
			M1051

	<b>Access and Trust</b>	Access Management	M0800 M0801 M1015 M1022 M1030 M1035
		Account Management	M1015 M1018 M1032 M1036 M1052
		Password Robustness and Exposure	M1027 M1043
		Privileged Account Management	M1025 M1026
		Role Segregation	M0800
		Wireless Access Management	M0806
	<b>Operations</b>	Efficient Distinction of Development, Testing and Operational Environments	M1048
		Risk Assessment	M1019
	<b>Defense</b>	Boundary Defense	M0802 M0807 M0808 M0809 M1020 M1031
		Cryptography	M1041
		Email and Web Browser Resilience	M1021
		Malware Defense	M1049
		Security Awareness and Training Program	M1017
	<b>Security Governance</b>	Audit Logs Management	M1047
		Penetration Tests and Red Team Exercises	M1050
<b>Individual</b>	<b>Behavior</b>	Security Behavior	M1017
	<b>Competency</b>	Security Skills Evaluation	M1017 M1027

		Training Completion and Scoring	M1017
--	--	------------------------------------	-------

*Note: ATT&CK Mitigation “M1055—Do Not Mitigate,” which is meant to associate with techniques that mitigation might increase risk of compromise and therefore mitigation is not recommended and has been omitted from this table.*

The Cyber-Security Culture framework has been created using a multidisciplinary approach towards information security. Therefore, its elements are meant to attribute to all different aspects of a business environment, including internal and external, organisational, and individual factors. MITRE ATT&CK, on the other hand, has been developed based on an extensive knowledge base of witnessed and documented violation incidents mainly related to technological-driven techniques. In other words, it is meant to describe how adversaries can take advantage of specific IT and OT vulnerabilities and weaknesses to achieve certain malicious goals. Consequently, cyber-security culture, due to its originating purposes, bears a broader nature than ATT&CK. Therefore, detection of MITRE ATT&CK risk does not require the evaluation of all dimensions and domains of the cultural framework. At least, in its current version, since the ATT&CK knowledge base is constantly evolving following the concurrent cyber-crime transformation.

As witnessed in Table 1, all six of the organisational dimensions participate in the ATT&CK risk assessment but without exploiting all sub-domains. Similarly, at the individual level, only two out of four dimensions are used. “Attitude” and “Awareness”, deriving from humanitarian sciences, are not immediately related to TTPs. These dimensions are, on the other hand, used to identify the Insider Threat (as presented in the following paragraph), which is not practically addressed using the ATT&CK technical approach.

To summarise the above, Table 1 reveals how starting from an overall security assessment of an organisation, using a structured evaluation methodology, one can exploit results related to specific security indicators to identify which security measures have not been properly implemented. Thus, understanding the ATT&CK TTPs the organisation is vulnerable against.

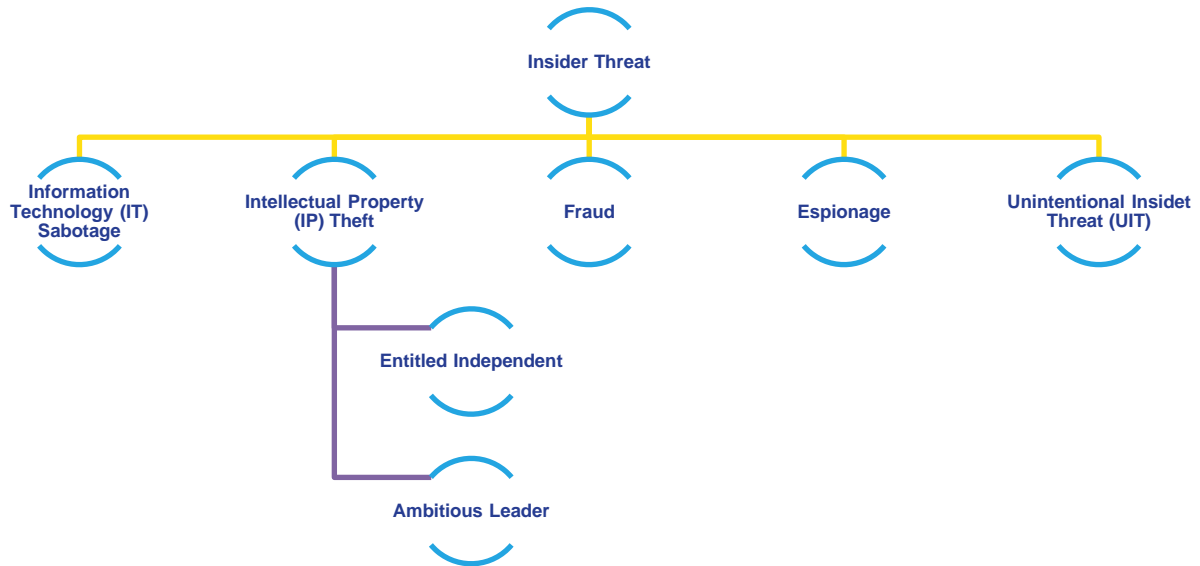
#### 2.2.1.2. MERIT MODEL

**The insider threat** has been recognised by both the scientific community and security professionals as one of the gravest security hazards for private companies, institutions, and governmental organisations. Over the last decades, extensive research on the types, associated internal and external factors, detection approaches, and mitigation strategies has been conducted. Various frameworks have been introduced in an attempt to understand and reflect the danger posed by this threat, whereas multiple identified cases have been classified in private or public databases.

During the 2<sup>nd</sup> year of the EnergyShield project, we have conducted extensive research related to the insider threat, which concluded to a journal publication [GEO21] presenting how the Cyber-Security Culture framework, with a clear focus on the human factor, can assist in detecting possible threats of both malicious and unintentional insiders. We have linked current insider threat categories with specific security domains of the framework and introduced an assessment methodology of the core contributing parameters. The specific approach takes into consideration technical, behavioural, cultural, and personal indicators and assists in identifying possible security perils deriving from privileged individuals.

In doing so, we have exploited one of the most recognisable and commonly accepted insider threat categorisations, the one proposed by the “**Insider Threat Study**”, a joint project conducted by the Secret Service and the Software Engineering Institute CERT Program at Carnegie Mellon University. Since 2001, the CERT National Insider Threat Center has conducted a variety of research projects on insider threat based on an expanded corpus of more than 1,500 cases from organisations across all industries. Their scientific contribution is demonstrated via a variety of publications throughout their long-standing presence in the domain. Though the attack methods vary depending on the industry, they have identified, analysed, and presented via several technical reports the main insider threat types and their subcategories, as a part of the **Management and Education of the Risk of Insider Threat (MERIT)** project:

- **Information Technology (IT) Sabotage:** Use of IT to direct specific harm toward an organisation or an individual.
- **Intellectual Property (IP) Theft:** Purposely abuse one’s credentials to steal confidential or proprietary information from the organisation.
  - **Entitled Independent:** An insider acting primarily alone to steal information to take to a new job or their own side business.
  - **Ambitious Leader:** A leader of an insider crime who recruits insiders to steal information for some larger purpose.
- **Fraud:** Unauthorised modification, addition, or deletion of an organisation’s data for personal gain, or theft of information that leads to an identity crime (e.g., identity theft, credit card fraud).
- **Espionage:** Obtaining, delivering, transmitting, communicating, or receiving information about the national defence with an intent, or reason to believe, that the information may be used to the injury of own’s country or the advantage of any foreign nation.
- **Unintentional Insider Threat (UIT):** Negatively affect the confidentiality, availability, or integrity of an organisation’s information or information systems via action or inaction without malicious intent.



**Figure 4. CERT Insider Threat Types**

We have then conducted a critical review of the scientific community research approaches, the available empirical literature findings and the corporate security professionals' testimonies related to the **insider threat factors**. This review resulted in a number of behavioural and technical, individual and organisational, qualitative and quantitative indicators practically affecting and formulating fertile ground for increased insider threat probability.

The next logical step was to classify the identified insider threat factors into umbrella terms unifying them and limiting them down to measurable security indicators, which can be addressed by the Cyber-Security Culture framework. Based on the semantic and contextual interpretation of the initially identified security factors, we closely studied their definitions and analysis based on the referenced research studies. We investigated the assessment approaches and validation techniques used by the aforementioned references in order to identify overlaps and relationships among these factors leading to unifications and classifications, concluding with the 11 key insider threat factors presented in Table 2.

**Table 2. Insider Threat Types and Contributing Security Factors**

	ITS	IPT	Fraud	Espionage	UIT
1 – Dissatisfaction: Stressful events, either work-related or personal, typically precede insider attacks. Examples of such events include employee dismissal, disputes with employers, perceived injustices, transfers or demotions, salary reductions, family problems. Dissatisfaction resulting from stressful events triggers concerning behaviors in individuals predisposed to malicious acts.		  (only for Entitled Independent)			
2 - Personality predispositions: Personality predispositions include serious mental health disorders, personality issues (e.g., self-esteem deficits, patterns of biased perceptions of self and others), addictions, social skills and decision-making deficits, history of legal, security or procedural rule violations. Specific personality traits, such as openness, extraversion, agreeableness, conscientiousness, risk perception and tolerance, which have been identified as related to specific security behaviours, have also been included in this umbrella term.					
3 – Enterprise role: The position an insider holds within an organisation (e.g., technical, managerial) along with the special skills, knowledge, privileges (e.g. domain or system administrator, advanced user), and access granted may seriously differentiate both the possibility as well as the type of insider threat posed against the enterprise he/she works for.					
4 – Concerning behaviour: Concerning behaviours, including personnel and security violations, precede the vast majority of insider cases prior to their attacks. Examples of such behaviours include tardiness, truancy, arguments with co-workers, poor job performance, security violations.					

5 – Employee profile: Employee profile, built based on a number of human attributes such as age, gender, tenure, level of seniority, have been examined in many cases of insider incidents and credited with a contributing role to the overall insider threat predisposition. Since these attributes are only parameters in a multidimensional issue, it is only fair to group them and examine them in combination. In other words, simply being a male senior engineer does not make one more prone to cyber-attacking your employer compared to a woman holding the same position.				
6 – Access Controls: Physical access controls (restrictions on gaining access to organisational facilities) and/or remote access controls (restrictions to computing and network enterprise resources) enforce organisational defence against the insider threat. However, lack of those controls or possible deficiencies in their enforcement encourage insider incidents allowing their prolong occurrence.				
7 – Sense of entitlement: This factor is being met only in cases of intellectual property theft and refers to the degree to which insiders felt entitled to information they stole. Information in these cases refers to work results produced by the insiders during their occupation in the victimised enterprise regardless of having or not signed relevant agreements or contracts.				
8 – Policy violation: Policy violations may be behavioural or technical in nature. This indicator is used to evaluate employees' compliance with the security policies and procedures in place.				
9 – Auditing: Auditing is used to describe and assess the ability and means an organisation utilises to detect, evaluate, and react against policy violations, technical or not, in order to prevent actual insider attack cases via positive or negative framing				



techniques.

10 – Policies and roles awareness: Enterprise policies and procedures awareness along with roles and responsibilities knowledge differentiate deliberate to unintentional security violations.

I

11 – Situation awareness: Unintentional insider incidents often result from information technology and security unfamiliarity and unawareness. Simple examples of this category include trusting a phishing email, visiting an unreliable website, downloading an executable file which contains more than it supposed to.

I

Our ultimate goal being to identify possible insider threats to an organisation based on its cyber-security culture assessment, we proceeded in identifying the security domains of our framework directly related to the 11 key insider threat factors presented in Table 2. Evaluation results from these security domains could assist in pinpointing potential insider risks when examined in combination, as presented in Table 3.

**Table 3. Cyber-Security Culture model relation to Insider Threat factors**

Level	Dimension	Domain	Insider Threat Factor
<b>Individual</b>	Attitude	Employee Satisfaction	1 - Dissatisfaction
		Employee Profiling	3 – Enterprise role 5 – Employee profile
	Awareness	Policies and Procedures Awareness	10 – Policies and roles awareness
		Roles and Responsibilities Awareness	10 – Policies and roles awareness
	Behaviour	Policies and Procedures	8 – Policy violation

		Compliance	
		Security Agent Persona	2 - Personality predispositions 7 – Sense of entitlement
		Security Behaviour	4 – Concerning behaviour
	Competency	Security Skills Evaluation	11 – Situation awareness
		Training Completion and Scoring	11 – Situation awareness
<b>Organisational</b>	Assets	Personnel Security	6 – Access Controls
	Access & Trust	Access Management	6 – Access Controls
	Defence	Information Security Policy & Compliance	9 – Auditing
	Security Governance	Audit Logs Management	9 – Auditing
		Incident Response & Management	9 – Auditing

As anticipated, insider threat risk is mainly addressed by the **individual level** of the suggested framework, which relates to the employee attitude, awareness, competency, and behaviour. In order to address the detailed personality predispositions dictated by the insider threat factors and link them directly with the “Behaviour” of the individuals, we enriched the controls used for the evaluation of this security dimension of our framework. More specifically, we enhanced the “Security Agent Persona” and the “Security Behaviour” domains by including measurement instruments exploring a variety of psychological constructs related to security behaviour, such as Domain-Specific Risk-Taking Scale [[ARB06](#)], General Decision-Making Style [[SGS95](#)], Consideration for Future Consequences [[SGB94](#)],

Barratt Impulsiveness Scale [PSB95], Need for Cognition [CPR82], Security Behaviour Intentions Scale [EPE15].

The few organisational dimensions and domains which contribute to the overall insider risk assessment are directly linked to the physical and digital access control management along with the security compliance auditing, monitoring and incident response management. Consequently, the proposed framework may indeed identify, among other possible cyber-threats or deficiencies, insider perils given a specific working reality.

### 2.2.2. RECOMMENDATIONS

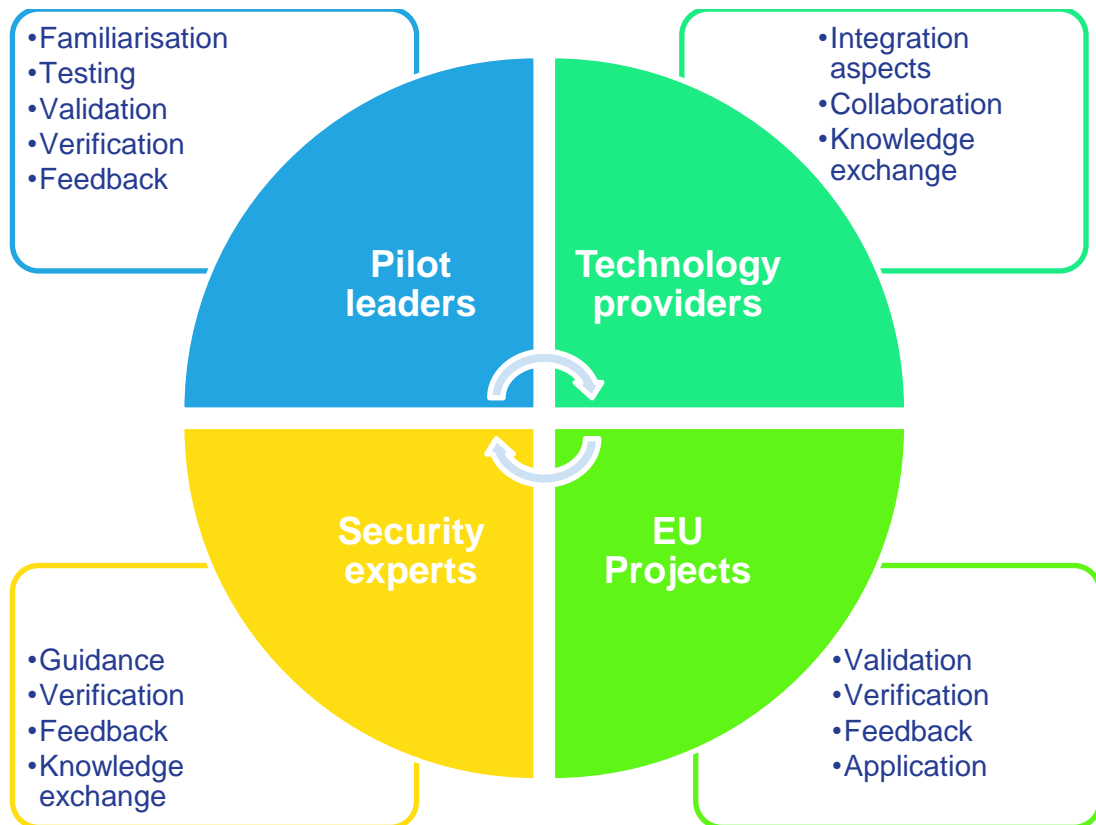
As described in detail in the previous paragraphs, the Cyber-Security Culture Framework has been related to the MITRE ATT&CK and MERIT models leading to the identification of possible adversary techniques an organisation is vulnerable against. Based on the mitigation strategies and patterns of the aforementioned models, the CSC framework proceeds in offering targeted insights for decision-makers regarding improving the security culture of the company. Towards that end, the CSC framework assists in planning and implementation of security culture training programs based on the identified cyber-threat perils.

## 2.3. APPLICATION

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 organisations. 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 CSC framework assisted SPHINX security specialists in the design of a two-phase security awareness campaign targeting health sector personnel.

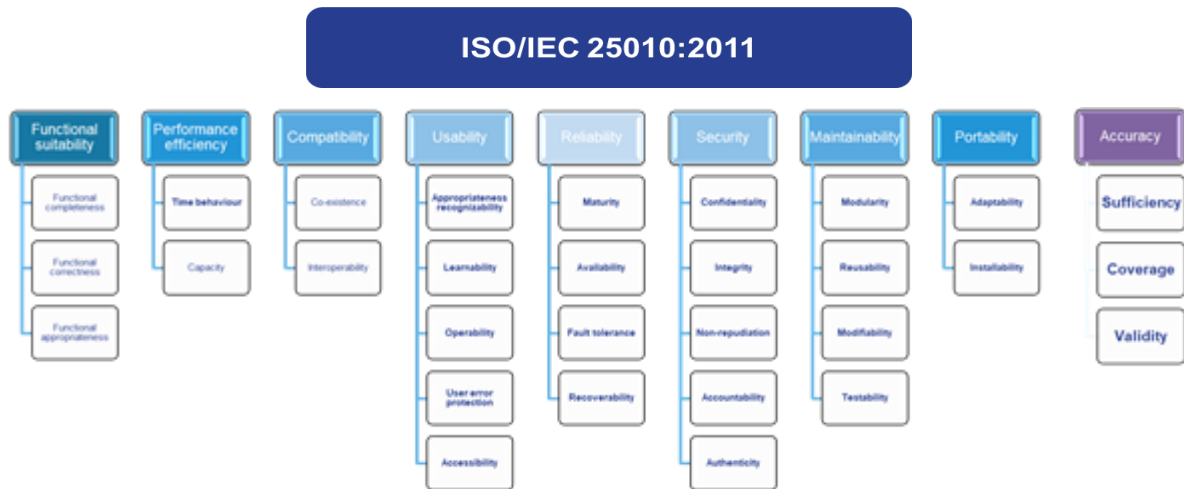
The CSC and its implementation tool, SBA, were evaluated and exploited in both wide application scenarios while gaining recognition by IT and security specialists of different business domains. The feedback provided throughout the process assisted in improving our methodology and approach towards end-users.



**Figure 5. SBA validation and integration pillars**

The SBA tool has been integrated into the EnergyShield Toolkit in the context of Tasks 5.1 - 5.4, as presented in D5.1 – D5.6, and is currently being validated by the pilot users in the context of Tasks 6.1 – 6.3. Their contribution throughout the design, development and integration phases of the tool was of great significance, improving and calibrating the tool to the EPES sector needs and challenges.

For the evaluation of the SBA tool, a product quality model composed of eight characteristics (which are further subdivided into sub-characteristics) shall be exploited. This model is being presented in the **ISO/IEC 25010:2011** standard. The characteristics and sub-characteristics provide consistent terminology for specifying, measuring, and evaluating system and software product quality. They also provide a set of quality characteristics against which stated quality requirements can be compared for completeness. This model has been extended with an extra characteristic, and associated sub-characteristics, in order to address features related to the accuracy of the expected results, as presented in Figure 6.



**Figure 6. SBA tool performance KPIs**

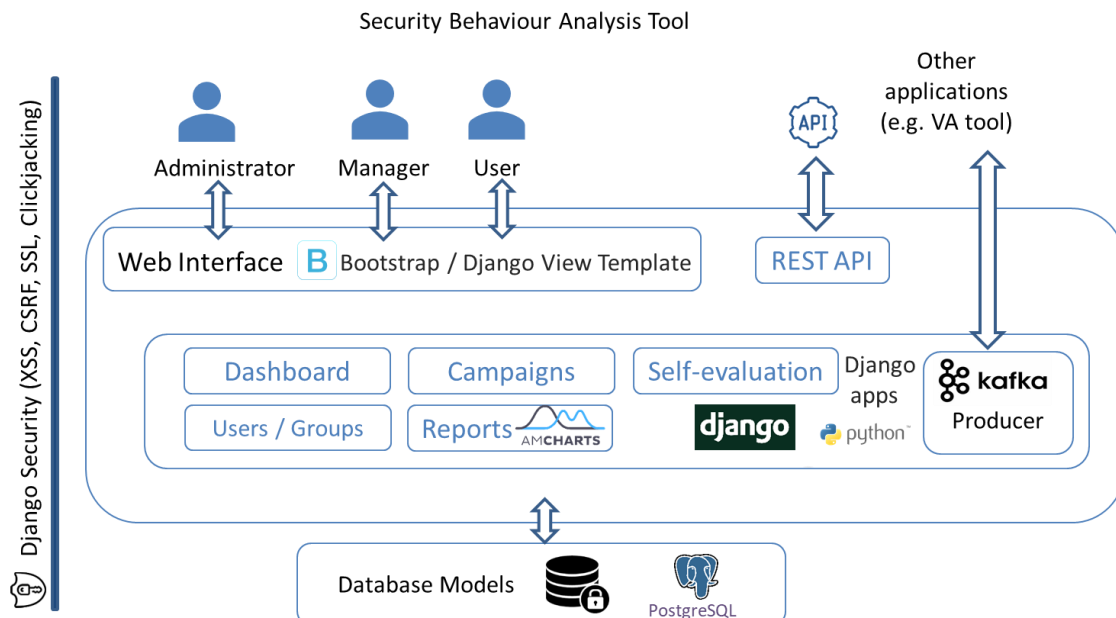
Based on the model, a list of KPIs has been defined to allow the technical evaluation of the SBA tool alongside the rest of the EnergyShield components as part of the WP6 integration and evaluation plan, which shall be demonstrated as part of D6.3.

### 3. SBA TOOL - FEATURES & CAPABILITIES

#### 3.1 TOOL ARCHITECTURE

The Security Behaviour Analysis (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 7. 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).

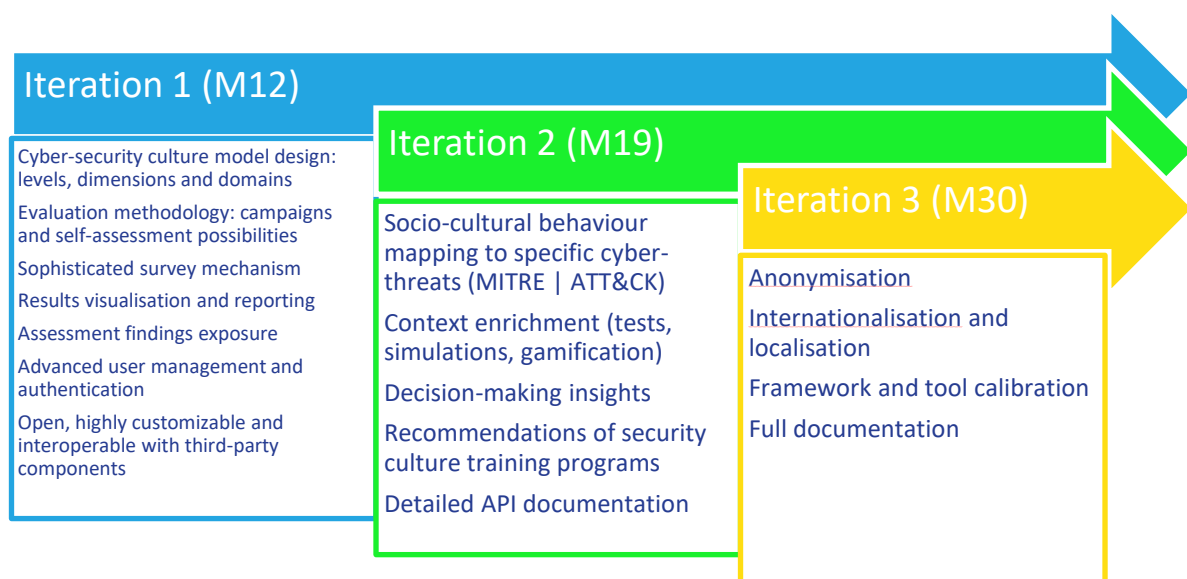


**Figure 7. SBA tool architecture**

The source code is being hosted on NTUA's GitLab environment.

### 3.2 TOOL ROADMAP

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 *D1.4 System architecture v1* and *D1.5 System architecture-final update* (Task 1.4: *Design the overall system architecture*). Figure 8 presents the main features of the SBA tool as developed during each one of its iterations.



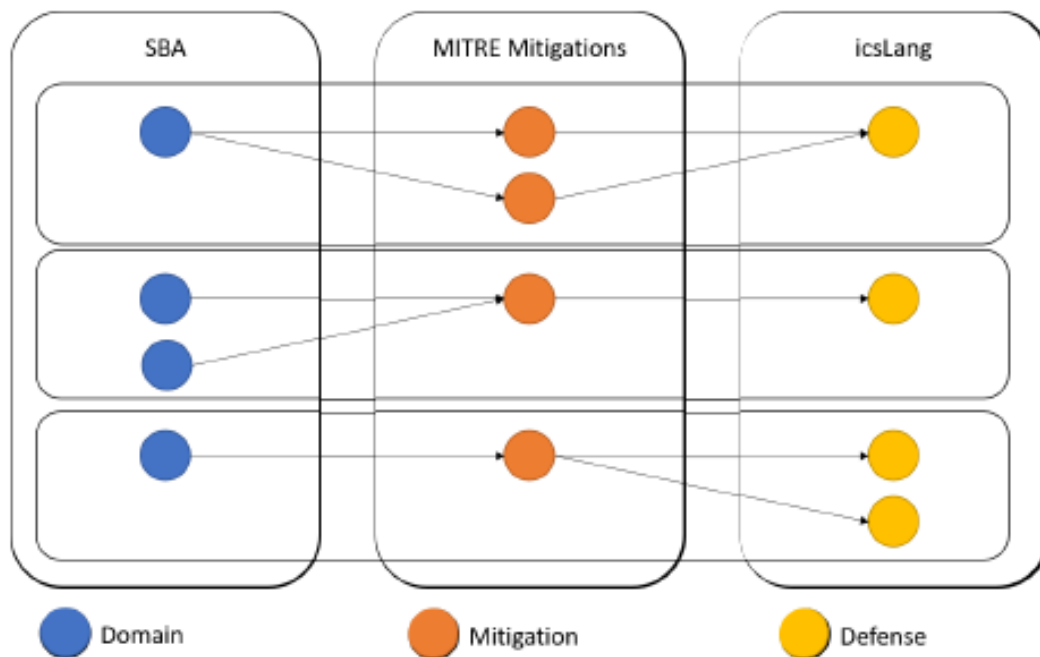
**Figure 8. SBA tool roadmap**

ANNEX 1 presents a full user manual of the tool where all of these features are presented in detail, allowing end-users to fully take advantage of the possibilities offered.

### 3.3 INTERFACES

As part of WP2, a robust mapping between the Vulnerability Assessment (VA) tool and the SBA tool has been founded and documented in a scientific publication [SIM21]. The VA tool depends on two components. On the one hand, the tool securiCAD facilitates the modelling of concrete architectures and performs attack simulations on them. On the other hand, the icsLang is based on the MAL framework, which codifies the meta-model used in securiCAD. To bring the information of the SBA and VA together, a mapping from SBA's levels and dimensions to icsLang is necessary. This mapping focuses on the general relation between these two concepts. However, for each organisation there are concrete

values and a concrete threat model that are used for the attack simulations. Obviously, these are different for every organisation.



**Figure 9. Exemplary mappings from SBA over MITRE ATT&CK to icsLang.**

Communication and data exchange among these two tools of the EnergyShield solution, SBA and VA, is achieved using both Kafka messages, for real-time events, and the REST API, for on-demand data extraction. Thus, allowing the exploitation of the SBA tool's evaluation results for realistic attack simulations performed by the VA tool.

### 3.1.1. REST API

SBA exposes a REST API allowing its interaction with the rest of the EnergyShield toolkit and/or with any other corporate operational system that needs to exploit the security culture metrics of the organisation. The specific API is fully documented in SwaggerHub [RES21], offering a detailed analysis of all available calls along with the response codes and structures.

A concise presentation of the full REST API is presented in the following paragraphs:



- **POST /api/token/**: Request an authentication token for a specific user.

**Parameters**

user: The user for whom a token is requested.

```
{
  "username": "username",
  "password": "password"
}
```

**Responses**

200: successful operation      {"token": dc2de81b2e7s"}

400: Wrong request data posted

403: Invalid username or password

404: Invalid url

- **GET /api/metrics/organisation/**: Get the metrics of the organisation for both individual and organisational dimensions.

**Parameters**

**token**: Token string generated from post request.

**Responses**

**200**: successful operation

**403**: Invalid token

**404**: Invalid url

```
{
  "metrics": {
    "dimensions": [
      {
        "title": "Competency",
        "value": 0.57,
        "level": "individual",
        "domains": [
          {
            "title": "Employee Competency",
            "value": 0.12
          }
        ]
      }
    ]
  }
}
```

- **GET /api/metrics/campaigns/**: Get all the programmed campaigns.

**Parameters**

**token**: Token string  
generated from post request.

**Responses**

**200**: successful operation

**403**: Invalid token

**404**: Invalid url

```
{
  "data": [
    {
      "id": 2,
      "title": "Example Campaign",
      "creation_date": "2020-6-25",
      "start_date": "2020-5-2",
      "end_date": "2020-5-25",
      "description": "Demo campaign",
      "assignees": [
        {
          "first_name": "User",
          "last_name": "User"
        }
      ],
      "questionnaires": [
        {
          "title": "title name"
        }
      ],
      "tests": [
        {
          "title": "Phishing Quiz"
        }
      ]
    }
  ],
  "total": 1
}
```

- **GET** /api/metrics/campaign/{campaign\_id}/: Get the info of a campaign.

**Parameters** **campaign\_id** : ID of campaign to return results

**token**: Token string generated from post request.

**Responses** **200**: successful operation

**403**: Invalid token

**404**: Campaign not found

```
{
  "campaign_info": {
    "id": 2,
    "title": "Example Campaign",
    "creation_date": "2020-6-25",
    "start_date": "2020-5-2",
    "end_date": "2020-5-25",
    "description": "This is a demo description for a campaign",
    "assignees": [
      {
        "first_name": "User",
        "last_name": "User"
      }
    ],
    "assignments": {
      "questionnaires": [
        {
          "title": "title name"
        }
      ],
      "tests": [
        {
          "title": "Phishing Quiz",
          "score": 0.76
        }
      ]
    }
  },
  "metrics": {
    "dimensions": [
      {
        "title": "Attitude",
        "value": 0.76,
        "level": "individual",
        "domains": [
          {
            "title": "Employee Climate",
            "value": 0.32
          }
        ]
      }
    ]
  }
}
```

- **GET** /api/metrics/user/{user\_id}/: Get the individual metrics of a user.

**Parameters** **user\_id**: ID of user to return results

**token**: Token string generated from post request.

**Responses** **200**: successful operation

**403**: Invalid token

**404**: User not found

```
{
  "metrics": {
    "dimensions": [
      {
        "title": "Competency",
        "value": 0.84,
        "level": "individual",
        "domains": [
          {
            "title": "Security Skills
Evaluation",
            "value": 0.98
          }
        ]
      }
    ]
  }
}
```

- **GET** /api/metrics/group/{group\_id}/: Get the metrics of a user group.

**Parameters** **group\_id**: ID of group to return results

**token**: Token string generated from post request.

**Responses** **200**: successful operation

**403**: Invalid token

**404**: Group not found

```
{
  "metrics": {
    "dimensions": [
      {
        "title": "Attitude",
        "value": 0.84,
        "level": "individual",
        "domains": [
          {
            "title": "Employee Climate",
            "value": 0.98
          }
        ]
      }
    ]
  }
}
```

### 1.1.1. KAFKA PRODUCER

Based on *D5.3 System release v1*, *D5.4 System release v2* and *D5.5 System release v3*, the EnergyShield toolkit components implement an asynchronous data exchange mechanism composed of data structures, and defined data flows in the system, using the Apache Kafka Architecture. Each tool produces JSON messages on predefined Kafka topics and, if necessary, consumes messages from other topics of interest.

More specifically, SBA produces **MSG04\_02\_SBA\_DATA\_PUBLISHED** messages published in the **KTOP04** topic whenever a security assessment campaign has been completed, thus whenever either all assignments generated by the specific campaign have been addressed or when the expiration date of the campaign is met. Therefore, SBA informs the rest of the EnergyShield toolkit that new security metrics related to the organisation have been generated and triggers new simulations, rules and post-actions to the rest of the platform elevating its results.

As defined in *D5.3 System release v1*, *D5.4 System release v2* and *D5.5 System release v3*, all Kafka messages have two main parts:

- **Header:** a fixed structure, valid for all messages, where data about message type, message producer, sent time, owner, version, etc. will be placed.
- **Body:** a dynamic structure, with specific content for each message. To be fully extensible, the content of the body will follow a standard format, having as fields array of references, and an array of name-value pairs.

An example of an **MSG04\_02\_SBA\_DATA\_PUBLISHED** message generated by SBA is presented below:

```
{
  "header": {
    "messageName": "MSG04_02_SBA_DATA_PUBLISHED",
    "messageVerMajor": "1",
    "messageVerMinor": "0",
    "msgId": "23",
    "sender": "SBA",
    "sentUtc": "2021-10-15 08:30:58",
    "envType": "Prod",
    "source": "SBA",
    "scope": "Restricted",
    "addresses": "10.129.159.98"
  },
  "body": {
    "msgType": "Result",
    "status": "Dispatched",
    "parameters": {
```

```

    "campaignID": "23",
    "urls": {
      "Organisation Report": "localhost:8000/api/metrics/organisation/",
      "Campaign Report": "localhost:8000/api/metrics/campaigns/23/"
    }
  }
}
}

```

Table 4 presents in detail all JSON fields contained within a Kafka message generated by the SBA tool.

**Table 4. Kafka Message Fields**

JSON field	Description	Example
<b>Header</b>		
"messageName": { "type": "string" }	A name distinguishing the messages generated by the tools.	"messageName": "MSG04_02_SBA_DATA_PUBLISHED"
"messageVerMajor": { "type": "integer" }	A number indicating the major version of the tool generating the message.	"messageVerMajor": "1"
"messageVerMinor": { "type": "integer" }	A number indicating the minor version of the tool generating the message.	"messageVerMinor": "0"
"msgId": { "type": "string" }	A unique identification string.	"msgId": "23"
"sender": { "type": "string" }	A string uniquely identifying the sender (e.g. application, module).	"sender": "SBA"
"sentUtc": { "type": "string" }	A timestamp (in the format YYYY-MM-DD HH:MM:SS) indicating the time the message was originally published by the tool.	"sentUtc": "2021-10-15 08:30:58"
"envType": { "type": "string" }	An enumeration indicating the status of the message.  Possible values: Test, Prod, Dev	"envType": "Prod"

<pre>"source": {   "type": "string" }</pre>	<p>A string indicating the originator of the message.</p> <p>Possible values AD, VA, SBA, DDM, SIEM</p>	<pre>"source": "SBA"</pre>
<pre>"scope": {   "type": "string" }</pre>	<p>A string indicating the scope of the message.</p> <p>Possible values: Restricted, Public, Confidential</p>	<pre>"scope": "Restricted"</pre>
<pre>"addresses": {   "type": "array",   "items": [     {       "type": "string"     },     {       "type": "string"     }   ] }</pre>	<p>IP addresses or identification of the sender devices.</p>	<pre>"addresses": "10.129.159.98"</pre>
<b>Body</b>		
<pre>"msgType": {   "type": "string" }</pre>	<p>The type of the message.</p> <p>Possible values: Alert, Info, Request, Result</p>	<pre>"msgType": "Result"</pre>
<pre>"status": {   "type": "string" }</pre>	<p>A string indicating the status of the message.</p> <p>Possible values: Dispatched, Received, Processed, Erroneous</p>	<pre>"status": "Dispatched"</pre>
<pre>"parameters": {   "type": "object" }</pre>	<p>Contains all SBA related information, including:</p> <ol style="list-style-type: none"> <li>The id of the campaign which was concluded.</li> <li>The exact REST API calls which can be invoked by the Kafka consumer to get detailed assessment results.</li> </ol>	<pre>"parameters": {   "campaignID": "23",   "urls": {     "Organisation Report": "localhost:8000/api/metrics /organisation/",     "Campaign Report": "localhost:8000/api/metrics /campaigns/23/"   } }</pre>

## 3.4 ADDITIONAL FEATURES

### 1.1.1. INTERNATIONALISATION & LOCALISATION

The goal of internationalisation and localisation is to allow a single Web application to offer its content in languages and formats tailored to its audience. Internationalisation is the act of preparing the software for localisation whereas localisation is the writing of the translations and local formats.

#### Security Agent Survey

1. What would you do if you saw a colleague not wearing their security pass around the office? \*

☐ Approach them immediately, point out that they're not wearing their pass and ask them to put it on. It is policy after all!

☐ Ask the person if they have been issued with a security pass and either take them to be issued with one, or offer them a helpful tip so they don't forget to wear it again.

☐ Check if they wear their pass tomorrow, this may have been just a temporary lapse. If it happens again, you may need to approach them or inform their manager.

☐ Ask them if they're aware of the security pass policy, point them to where they can find a copy, and suggest they put on their pass as soon as possible.

English

#### Questionario sugli agenti di sicurezza

1. Cosa fai se vedi un collega senza cartellino di riconoscimento in un ufficio/area ritenuta critica? \*

☐ Mi avvicino subito a loro indicandogli l'errore e chiedendo di mettersi il cartellino. Si tratta di politiche aziendali dopo tutto!

☐ Gli chiedo se gli è stato assegnato un cartellino di riconoscimento, in caso contrario li supporto nel richiederne uno. Suggerisco loro uno stratagemma per non dimenticarsi mai di indossarlo.

☐ Il giorno dopo controllo se si verifica di nuovo la disattenzione o se è stata solo una svista. Se riuscissero li avviso e in caso informo il loro responsabile.

☐ Gli ribadisco le politiche aziendali in termini di sicurezza, gli dico dove possono trovarle e gli indico di indossare il cartellino il più velocemente possibile.

Italian

#### Проучване на агента за сигурност

1. Какво бихте направили, ако видите колега, който не носи пропуска си за сигурност в офиса? \*

☐ Приближавате се незабавно до тях, посочвате, че не носят пропуска си и ги молите да го сложат. Все пак това е политика!

☐ Питате човека дали е получил пропуск за сигурност и или го водите, за да му бъде издаден такъв, или му давате съвет, за да не забрави да го носи отново.

☐ Проверявате дали носи пропуска си на другия ден утре, това може да е било само временен пропуск. Ако се случи отново, може да се наложи да се обърнете към тях или да информирате техния мениджър.

☐ Питате го дали знае за политиката за пропуска по отношение на сигурността, насочвате го до мястото, където може да намери копие, и му предлагате да сложи пропускат си възможно най-скоро.

Bulgarian

**Figure 10. Questionnaire localisation**

Internationalisation was procured throughout all of the development iterations of the SBA tool, aiming to support at least three languages: English, Italian and Bulgarian. Since the translation of the rich questionnaire content was of crucial importance for both our pilots, it was initiated early in the project and was concluded during the 3<sup>rd</sup> iteration of the tool with the valuable contribution of both our pilots.



### 1.1.2. ANONYMISATION

As with every corporate assessment tool dealing with personal data, our CSC framework, reaching down to an individual level, conforms with all regional and international laws protecting human's privacy. Therefore, our tool ensures compliance with the European Data Protection Regulation (GDPR), following ethics procedures described in WP10, meaning properly informing employees, and ensuring their written consent prior to campaign participation while offering **anonymisation** possibilities which can be enabled or disabled based on organisation needs and policies.

Thus, SBA contributes to understanding individual security risks and training needs, discomfort from demanding and inapplicable policies, and difficulties deriving from working security routine. In other words, SBA accommodates working force by retrieving security gaps, pinpointing policy complexity and, finally, facilitating participation in cyber-security defence. Using the anonymisation feature, ensures that SBA is not being used as a rating mechanism and an employee competency guide since working abilities and professionalism do not always go hand-by-hand with information security awareness. Security professionals and officers need to safeguard its role and usage, as with all security infrastructure, and to guide users through a prosperous exploitation.

## 4. PROPOSED INNOVATION & MARKET PERSPECTIVES

Tool	Security Behaviour Analysis
<b>Leading partner</b>	NTUA
<b>Contributing partners</b>	FOR, KTH, SC, IREN
<b>Proposed innovation</b>	NTUA, combining their long-standing presence and expertise on multi-criteria decision making and evaluations, risk-management, cyber-security, energy, and software development, focused on designing, developing, and implementing a cyber-security culture framework with a clear focus on the human factor. Using a holistic approach towards security culture, they emphasised on a simplified evaluation procedure carefully adapted to the energy sector. The specific framework manages to co-examine internal with external factors, organisational with individual parameters, along with their many interconnections and interactions.
<b>Technical innovation</b>	SBA uses a variety of techniques, including assessments with respect to different dimensions in both an individual and organisational level, simulations (e.g., phishing) and gamification (e.g., password strength test), to evaluate employee security awareness and properly adjust security training programs crafting them to specific organisational and individual needs. The specific tool identifies areas of vulnerability and attempts to influence employee behaviour to create a security-minded and compliance-oriented workforce.
<b>Problem addressed</b>	<p>During the last decades, the scientific society has focused on developing evaluation frameworks to assist corporations in assessing their security status while locating possible gaps and weaknesses. Yet, the vast majority of these frameworks does not dive deeper into what is considered by most the gravest security factor: the human being.</p> <p>An organisation's biggest threat to privacy and security, even if not acknowledged, are their own staff. Employee security awareness is a key link to an organisation's security chain since even the most well-guarded corporation is defenceless with no security culture. Thus, it became apparent that the market is in need for a tool which is able to assess and improve the security culture of an organisation.</p>
<b>Competitive analysis</b>	Based on Gartner Magic Quadrant for Security Awareness Computer-Based Training (published on 18th July 2019) [GMG19], vendors currently in recognisable position within the market

	<p>landscape are the following:</p> <ul style="list-style-type: none"> <li>• Barracuda</li> <li>• Cofense</li> <li>• Global Learning Systems</li> <li>• Infosec</li> <li>• Inspired eLearning</li> <li>• Junglemap</li> <li>• KnowBe4</li> <li>• MediaPRO</li> <li>• MetaCompliance</li> <li>• PhishLabs</li> <li>• Proofpoint</li> <li>• SANS Institute</li> <li>• Security Innovation</li> <li>• Terranova Security</li> </ul> <p>Market leaders exhibit a personalised evaluation and training approach trimmed to each organisational role and individual. Additionally, the variety and continuously enriched pallet of assessment and training modules act as a USP for most tools. Figure 11 Figure 11 presents a competitive comparison of the SBA tool with the aforementioned market leaders as it has been analysed in <i>D8.2 - Exploitation Report</i>.</p>
<b>Key aspects of the innovation</b>	<p>Innovation advantages of the SBA tool are summarised as follows:</p> <ul style="list-style-type: none"> <li>• It combines organisational and individual factors affecting and formulating the cyber-security culture of an organisation. Available security frameworks and market solutions tend to focus on one of these two dimensions whereas SBA examines their co-existence and many interactions.</li> <li>• It identifies possible cyber-threats using frameworks widely accepted both by the academic community and the professional society, such as the MITRE ATT&amp;CK and MERIT.</li> <li>• It provides custom recommendations on an individual and organisational (e.g., managerial) level, based on the detected vulnerabilities.</li> <li>• It is customisable and fully adjustable to any business domain and corporation (custom questionnaires can be introduced, different weights per security factor, etc.).</li> </ul>

<b>Academic potential (processed, research tools)</b>	<p>The SBA tool along with its underlying CSC framework have been designed and developed using a holistic approach. Thus, they can be exploited by any size and kind of organisation regardless of its business domain, specialisation, technological status and security readiness. It can also be used by any operational structure demonstrating a definite distinction between a decision-making board and a production unit. It can be adjusted to any business field by calibrating metrics defined for each of its domains. Additionally, it can be expanded and updated with little effort to constantly keep pace with the continuously transforming business environment.</p> <p>SBA has already been validated via two large-scale applications during the COVID-19 crisis [GED20] and to the health domain [GEM21] with impressive results. Similarly, it can be utilised in any academic environment to assess the cyber-security culture of individuals employed in educational institutions and/or students.</p> <p>Additionally, the specific framework and tool have already led to three (3) conference papers, six (6) indexed journal publications and one (1) post-graduate thesis, whereas one (1) PhD thesis and two (2) more manuscripts are currently being prepared.</p>
<b>Commercial potential (products, services)</b>	<p>SBA, being a cyber-security tool developed by the National Technical University of Athens (NTUA), an educational and research institution, has been made publicly available as open source (MIT license).</p> <p>Therefore, its commercial exploitation mainly focuses on promoting consultancy services related to cyber-security culture assessment and awareness cultivation training programs.</p>
<b>Marketing potential</b>	<p>The SBA tool has been showcased in multiple conferences and workshops while its underlying framework and scientific basis have been presented in detail in various journal articles. Security agencies and experts have expressed concrete interest and provided valuable feedback.</p> <p>Two major pilot scenarios have already been applied during the COVID-19 pandemic aiming Critical Infrastructures [GED20] and the Health Sector in specific [GEM21]. Participating parties expressed their interest in further utilising the specific tool and its potentials while representatives from other business domains, such as education, banking, telecommunications, have reached out asking for demos and targeted use case applications.</p>
<b>Publications</b>	<p>As mentioned previously, the specific framework and tool have already led to three (3) conference papers and six (6) indexed journal publications.</p>

<b>References</b>	[GEO20, GES20, GEA20, GED20, GEO21, GEA21, SIM21, GEM21]
<b>Patents</b>	N/A
<b>Innovation disclosure</b>	N/A
<b>Pending disclosure</b>	N/A
<b>Links to the proposed innovation, if any</b>	MIT License

Tools	Phishing Simulations	Smishing	Vishing	Found Physical Media	Other social engineering attacks	Malware	Compromised Credentials	Fraud	Automation	Behavior Assessment	Attitude Assessment	Competency Assessment	Organisational Assessment	Risk Assessment	Role Based	Forensic alerts	Cyber security training	Encryption	Metrics	Detection of vulnerabilities
Cofense	✓																			
Proofpoint	✓					✓	✓		✓							✓	✓	✓		✓
Barracuda Phishline	✓	✓	✓	✓																
Webroot	✓				✓												✓			
Cyber Risk Aware	✓	✓										✓					✓			
LucySecurity	✓	✓		✓	✓	✓											✓			
Kaspersky	✓								✓				✓				✓			
Terranova	✓								✓								✓			
Infosec	✓								✓							✓	✓			
Conformance cybersecurity	✓				✓								✓				✓			✓
CybSafe	✓	✓	✓	✓	✓				✓	✓	✓		✓				✓		✓	✓
Elevate	✓												✓				✓			
Popcorn Training	✓																✓			
Security Advisor	✓																✓			
Zeguro	✓																✓			
Navex Global	✓								✓					✓			✓			
KnowBe4	✓				✓				✓				✓				✓			
Media Pro	✓	✓															✓			
Inspired eLearning	✓															✓	✓		✓	
<b>SBAM</b>	✓			✓	✓				✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓

Tools	Compliance	Data Protection	Gamification	Use of Videos and other educational materials	Easy integration	DNS protection	Progress Measurement	Visualization Tools	Threat simulation features (time stamping, DLP, etc.)	Cloud based	Backup	Reporting Center	LMS	Compromise Assessment	Multi-Language	Policy and procedure development	Mobile	Conflict of interest management
Cofense	✓																	
Proofpoint	✓	✓						✓										
Barracuda Phishline	✓	✓	✓	✓			✓		✓	✓	✓	✓	✓					
Webroot	✓			✓	✓	✓												
Cyber Risk Aware	✓		✓	✓			✓											
LucySecurity	✓							✓										
Kaspersky	✓							✓										
Terranova	✓																	
Infosec	✓																	
Conformance cybersecurity	✓																	
CybSafe	✓			✓								✓				✓	✓	
Elevate	✓																	
Popcorn Training	✓		✓	✓														
Security Advisor	✓							✓				✓					✓	
Zeguro	✓																	
Navex Global	✓						✓					✓				✓	✓	✓
KnowBe4	✓																	
Media Pro	✓	✓															✓	
Inspired eLearning	✓																✓	
<b>SBAM</b>	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Figure 11. Competitive comparison of the SBA tool.

## 5. CONCLUSION AND NEXT STEPS

This deliverable presented the Cyber-Security Culture Framework and the corresponding Security Behaviour Analysis tool 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.

Moreover, the capabilities, interfaces and techniques of the tool have been analysed, offering a detailed user manual for administrators, managers and simple users.

Future steps in our work include, but are not limited to, the following:

- Calibrating the security culture framework by adjusting the weights of each security element contained within the suggested model.
- Evaluating and further improving both the suggested framework and tool based on the provided by the pilots' feedback.
- Fine-tuning the integration of SBA with the EnergyShield toolkit.
- Expanding and adjusting our solution to other business domains and application areas.

## REFERENCES

- [KAN09] Bounas, Kanaris & Georgiadou, Anna & Kontoulis, Michalis & Mouzakis, Spiros & Askounis, Dimitris. (2020). Towards A Cybersecurity Culture Tool Through A Holistic, Multi-Dimensional Assessment Framework. 135-139. 10.33965/is2020\_202006C016.
- [GEO20] Anna Georgiadou, Spiros Mouzakis, 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
- [GES20] Georgiadou, Anna, Spiros Mouzakis 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 Mouzakis 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., Mouzakis, 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>
- [GEO21] Anna Georgiadou, Spiros Mouzakis & 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.; Mouzakis, S.; Askounis, D. Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework. Sensors 2021, 21, 3267. <https://doi.org/10.3390/s21093267>
- [SIM21] Simon Hacks, Ismail Butun, Robert Lagerström, Andrei Buhaiu, Anna Georgiadou, and Ariadni Michalitsi Psarrou. 2021. Integrating Security Behavior into Attack Simulations. In The 16th International Conference on Availability, Reliability and Security (ARES 2021). Association for Computing Machinery, New York, NY, USA, Article 120, 1–13. DOI:<https://doi.org/10.1145/3465481.3470475>
- [GEM21] Georgiadou, Anna, Ariadni Michalitsi-Psarrou, Fotios Gioulekas, Evangelos Stamatiadis, Athanasios Tzikas, Konstantinos Gounaris, Georgios Doukas, Christos Ntanos, Luís Landeiro Ribeiro, and Dimitris Askounis. 2021. "Hospitals' Cybersecurity Culture during the COVID-19 Crisis" Healthcare 9, no. 10: 1335. <https://doi.org/10.3390/healthcare9101335>
- [RES21] National Technical University of Athens. (2021, 11 03). Swagger. Retrieved from [sba-rest-api|3.0.0: https://app.swaggerhub.com/apis/Ddimitrako/sba-rest\\_api/3.0.0](https://app.swaggerhub.com/apis/Ddimitrako/sba-rest_api/3.0.0)
- [ARB06] A.-R. Blais and E. U. Weber, "A Domain-Specific Risk-Taking (DOSPERT) scale for adult populations," *Judgment and Decision Making*, vol. 1, no. 1, p. 33–47, 2006.
- [SGS95] S. G. Scott and R. A. Bruce, "Decision-Making Style: The Development



- and Assessment of a New Measure," *Educational and Psychological Measurement*, vol. 5, no. 5, pp. 818-831, 1995.
- [SGB94] A. Strathman, F. Gleicher, D. S. Boninger and S. Edwards, "The Consideration of Future Consequences: Weighing Immediate and Distant Outcomes of Behavior," *Journal of Personality and Social Psychology*, vol. 66, no. 4, pp. 742-752, 1994.
- [PSB95] J. H. Patton, M. S. Stanford and E. S. B. PhD., "Factor structure of the Barratt impulsiveness scale," *Journal of Clinical Psychology*, vol. 51, no. 6, pp. 768-774, 1995.
- [CPR82] J. T. Cacioppo and R. E. Petty, "The Need for Cognition," *Journal of Personality and Social Psychology*, vol. 42, no. 1, pp. 116-131, 1982.
- [EPE15] S. Egelman and E. Peer, "Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS)," in *33rd Annual ACM Conference on Human Factors in Computing Systems*, Seoul Republic of Korea, 2015.
- [SPH19] SPHINX Project EU. SPHINX Project EU. SPHINX., 1 January 2019, Available online: <https://sphinx-project.eu/>. (Accessed on 19 June 2021).
- [GMG19] Gartner. Gartner Research. 18 July 2019, Available online: <https://www.gartner.com/en/documents/3950454/magic-quadrant-for-security-awareness-computer-based-tra> (Accessed on 17 November 2021).



# ANNEX – SECURITY BEHAVIOUR ANALYSIS TOOL – USER MANUAL

## 1. CYBER-SECURITY CULTURE FRAMEWORK

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, a number of 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.

## 2. MAIN CONCEPTS

Based on the Cyber-Security Culture Framework, there is a firm distinction among three different business user roles:

- **Administrator** (superuser privileges): usually a system administrator or security officer with full privileges over the security culture assessment life-cycle of the organisation and, therefore, of the SBA tool. They are responsible for user management, global groups and campaigns creation and management.
- **Manager**: any user who acts as a leader of an employee group and is responsible for their security assessment, evaluation and training. They are granted manager privileges within the SBA tool, allowing them to create new users (practically inviting them to access the tool), groups, campaigns (accessible only to themselves apart from the administrators), and monitor their status and progress by obtaining a number of graphical reports.

- **User:** simple user able to participate in campaigns or perform a number of self-assessment iterations in order to evaluate their security culture status and sharpen their information security knowledge, familiarity and awareness.

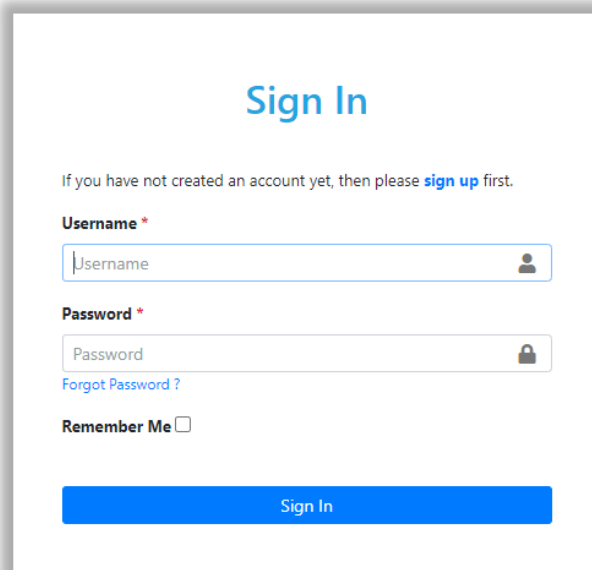
The corresponding roles have been implemented in the SBA tool, offering customisation and personalisation of the security assessment experience. Other important security concepts used within the tool are the following:

- **Campaign:** a security culture assessment iteration designed by a manager targeting specific security domains and user groups or individuals. It has a certain duration (start and end date) and results in a number of assignments to the participating employees with a determined expiration. It provides a snapshot of the security culture status of a part of the organisation giving useful insights and feedback to decision-makers.
- **Self-assessment:** an interactive way of self-evaluating your security awareness, compliance and readiness while improving your security knowledge and culture. Via multiple repetitions, it can also be considered as a means of self-training both to the security policies and procedures of the organisation and on the various information security threats and current reality.
- **Threat:** a cyber-security threat originating from either external adversaries or insiders, meaning employees or contractors, that could potentially harm the organisation, wittingly or unwittingly.
- **Recommendation:** a suggestion meant to define in detail the awareness training programs and seminars, along with their main goals and objectives, needed for the organisation to enhance and elevate its defence against identified cyber-security threats.

### 3. STRUCTURE

The SBA Tool is a web-based application. To access the tool services, the users need to initially sign in (Figure 12).

## Security Behaviour Analysis



**Sign In**

If you have not created an account yet, then please [sign up](#) first.

**Username \***

**Password \***

[Forgot Password ?](#)

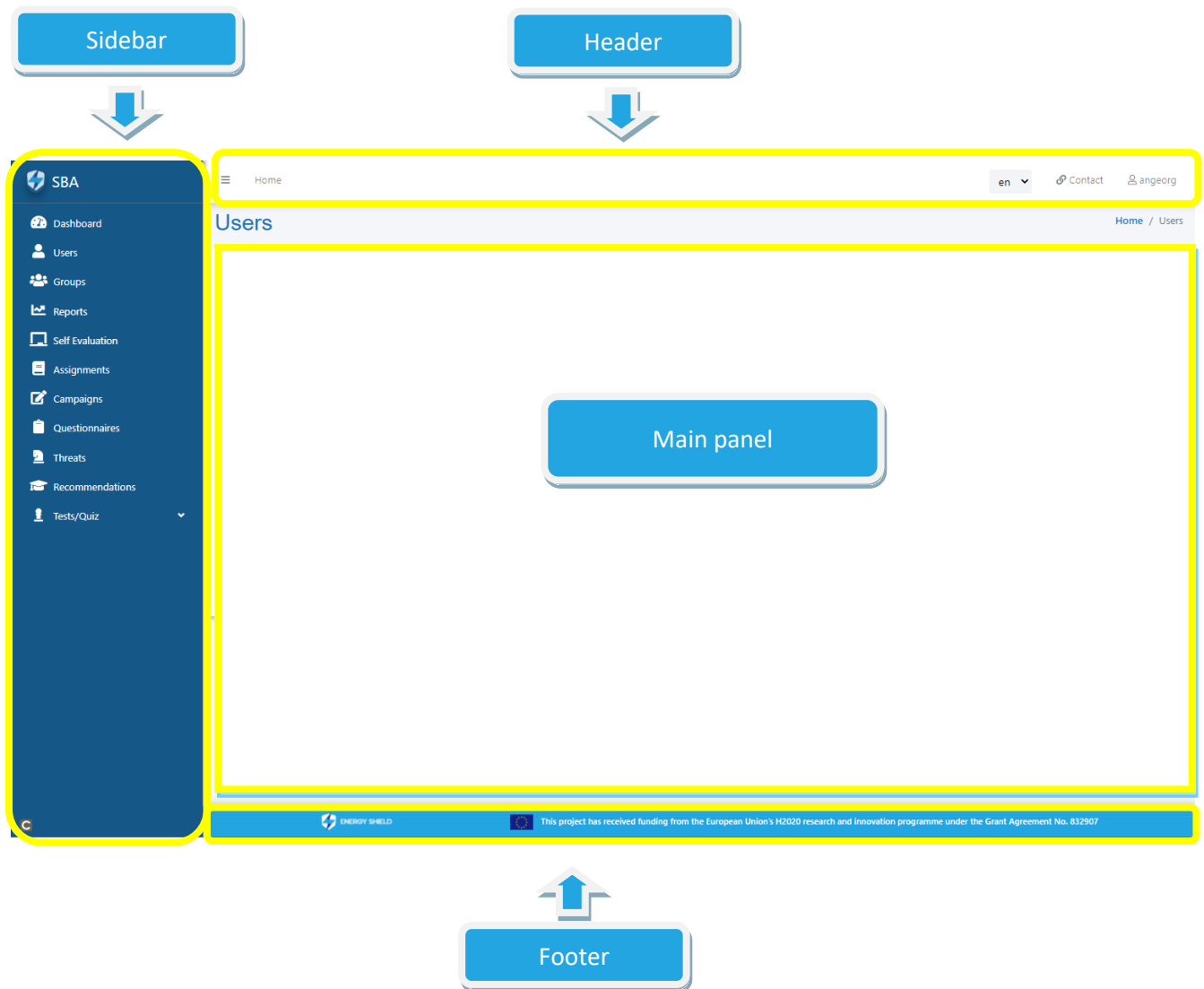
**Remember Me** ☐

**Sign In**

**Figure 12. Sign-in view**

Providing valid credentials leads the user to a personalised home page which differs depending on user role and privileges. The SBA tool console is divided into four (4) main parts (Figure 13):

- **Header:** offers localisation possibilities via the “select language” menu, project contact information and a user submenu offering access to profile, change password and sign-out options.
- **Sidebar:** offers access to different views of the tool (user role and privilege dependent).
- **Footer:** contains project-related information and a connection to project’s official website.
- **Main panel:** is the main presentation part of the tool.



**Figure 13. Console layout**

Depending on user role and privileges, the sidebar offers a number of different options:

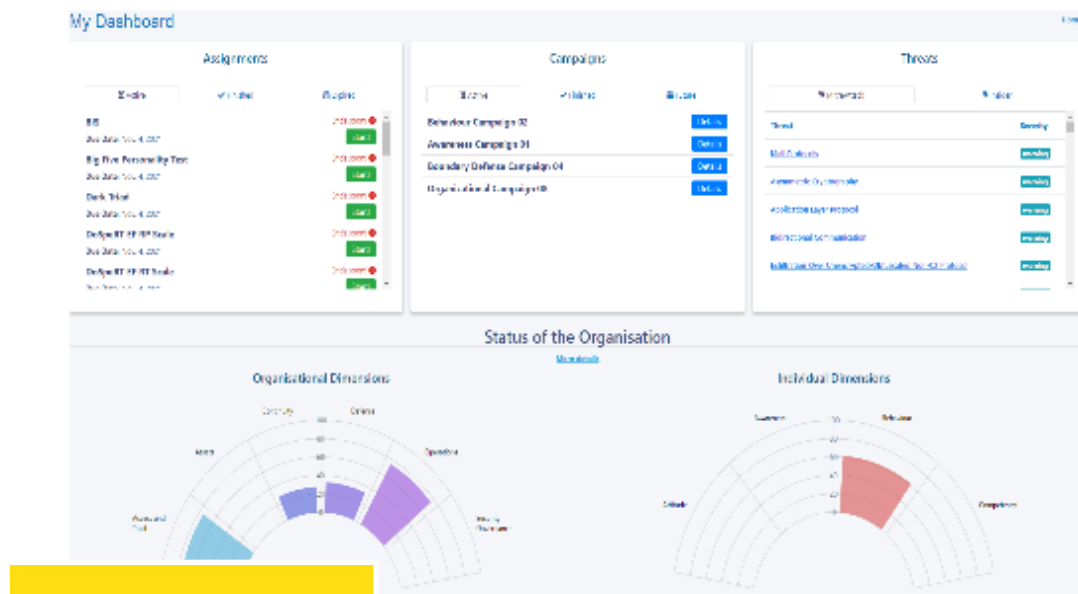
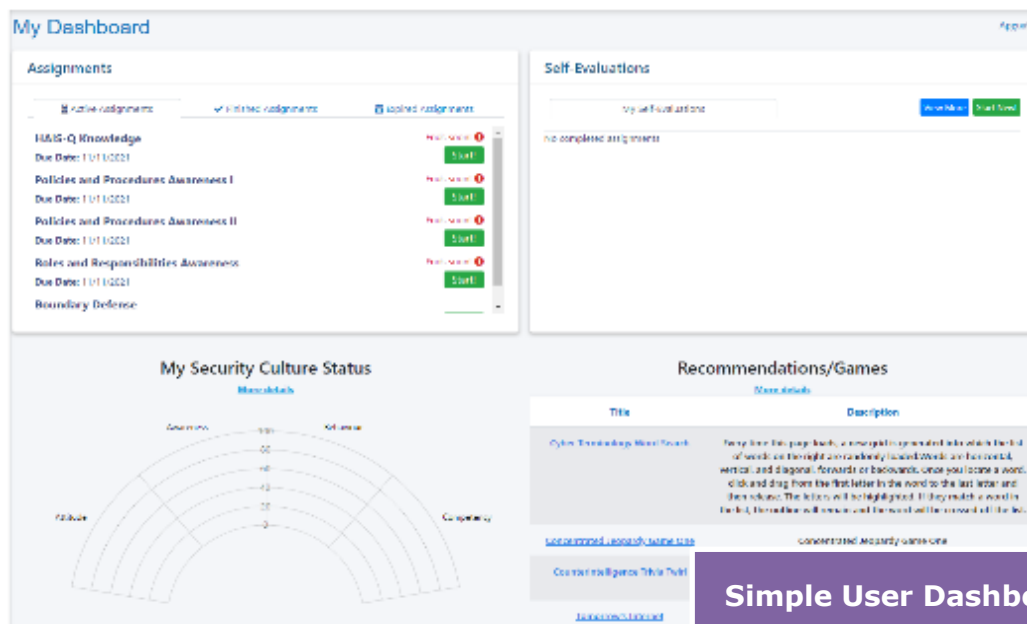
- **Dashboard:** bears a different skeleton depending on user role, allowing an overall functionality view and control of the tool.
- **Users** (visible only to administrators and managers): listing the participating members of the tool along with a number of organisational info.
- **Groups** (visible only to administrators and managers): listing the groups of the tool serving different evaluation purposes.
- **Reports:** visualisation of the security culture assessment results and status.
- **Self Evaluation:** offering individuals the possibility to run a number of questionnaires and tests at their own pace.

- **Assignments:** listing of all the assignments made to the logged-in user via the various campaigns addressed to them.
- **Campaigns** (visible only to administrators and managers): materialisation of a security culture evaluation iteration with direct assignments of specific questionnaires and tests to dedicated individuals or groups.
- **Questionnaires** (visible only to administrators and managers): listing of available questionnaires of the tool while correlating them to the security culture model.
- **Threats** (visible only to administrators and managers): displaying identified threats based on the organisation's current cyber-security culture assessment results.
- **Recommendations:** this view differentiates based on the user roles and privileges. Simple users are presented with a listing of free online games for self-training, whereas administrators and managers are additionally presented with general and specific training recommendations targeting identified cyber-security weaknesses of the organisation.
- **Tests/Quiz** (visible only to administrators and managers): an interactive designing workspace, offering the possibility to create custom email phishing simulation and quiz templates, thus, making them available for customised evaluation tests.

The following paragraphs present in detail each one of the above options of the tool while correlating it to its underlying cyber-security culture framework.

### 1.1. DASHBOARD

Having signed in, the user lands in the dashboard screen, which, depending on the user role and privileges, provides an overall preview of the SBA tool functionality (including pending assignments, cyber-security status graphs and tips, etc.) while offering quick access to targeted submenus, as exhibited in Figure 14.

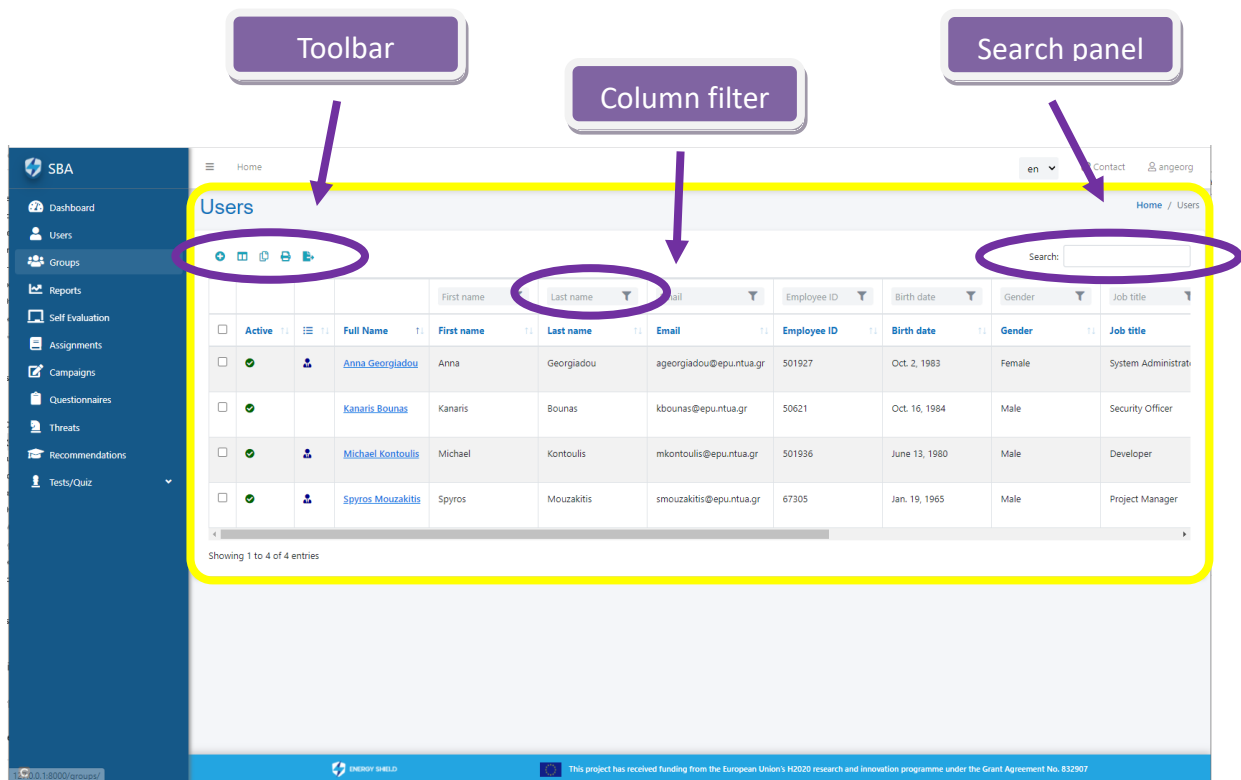

**Manager Dashboard**

**Simple User Dashboard**
**Figure 14. Dashboard view**

## 1.2. USERS

This view (visible only to administrators and managers) displays users' information in a responsive table offering searching and multiple column filtering capabilities, as presented in Figure 15. The toolbar present in the upper left part contains the following buttons:

- **Add**: dropdown menu allowing creations of new user and group.
- **Show/Hide columns**: control over column visibility.

- **Copy:** copies selected table rows and columns to clipboard.
- **Print:** prints selected table rows and columns while invoking the web browser print menu.
- **Export to file:** dropdown menu allowing the export of the selected table rows and columns to different file formats (Excel, CSV and PDF).




**Figure 15. Users view**

Selecting one of the displayed users (by clicking on their full name) redirects you to the user profile view, which, depending on access user role (administrator, manager or simple user) and privileges, presents user-specific information and offers a number of different control actions.

As presented in Figure 16, the user profile view contains:

- **Summary panel:** generic user details (e.g. full name, job description)
- **Personal Information Tab:** first and last name, contact details, organisation info, and so on.
- **Account Tab** (visible only to administrators): account privileges and group membership.
- **Assignments** (visible only to administrators or profile owners): table view of all user assignments (completed, expired, pending) with score achievement, completion and expiration date and redirection link to assignment execution.

**Profile: Anna Georgiadou**



**Anna Georgiadou**  
System Administrator

Department: Information & Security

Company: DISSENTIA

Member since: 09 Feb 10, 2020, 1:51 pm

[Disable](#)

**Personal Information**

First name: Anna, Last name: Georgiadou, Username: angeo123

Employment id: 0012327, Birth date: 10/05-10-62, Gender: Female

Notes: Supervisor

[Contact Details](#)


**Organizational Information**

Job title: System Administrator, Department: Information & Security

Company: DISSENTIA

**Personal Info Tab**

**Profile: Anna Georgiadou**



**Anna Georgiadou**  
System Administrator

Department: Information & Security

Company: DISSENTIA

Member since: 09 Feb 10, 2020, 1:51 pm

[Disable](#)

**Personal Information**

**Manager status**


**Supervisor status**

**Group Members**

Available	Selected
<p>Learning unit</p> <p>10/05-10-62</p> <p>10/05-10-62</p>	<p>10/05-10-62</p> <p>10/05-10-62</p> <p>10/05-10-62</p>

**Account Tab**

**Profile: Anna Georgiadou**



**Anna Georgiadou**  
System Administrator

Department: Information & Security

Company: DISSENTIA

Member since: 09 Feb 10, 2020, 1:51 pm

[Disable](#)

**Personal Information**

**Account**

**Status**

**Assignments**

Status	Assignment	Score	Completion Date	Expiration Date
Completed	Security Awareness Training	100%	May 12, 2020	May 12, 2020
Completed	Security Awareness Training	100%	May 12, 2020	May 12, 2020
Completed	Security Awareness Training	100%	May 12, 2020	May 12, 2020
Completed	Security Awareness Training	100%	May 12, 2020	May 12, 2020
Completed	Security Awareness Training	100%	May 12, 2020	May 12, 2020
Completed	Security Awareness Training	100%	May 12, 2020	May 12, 2020

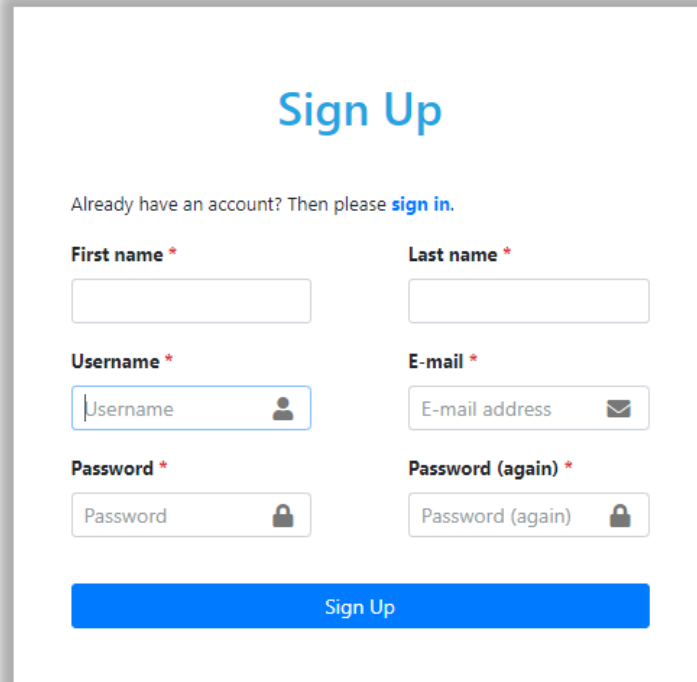
**Assignments Tab**

Figure 16. User profile view



For the creation of a new user, two options are available:

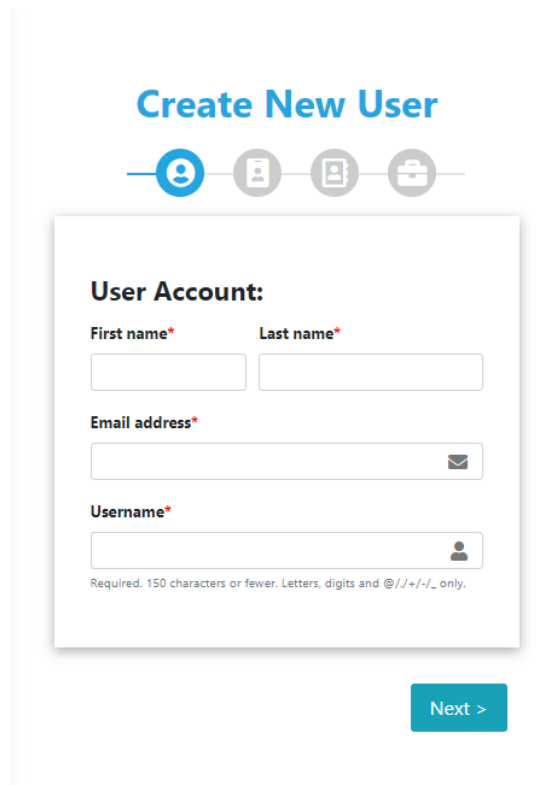
- **Signup form** (Figure 17): link to a specific form could be distributed via any corporate tool or simply via email. Users need to complete their first and last name, username and password and an email, which shall be used as a security verification control, to sign up to the SBA tool and gain access as simple users.



The image shows a 'Sign Up' form with a white background and a blue border. At the top, the text 'Sign Up' is displayed in a large, blue, sans-serif font. Below this, a link 'Already have an account? Then please [sign in](#).' is shown in a smaller, grey font. The form contains six input fields arranged in two columns. The left column has fields for 'First name \*', 'Username \*', and 'Password \*'. The right column has fields for 'Last name \*', 'E-mail \*', and 'Password (again) \*'. Each field is a white rectangle with a thin grey border. The 'Username' and 'Password' fields have small user and lock icons respectively. The 'E-mail' and 'Password (again)' fields have small envelope and lock icons respectively. At the bottom of the form is a large, solid blue button with the text 'Sign Up' in white, centered.

**Figure 17. Sign-up view**

- **Create new user wizard** (available only to administrators): accessible via the users and groups view toolbar (Figure 18). The wizard guides you through the creation procedure of a new user offering the possibility to complete both required and optional fields. Upon successful completion, a verification email is sent to the newly created user, and confirmation is expected for the account to be accessible.



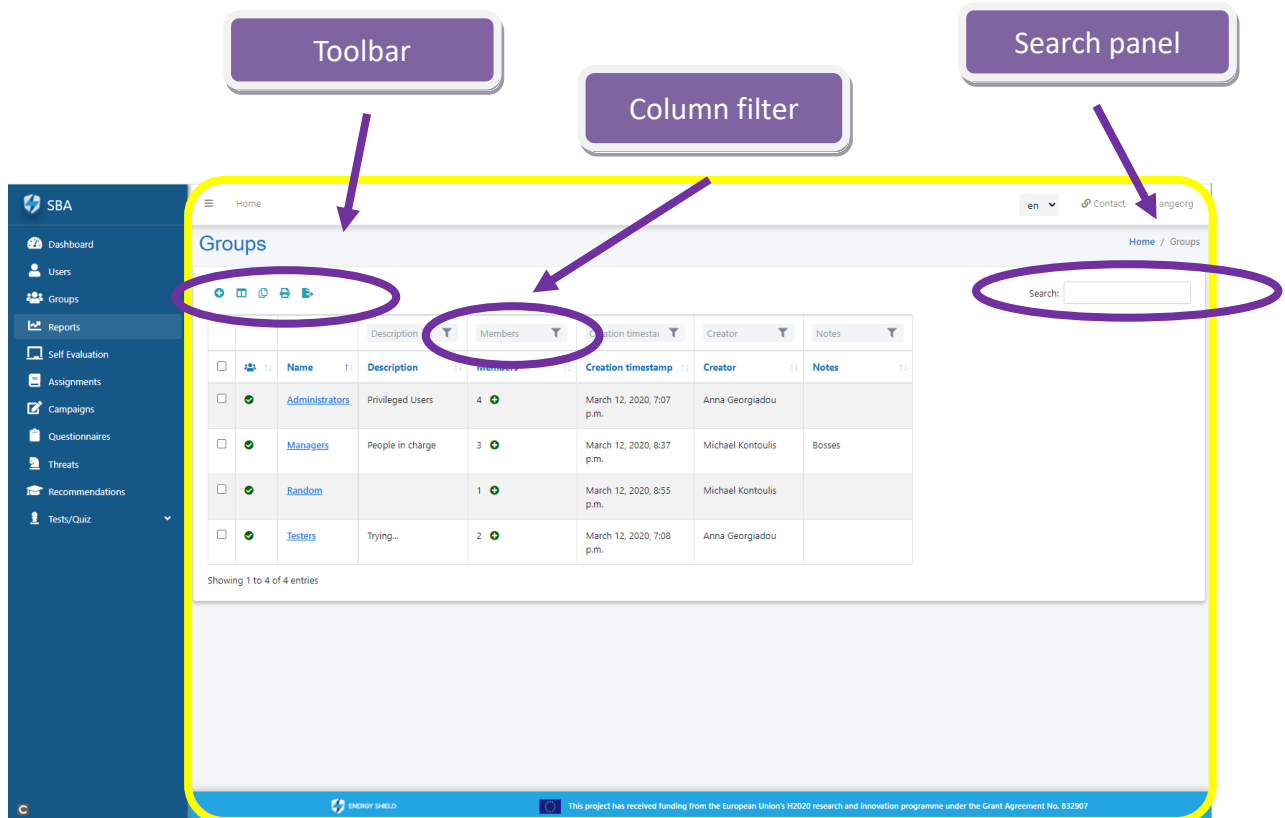
The image shows a 'Create New User' wizard interface. At the top, there's a title 'Create New User' in blue. Below it is a progress bar with four circular icons: a person (active), a document, a folder, and a briefcase. The main form is titled 'User Account:' and contains four fields: 'First name\*' and 'Last name\*' (each with a text input box), 'Email address\*' (with a text input box and an envelope icon), and 'Username\*' (with a text input box and a person icon). Below the 'Username\*' field, there is a small note: 'Required. 150 characters or fewer. Letters, digits and @/./+/-/\_ only.' At the bottom right of the form, there is a blue button labeled 'Next >'.

**Figure 18. Create new user wizard**

### 1.3. GROUPS

This view (visible only to administrators and managers) displays groups' information in a responsive table offering searching and multiple column filtering capabilities, as presented in Figure 19. The toolbar present in the upper left part contains the following buttons:

- **Add:** dropdown menu allowing creations of new user and group.
- **Show/Hide columns:** control over column visibility.
- **Copy:** copies selected table rows and columns to clipboard.
- **Print:** prints selected table rows and columns while invoking the web browser print menu.
- **Export to file:** dropdown menu allowing the export of the selected table rows and columns to different file formats (Excel, CSV and PDF).



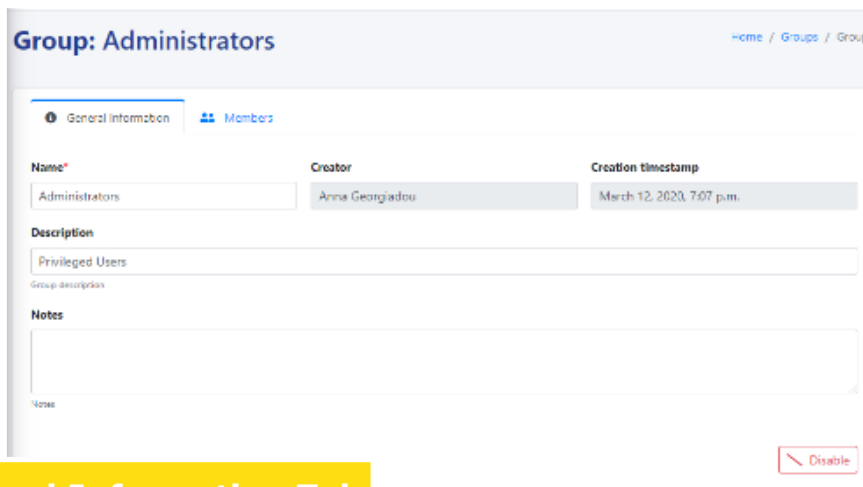
**Figure 19. Groups view**

Groups view exhibits **global groups** (description used for groups created by the administrators of the tool) to all users. If the signed-in user is a manager, along with global groups, the table also contains the groups created by the specific user. Administrators, as expected, have access and view to all groups available.

Selecting one of the displayed groups (by clicking on its name) redirects you to the group details view, which presents group-specific information and offers a number of different control actions.

As presented in Figure 20, the group details view contains:

- **General Information Tab:** name, creation details, description, and so on.
- **Members Tab:** members of the group.



**Group: Administrators** [Home](#) / [Groups](#) / [Group](#)

**General Information** **Members**

**Name\*** **Creator** **Creation timestamp**

Administrators Anna Georgiadou March 12, 2020, 7:07 p.m.

**Description**

Privileged Users

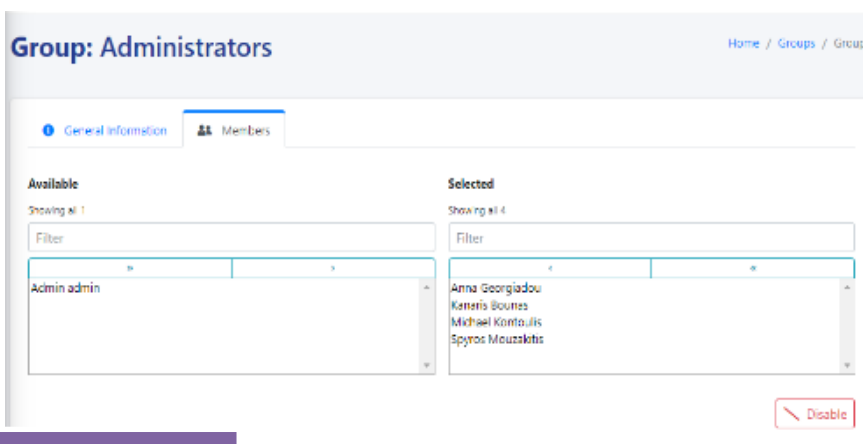
Group description

**Notes**

Notes

[Disable](#)

**General Information Tab**



**Group: Administrators** [Home](#) / [Groups](#) / [Group](#)

**General Information** **Members**

**Available** **Selected**

Showing all 1 Showing all 4

Filter

Admin admin

Filter

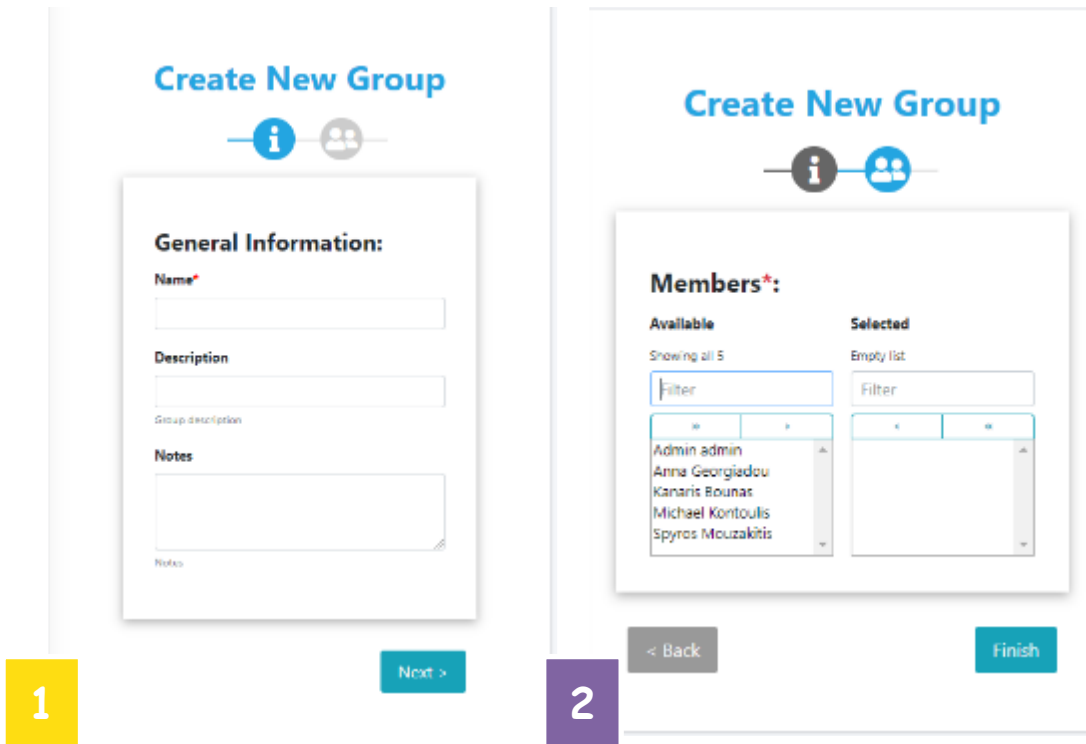
Anna Georgiadou  
Kateris Bouras  
Michael Kontoulis  
Spyros Mouzakitis

[Disable](#)

**Members Tab**

**Figure 20. Group details view**

The **Create new group wizard** is accessible via the users and groups view toolbar (Figure 21). The wizard guides you through the creation procedure of a new group offering the possibility to complete both required and optional fields.



**Create New Group**

**General Information:**

Name\*

Description

Notes

Next >

**Members\*:**

Available

Showing all 5

Filter

Admin admin
Anna Georgiadou
Kanaris Bounas
Michael Kontoulis
Spyros Mouzakitis

Selected

Empty list

Filter

< Back

Finish

Figure 21. Create new group wizard

#### 1.4. REPORTS

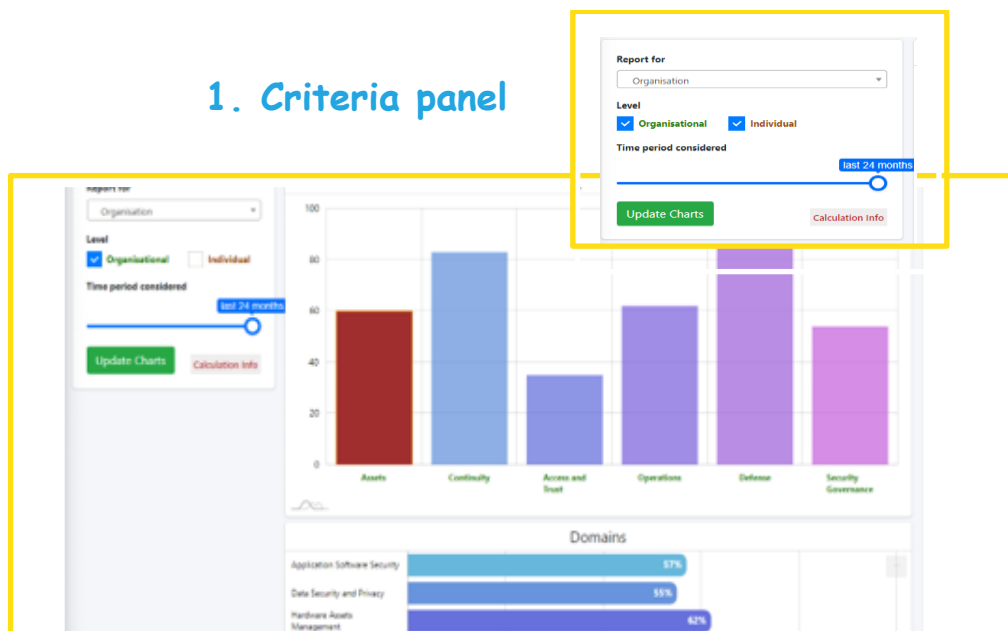
This view offers access to the reporting and visualisation mechanism of the SBA tool. The displayed information is properly filtered depending on user role and privileges guiding the user through the creation of a suitable security culture assessment analysis report.

As presented in Figure 22, this view consists of three main parts:

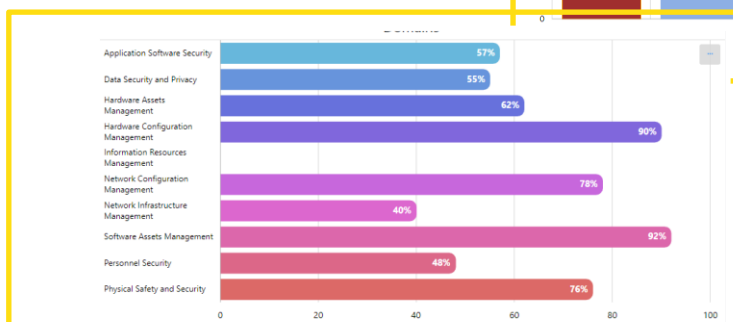
- **Criteria panel (visible only to manager and administrators):** user can select to create an organisation, campaign or group report by making the corresponding choice from the drop-down menu. Depending on the selection, the rest of the panel is updated to demonstrate available options. A level filter is also present in all cases to allow isolation of the different security culture levels (organisational and individual). At the bottom of the criteria panel, a time slide bar enables the user to further trim reported data adjusting time window (starting from a 24-months period). Having inserted desired reporting criteria, the user may preview security dimensions status by simply clicking on the “Update Charts” button. “Calculation info” button pops up a new window offering a detailed preview of the survey responses that were used for the calculation of the metrics displayed on the charts. More specifically, calculation info is divided into the cyber-security culture model dimensions and domains and reach down to a questionnaire level.

- **Security Dimensions board:** contains a responsive vertical bar chart of the cyber-security dimensions. In the case of a simple user, it is limited down to security culture individual-level dimensions demonstrating data for the specific user while, for managers and administrators, charts are formulated based on the criteria panel. Hovering over any element of the chart gives an overview of its details, while clicking on it updates the **Domains board** accordingly. At the upper right corner of the board, an export button is available, offering a variety of formatting options (image, data, print).
- **Domains board:** contains a horizontal bar chart of the cyber-security domains related to the selected dimension. At the upper right corner of the board, an export button is available, offering a variety of formatting options (image, data, print).

## 1. Criteria panel



## 2. Security Dimensions Board

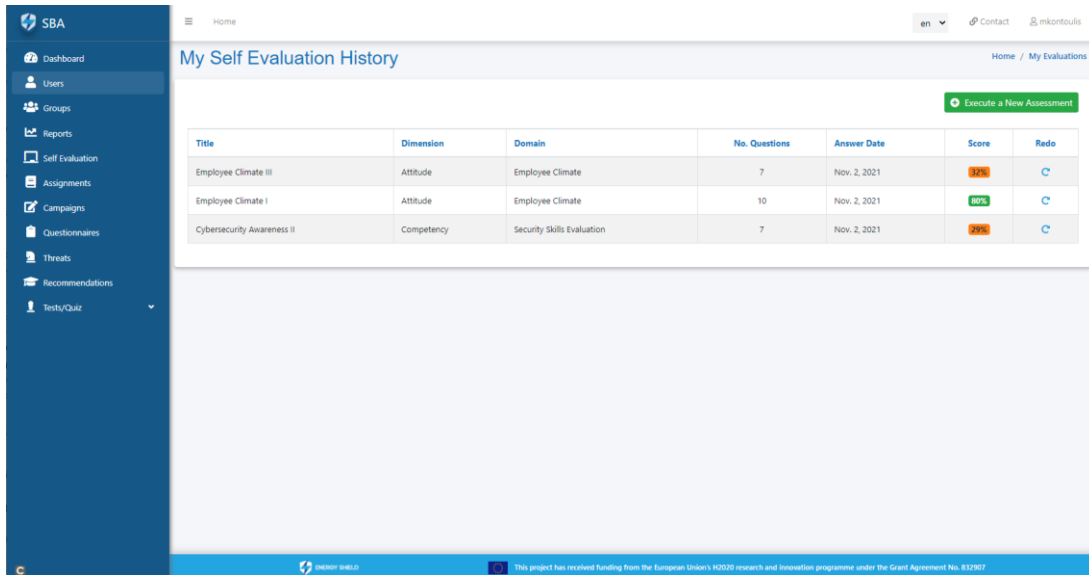


## 3. Domains Board

Figure 22. Reports view

## 1.5. SELF EVALUATION

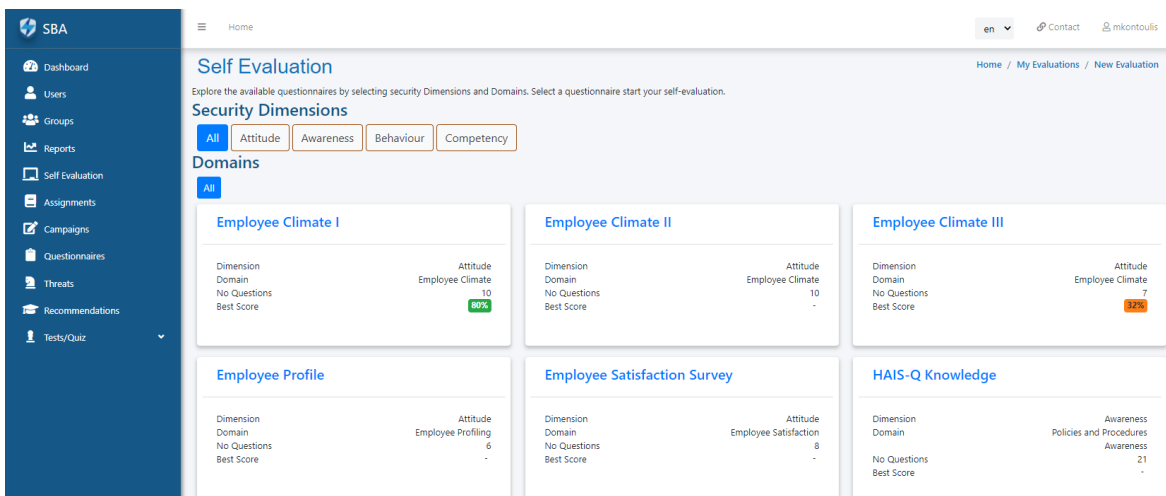
This view offers access to the self-evaluation mechanism of the SBA tool. It displays a self-evaluation history log containing all surveys completed by the sign-in user along with an achievement score and the affected security culture dimensions and domains as presented in Figure 23.



Title	Dimension	Domain	No. Questions	Answer Date	Score	Rate
Employee Climate III	Attitude	Employee Climate	7	Nov. 2, 2021	32%	C
Employee Climate I	Attitude	Employee Climate	10	Nov. 2, 2021	80%	C
Cybersecurity Awareness II	Competency	Security Skills Evaluation	7	Nov. 2, 2021	25%	C

**Figure 23. Self-evaluations view**

On the upper right part, an “Execute a New Assessment” button is available, redirecting the user to the self-evaluation view presented in Figure 24, which displays all available individual level questionnaires along with a number of security culture model correlation details and the highest related achievement score. The users can preview their cyber-security performance status and exercise via triggering the execution of any of the available assessment questionnaires by simply clicking on the questionnaire of interest.



Dimension	Attitude
Employee Climate I	Employee Climate
No Questions	10
Best Score	80%

Dimension	Attitude
Employee Climate II	Employee Climate
No Questions	10
Best Score	-

Dimension	Attitude
Employee Climate III	Employee Climate
No Questions	7
Best Score	32%

Dimension	Attitude
Employee Profile	Employee Profiling
No Questions	6
Best Score	-

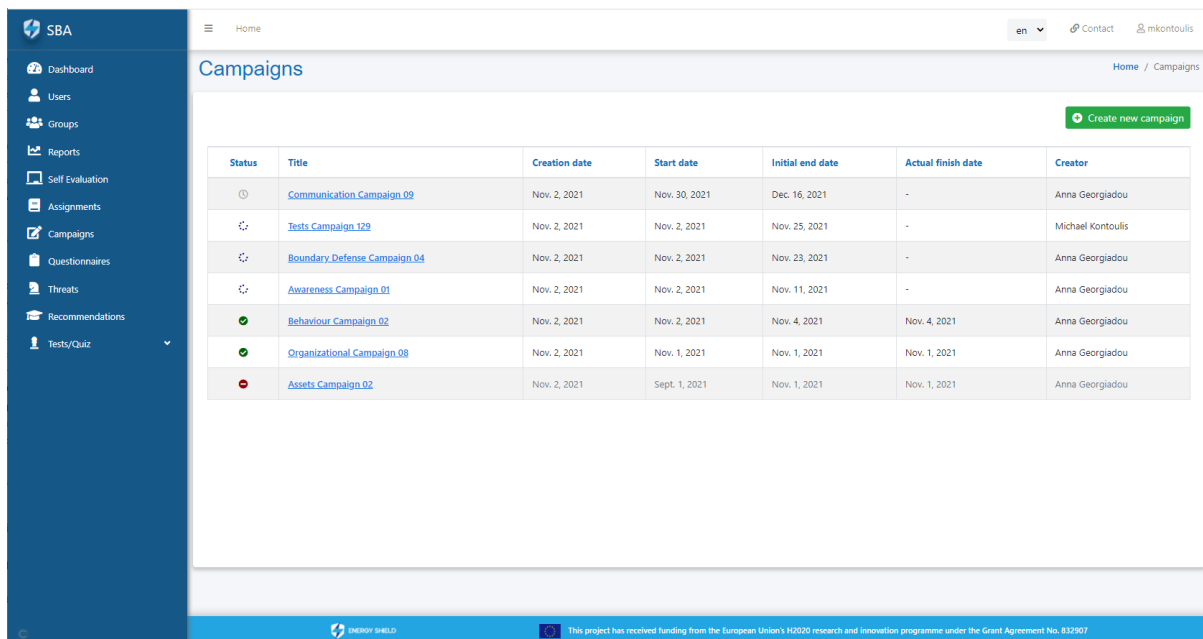
Dimension	Attitude
Employee Satisfaction Survey	Employee Satisfaction
No Questions	8
Best Score	-

Dimension	Awareness
HAIS-Q Knowledge	Policies and Procedures
No Questions	Awareness
Best Score	21

**Figure 24. Execute new assessment view**

## 1.6. CAMPAIGNS

This view (available only to administrators and managers) displays campaigns' information in a table as presented in Figure 25.



Status	Title	Creation date	Start date	Initial end date	Actual finish date	Creator
🕒	<a href="#">Communication Campaign 09</a>	Nov. 2, 2021	Nov. 30, 2021	Dec. 16, 2021	-	Anna Georgiadou
⚙️	<a href="#">Tests Campaign 129</a>	Nov. 2, 2021	Nov. 2, 2021	Nov. 25, 2021	-	Michael Kontoulis
⚙️	<a href="#">Boundary Defense Campaign 04</a>	Nov. 2, 2021	Nov. 2, 2021	Nov. 23, 2021	-	Anna Georgiadou
⚙️	<a href="#">Awareness Campaign 01</a>	Nov. 2, 2021	Nov. 2, 2021	Nov. 11, 2021	-	Anna Georgiadou
✅	<a href="#">Behaviour Campaign 02</a>	Nov. 2, 2021	Nov. 2, 2021	Nov. 4, 2021	Nov. 4, 2021	Anna Georgiadou
✅	<a href="#">Organizational Campaign 08</a>	Nov. 2, 2021	Nov. 1, 2021	Nov. 1, 2021	Nov. 1, 2021	Anna Georgiadou
❌	<a href="#">Assets Campaign 02</a>	Nov. 2, 2021	Sept. 1, 2021	Nov. 1, 2021	Nov. 1, 2021	Anna Georgiadou

**Figure 25. Campaigns view**

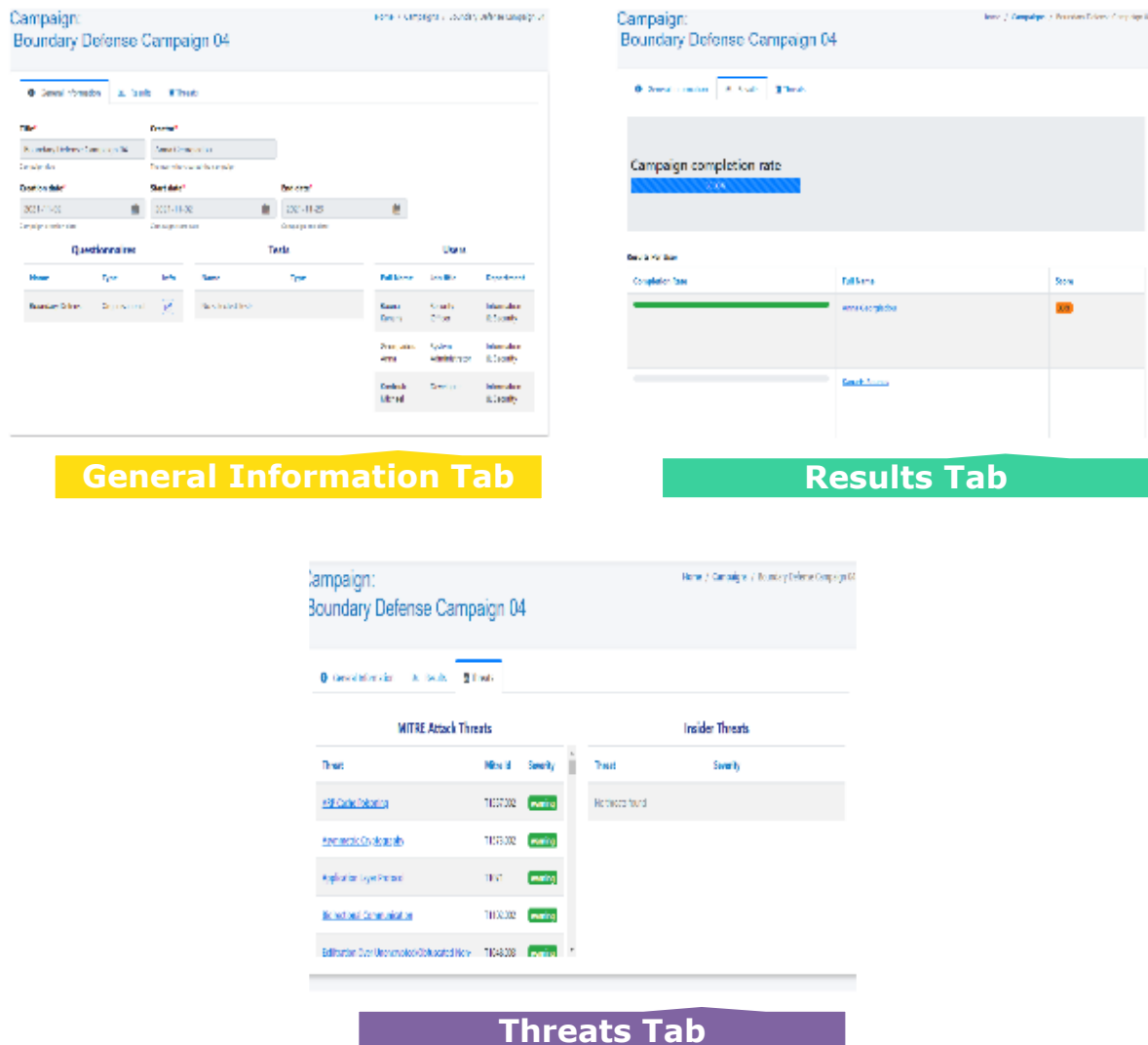
The campaigns' view exhibits **global campaigns** (description used for campaigns created by the administrators of the tool) to all users. If the signed-in user is a manager, along with global campaigns, the table also contains the campaigns created by the specific user. Administrators, as expected, have access and view to all campaigns available.

Selecting one of the displayed campaigns (by clicking on its title) redirects you to the campaign details view, which presents campaign-specific information and offers a number of different control actions.

As presented in Figure 26, the campaign details view contains:

- **General Information Tab:** title, creation details, start and end date, questionnaires and tests assigned and participants.
- **Results Tab:** summary of the results per user along with progress status.
- **Threats Tab:** summary of the identified cyber-security threats based on the evaluation results of the campaign.

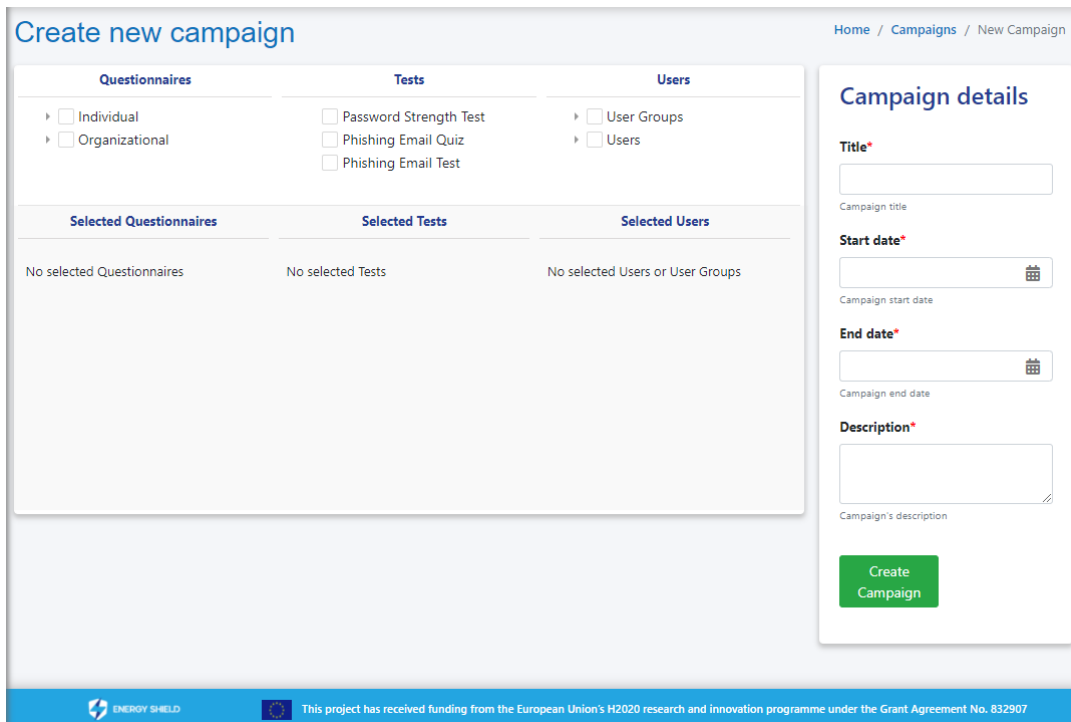




**Figure 26. Campaign details' view**

On the upper right part of the campaigns view, a “Create New Campaign” button is available, redirecting the user to the creation view presented in Figure 27. This view consists of:

- **Assignment card:** presents, in a tree view, the available questionnaires, tests, users and groups. Selecting any of these results in listing them on the lower part of the card while making correlated assignments between security culture controls and the corresponding campaign participants.
- **Campaign details card:** holds the campaign title along with the start and end date of the assessment period.

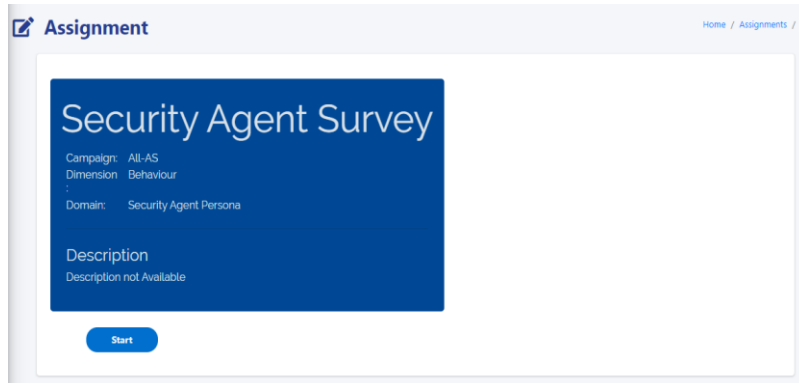


**Figure 27. Create new campaign view**

Upon creation of a campaign, a number of assignments are created and presented to the corresponding assignees through alternative paths, as follows:

- **Dashboard -> Assignments Card:** presents and offers access to active assignments. Additionally, it lists the completed and expired ones in different tabs.
- **User profile -> Assignment Tab:** presents user assignments along with a number of details offering access to the pending ones.
- **Assignments:** presents all users assignments along with a number of details, such as status, due date, etc. (paragraph 1.7 presents in detail the specific view).

When an active assignment is selected by its assignee, if it refers to a questionnaire, the survey execution mechanism is triggered, and an evaluation iteration is initiated, guiding the user through its completion. Upon submission, an achievement score is presented to the end-user.



**Assignment** Home / Assignments / 3

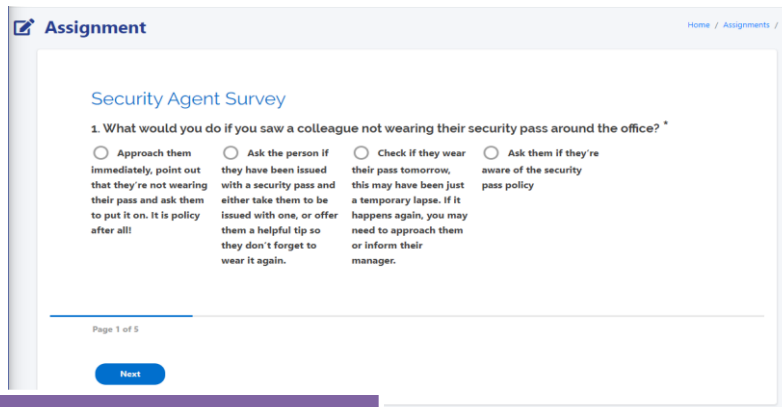
## Security Agent Survey

Campaign: All-AS  
Dimension: Behaviour  
Domain: Security Agent Persona

Description  
Description not Available

[Start](#)

### Initial Survey Page



**Assignment** Home / Assignments / 3

## Security Agent Survey

1. What would you do if you saw a colleague not wearing their security pass around the office? \*

☐ Approach them immediately, point out that they're not wearing their pass and ask them to put it on. It is policy after all!

☐ Ask the person if they have been issued with a security pass and either take them to be issued with one, or offer them a helpful tip so they don't forget to wear it again.

☐ Check if they wear their pass tomorrow, this may have been just a temporary lapse. If it happens again, you may need to approach them or inform their manager.

☐ Ask them if they're aware of the security pass policy

Page 1 of 5

[Next](#)

### Execution Page

**Figure 28. Questionnaire assignment execution**

If the assignment refers to a test, then the corresponding test is initiated, guiding the user through its completion. Upon submission, an achievement score is presented to the end-user.

# Password Strength Test

Type your passwords to check their strength

**Test password 1\*** **Retype Test password 1\***

**Test password 2\*** **Retype Test password 2\***

**Test password 3\*** **Retype Test password 3\***

[Calculate Score](#)

### About the game

In this game you can test the strength of your passwords.  
Insert 3 passwords like the ones that you usually use in order to evaluate their strength.

Your input is NOT saved, so feel free to test any kind of passwords.

## Password Strength Test

# Phishing Quiz

Decide whether a mail is a fraud or not

Email 1 of 2

**Google** <no-reply@google.support>  
to me

20:39 PM

Your account has been compromised!

Hi,  
Someone just used your password to try to sign in to your Google Account.

Information:  
Monday, November 30, 2020 at 4:38:11 PM GMT+02:00  
Slatina, Romania  
Firefox browser

Google stopped this sign-in attempt. You should change you password immediately

CHANGE PASSWORD

Phishing Email

Legit Email

Next Email

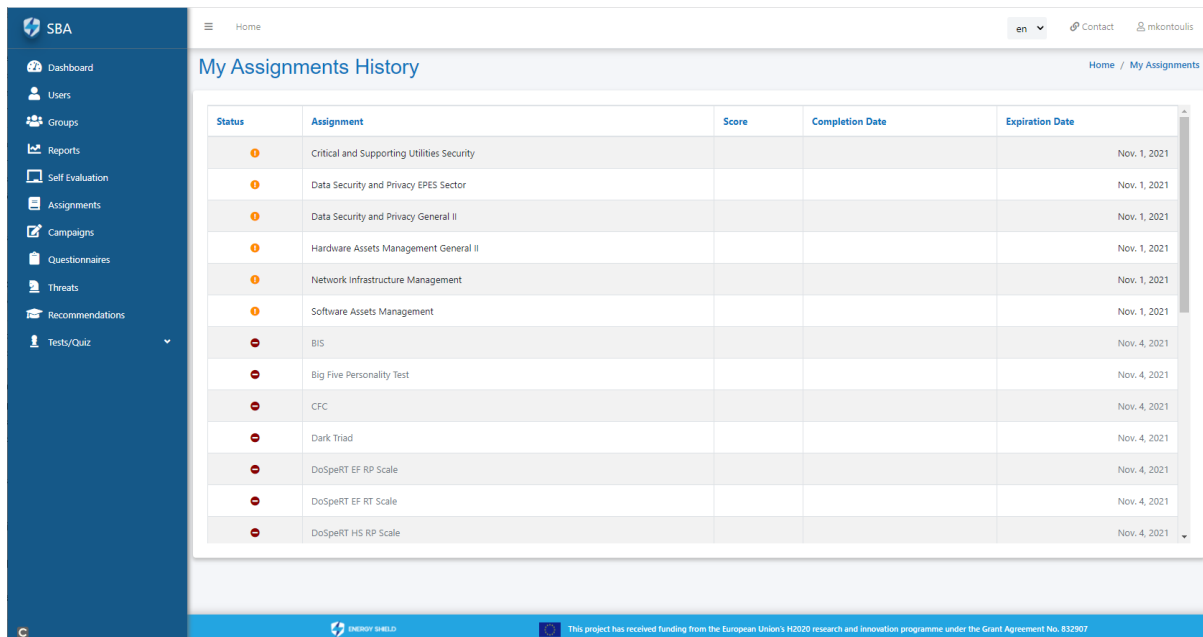
## Phishing Email Quiz

**Figure 29. Test assignment execution**

## 1.7. ASSIGNMENTS

This view displays all assignments, questionnaires and tests (apart from the phishing simulation test) made to the signed-in user via the different campaigns

they are participating in. In case the same questionnaire or test is assigned to them via different campaigns more than once during the same period, the tool ensures the user completes only once the assignment and the corresponding score is used in all related metrics.



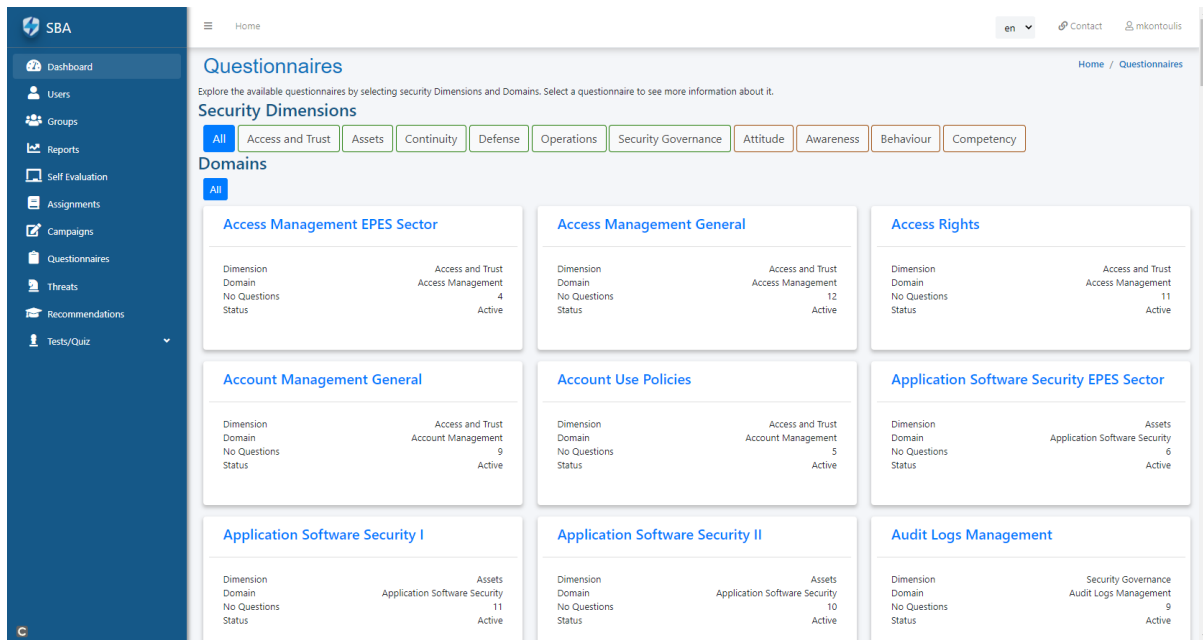
Status	Assignment	Score	Completion Date	Expiration Date
🟡	Critical and Supporting Utilities Security			Nov. 1, 2021
🟡	Data Security and Privacy EPES Sector			Nov. 1, 2021
🟡	Data Security and Privacy General II			Nov. 1, 2021
🟡	Hardware Assets Management General II			Nov. 1, 2021
🟡	Network Infrastructure Management			Nov. 1, 2021
🟡	Software Assets Management			Nov. 1, 2021
🔴	BIS			Nov. 4, 2021
🔴	Big Five Personality Test			Nov. 4, 2021
🔴	CFC			Nov. 4, 2021
🔴	Dark Triad			Nov. 4, 2021
🔴	DoSpERT EF RP Scale			Nov. 4, 2021
🔴	DoSpERT EF RT Scale			Nov. 4, 2021
🔴	DoSpERT HS RP Scale			Nov. 4, 2021

**Figure 30. Assignments view**

If an active assignment is selected, by clicking on its hyperlinked title, the survey or the test execution mechanism is triggered, depending on the nature of the assignment, and an evaluation iteration is initiated guiding the user through its completion (as presented in 1.6).

## 1.8. QUESTIONNAIRES

This view (available only to administrators and managers) displays the available cyber-security culture questionnaires while correlating them with the suggested model (levels, dimensions and domains) as presented in Figure 31.

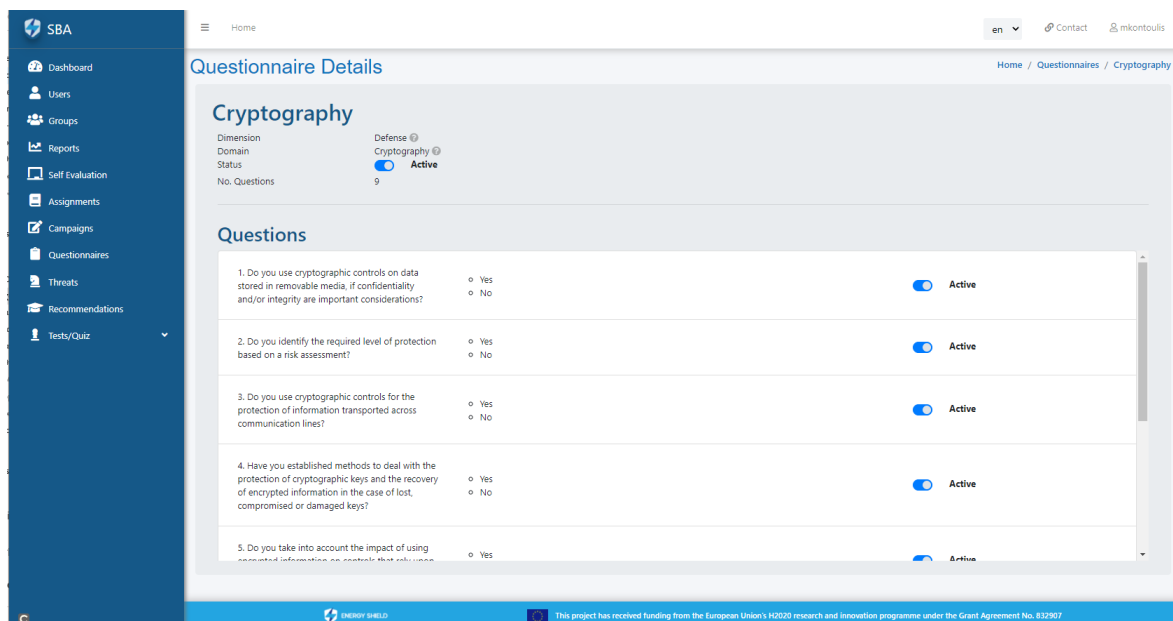


**Figure 31. Questionnaires view**

Selecting one of the displayed questionnaires (by clicking on its title) redirects you to the questionnaire details view, which presents questionnaire-specific information offering control over its activity status.

As presented in Figure 32, the questionnaire details view presents:

- Information correlating the questionnaire with the underlying cyber-security culture model.
- Questions along with their available options and control over their activity status.



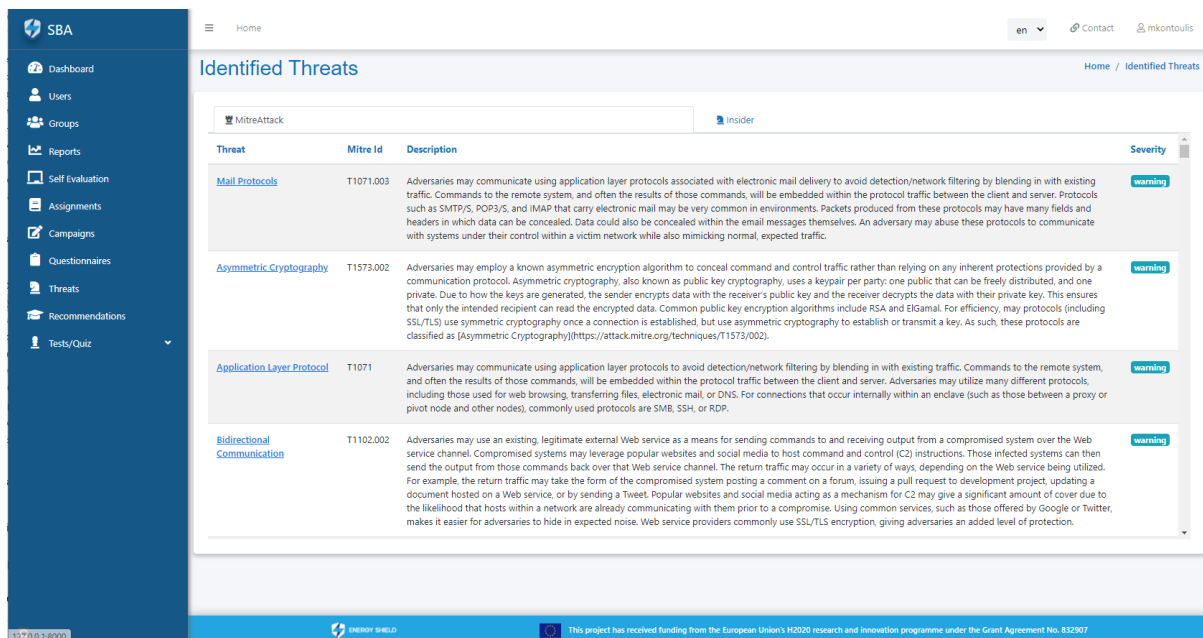
**Figure 32. Questionnaire details view**

## 1.9. THREATS

This view (available only to administrators and managers) displays the identified cyber-security threats the organisation is vulnerable against based on the evaluation campaigns held.

As presented in Figure 34, the recommendations view contains:

- **MITRE ATT&CK Tab:** listing all identified threats based on the hybrid MITRE ATT&CK Model for an OT Environment, consisting of a combination of the Enterprise and the ICS threat model. The specific tab enables the user to further investigate the attack patterns by offering an interconnection with the MITRE ATT&CK official website.
- **Insider Tab:** listing all identified insider threats based on the MERIT model developed by the Secret Service and the Software Engineering Institute CERT Program at Carnegie Mellon University.



Threat	Mitre Id	Description	Severity
<a href="#">Mail Protocols</a>	T1071.003	Adversaries may communicate using application layer protocols associated with electronic mail delivery to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Protocols such as SMTP/S, POP3/S, and IMAP that carry electronic mail may be very common in environments. Packets produced from these protocols may have many fields and headers in which data can be concealed. Data could also be concealed within the email messages themselves. An adversary may abuse these protocols to communicate with systems under their control within a victim network while also mimicking normal, expected traffic.	warning
<a href="#">Asymmetric Cryptography</a>	T1573.002	Adversaries may employ a known asymmetric encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Asymmetric cryptography, also known as public key cryptography, uses a keypair per party: one public that can be freely distributed, and one private. Due to how the keys are generated, the sender encrypts data with the receiver's public key and the receiver decrypts the data with their private key. This ensures that only the intended recipient can read the encrypted data. Common public key encryption algorithms include RSA and ElGamal. For efficiency, many protocols (including SSL/TLS) use symmetric cryptography once a connection is established, but use asymmetric cryptography to establish or transmit a key. As such, these protocols are classified as [Asymmetric Cryptography](https://attack.mitre.org/techniques/T1573/002).	warning
<a href="#">Application Layer Protocol</a>	T1071	Adversaries may communicate using application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.	warning
<a href="#">Bidirectional Communication</a>	T1102.002	Adversaries may use an existing, legitimate external Web service as a means for sending commands to and receiving output from a compromised system over the Web service channel. Compromised systems may leverage popular websites and social media to host command and control (C2) instructions. Those infected systems can then send the output from those commands back over that Web service channel. The return traffic may occur in a variety of ways, depending on the Web service being utilized. For example, the return traffic may take the form of the compromised system posting a comment on a forum, issuing a pull request to development project, updating a document hosted on a Web service, or by sending a Tweet. Popular websites and social media acting as a mechanism for C2 may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection.	warning

Figure 33. Threats view

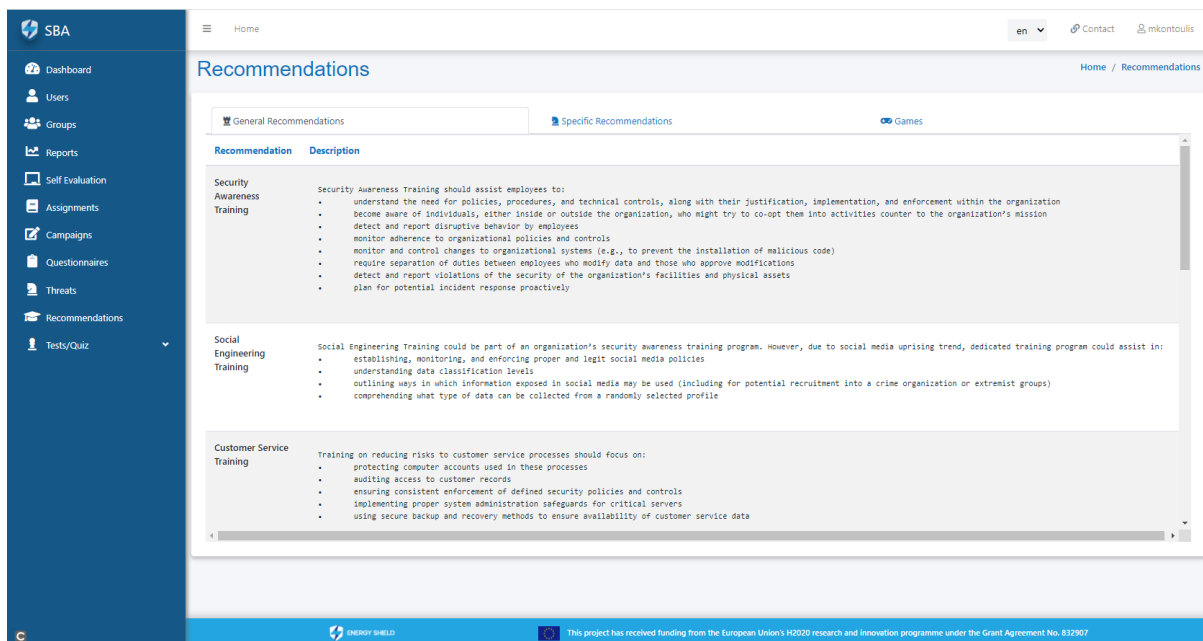
## 1.10. RECOMMENDATIONS

This view (available only to administrators and managers) displays a number of training recommendations aiming to assist the organisation in enhancing its cyber defence against the identified threats.

As presented in Figure 34, the recommendations view contains:

- **General Recommendations Tab:** listing training recommendations encompassing three aspects of the organisation:
  - Insider Threat Awareness Training for all organisational personnel (employees, contractors, consultants)
  - Training for Insider Threat Program personnel

- Role-based training for mission specialists that are likely to observe certain aspects of insider threat events, e.g.:
  - Human Resources
  - Information Assurance
  - Compliance Inspection
  - Legal Counsel
  - Behavioural Sciences
  - Information Governance
  - Finance
- **Insider Recommendations Tab:** listing training recommendations targeting the cyber-security threats the organisation is prone against based on the evaluation campaigns results.
- **Games:** listing a number of free online games where users can cultivate their cyber-security culture while playing and enjoying themselves. The specific games have been developed by security experts, agencies and educational institutions targeting individuals of different ages, nationalities, cultures and professional backgrounds.



**Figure 34. Recommendations view**

### 1.11. TESTS/QUIZ

This view (available only to administrators and managers) offers a workspace where a user can customise the available tests to better address the organisational needs. This menu offers the following options:

- **Phishing Quiz Creation Form:** this form allows the user to create a new email entry which shall later on become available for usage to the Email Phishing Quiz. Information required includes the sender email and display name, the email title, a phishing flag indicating whether the email is legit or



not and an email file (UTF-8 encoded HTML file). When all information is filled in, an email preview offers the possibility to the user to overview the result prior to uploading it to the SBA tool.

- **Phishing Simulation Creation Form:** this form allows the user to create a new email entry which shall later on become available for usage to the Email Phishing Simulation. Information required includes the email title, the email subject and an email file (UTF-8 encoded HTML file). The email file needs to be properly edited prior to uploading so as to include the encrypted link provided within the form. If not, an error message shall inform the user that the email file does not meet the required specifications. When all information is provided appropriately, an email preview offers the possibility to the user to overview the result prior to uploading it to the SBA tool.

### Email Creation Form

Upload your html source code with additional information

**Sender email\***

**Is a Phishing email?\***

☒ Yes

☐ No

**Sender display name\***

**Email file\***

No file chosen

**Email title\***

Email Preview

No email inserted

Phishing Quiz Creation Form

### Simulation Email Form

Create an email to run phishing simulation. Please provide somewhere in your email the encrypted link. Insert only .html or .txt files

**Title\***

**Email subject\***

**Encrypted link\***

**Email file\***

No file chosen

Email Preview

No email inserted

Phishing Simulation Creation Form

**Figure 35. Test/Quiz views**

The uploaded emails, in both cases, become instantly available for selection to the campaign creation form (tests submenu).

## DEVELOPING THE CYBER-TOOLKIT THAT PROTECTS YOUR ENERGY GRID

---



[www.energy-shield.eu](http://www.energy-shield.eu)

