



SMESEC

Protecting Small and Medium-sized Enterprises digital technology through an innovative cyber-SECurity framework

D5.5 Open Call Design, Implementation and Results Report

Document Identification			
Status	Final	Due Date	31/05/2020
Version	1.0	Submission Date	07/06/2020

Related WP	WP5, WP3	Document Reference	D5.5
Related Deliverable(s)	D5.4, D3.6, D3.7	Dissemination Level (*)	PU
Lead Organization	FORTH	Lead Author	Manos Athanatos, FORTH
Contributors		Reviewers	Philippe Cousin, EGM Filip Gluszak, GridPocket

Keywords:
Open Call, Evaluation, Testing, Results

This document is issued within the frame and for the purpose of the SMESEC project. This project has received funding from the European Union's Horizon2020 framework Programme H2020-DS-SC7-2016 under Grant Agreement No. 740787 and supported by Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 17.00067. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the European Commission.

This document and its content are the property of the SMESEC Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the SMESEC Consortium or the Partners detriment and are not to be disclosed externally without prior written consent from the SMESEC Partners.

Each SMESEC Partner may use this document in conformity with the SMESEC Consortium Grant Agreement provisions.

(*) Dissemination level.-**PU**: Public, fully open, e.g. web; **CO**: Confidential, restricted under conditions set out in Model Grant Agreement; **CI**: Classified, **Int** = Internal Working Document, information as referred to in Commission Decision 2001/844/EC.

Document Information

List of Contributors	
Name	Partner
Jose Francisco Ruiz	ATOS
Alberto Miranda	ATOS
Pablo Barrientos Lobato	ATOS
Christos Tselios	CITRIX
Philippe Cousin	EGM
Samuel Fricker	FHNW
Alireza Shojaifar	FHNW
Manos Athanatos	FORTH
George Tsirantonakis	FORTH
Sotiris Ioannidis	FORTH
Christos Papachristos	FORTH
Demetres Mavroeidis	FORTH
Kostas Lampropoulos	UOP
Bilge Yigit Ozkan	UU

Document History			
Version	Date	Change editors	Changes
0.1	14/02/20	M. Athanatos, FORTH	TOC, Initial Draft
0.5	14/03/20	S.Ioannidis, FORTH	Final TOC, Initial Input
0.6	03/04/20	B. Yigit Ozkan, UU	Section 3.1, 3.4 finalized
0.61	05/04/20	G.Tsirantonakis, FORTH	Section 2 finalised, Section 1 update
0.62	06/04/20	S. Fricker, FHNW	Section 3.2 finalized
0.63	08/04/20	D.Mavroeidis, FORTH	Section 3.5, 3.6 finalised
0.64	20/04/20	A. Krithinakis, FORTH	Section 3.3 added, changes to the table of 2.3 from SCYTL and UU were consolidated
0.65	24/04/20	C.Papachristos, FORTH	Section 4.2 Final draft
0.65	27/04/20	M.Athanatos, FORTH	Executive Summary, Conclusions final draft
0.65	05/05/20	B. Yigit Ozkan, UU A. Miranda, ATOS	Added Annexes, input to section 4.7
0.7	10/05/20	M.Athanatos, FORTH C. Tselios, CITRIX	Conclusion completed, References and List of Acronyms updated. Section 4.1 added.
0.75	11/05/20	K.Lampropoulos, FORTH	Added input to section 4.5
0.80-0.85	22/05/20	P.COUSIN EGM	Analysis in section 4.5 +4.4
0.90	25/05/20	M.Athanatos, FORTH	Integration of Input, uniformity changes.

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	2 of 115
Reference:	D5.5	Dissemination:	PU
	Version:	1.0	Status:
			FINAL

0.91	30/05/20	S.Fricker, A.Shojaifar, FHNW	CYSEC awareness impact evaluation
0.91_QA	01/06/20	Philippe Cousin, EGM	QA1 review
0.91_QA2	03/06/20	Filip Gluszak ,Adam Nawarycz, GRIDP	QA2 review
0.92	05/06/20	Manos Athanatos, FORTH	Final version to be sent to the coordinator
1.0	07/06/20	ATOS	Quality check and submission to EC

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Manos Athanatos (FORTH)	05/06/2020
Technical manager	Christos Tselios(CITRIX)	05/06/2020
Quality manager	Rosana Valle(ATOS)	07/06/2020
Project Manager	Jose Francisco Ruiz (ATOS)	07/06/2020

Table of Contents

Document Information	2
List of Tables.....	6
List of Figures	7
List of Acronyms.....	9
Executive Summary	10
1 Introduction	11
1.1 Purpose of the document	11
1.2 Relation to other project work.....	11
1.3 Structure of the document	11
2 Open Call Initial Design and Dissemination	13
2.1 Introduction	13
2.2 Open Call Categories.....	14
2.2.1 Category 1. Red Team.....	14
2.2.2 Category 2a. Full Integration and testing	15
2.2.3 Category 2b: External API Integration.....	15
2.2.4 Category 3: SME Association	15
2.3 Open Call Dissemination Activities	16
3 Applications and Evaluation Process	18
3.1 Introduction	18
3.2 Application Process	18
3.3 Evaluation Process	20
3.3.1 Eligibility Criteria.....	20
3.3.2 Evaluation Criteria.....	20
3.3.3 Marking Guideline.....	21
3.3.4 Calculating the Scores	22
3.3.5 Criteria for Profiling the Category 2a Applicants	22
3.4 Evaluation Committee	23
3.5 Evaluation Results (@FORTH).....	25
3.6 Summary of Execution Plan.....	26
4 Open Call Results.....	29
4.1 “Category 1. Red Team”—Technical Results and Findings	29
4.1.1 Security Findings.....	29
4.1.2 SMESEC Recommendations.....	29

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	4 of 115
Reference:	D5.5	Dissemination:	PU
	Version:	1.0	Status:
			FINAL

4.2	“Category 2a: Full Integration and testing” Technical Results	29
4.2.1	Provided Tests	29
4.2.2	Summary of tests for Category 2a	31
4.2.3	BLACKBOXSECU	33
4.2.4	CareAcross	38
4.2.5	AESSE.NET	41
4.2.6	ITML	44
4.2.7	Fraud Line	47
4.3	“Category 2b: External API Integration” Technical Results	49
4.3.1	AEGIS	50
4.3.2	After Tech.....	51
4.3.3	RKL	52
4.4	“Category 3: SME Association”—Activities and Results	53
4.4.1	SMESEC promotion and engagement	53
4.4.2	SMESEC Promoting Security Awareness	54
4.4.3	Feedback on SMESEC	55
4.5	Training and Awareness -- Results.....	57
4.5.1	Training Courses and Material	57
4.5.2	Impact on Awareness (CYSEC tool used by the OpenCall SMEs).....	61
4.5.3	Results	65
4.5.4	Analysis	75
4.5.5	Overview of the impact	78
4.6	Lesson Learnt	78
4.6.1	Summary and Conclusions for Category 2a	79
4.6.2	Summary and Conclusions for Category 2b.....	80
4.7	Additional Input	81
5	Conclusions	83
6	References	84
	<i>ANNEX I – Category 1 Contractual technical tasks</i>	85
	<i>ANNEX II - Category 2a Contractual technical tasks</i>	86
	<i>ANNEX III - Category 2b Contractual technical tasks</i>	87
	<i>ANNEX IV- Category 3 Contractual technical tasks</i>	88
	<i>ANNEX V- Application Evaluation Templates</i>	89
	<i>ANNEX VI- Questionnaires</i>	94

List of Tables

Table 1 Dissemination activities for the Open Call (per partner).....	16
Table 2 Eligibility Criteria and their applicability to the categories.	20
Table 3 Evaluation Criteria and Their Applicability to the Categories	20
Table 4 Marking Guideline for the Evaluation Process	21
Table 5 Criteria for Profiling for Category 2a Applications	22
Table 6 Guideline for Profiling Category 2a Applicants.....	22
Table 7. Institute/Company of each Committee Member	24
Table 8. Open call applicants’ origin country per category	25
Table 9. Reviewers' final scores.....	25
Table 10. Accepted SMEs to be funded by SMESEC.....	26
Table 11. Open Call Execution Plan	26
Table 12. List of tests for the Open Call evaluation process.....	30
Table 13. Category 2a Tests' Summary	32
Table 14. List of tests executed from BLACKBOXSECU	33
Table 15. List of tests executed from CareAcross.....	38
Table 16. List of tests executed from AESSE.NET	41
Table 17. List of tests executed from ITML.....	44
Table 18. List of tests executed from ITML.....	47
Table 19: A detailed list of threat, vulnerabilities, and security controls for refreshing interviewees’ minds	62
Table 20: CYSEC evaluation survey questionnaire	64
Table 21: The questionnaire template for the structured interview with the use case partners	65
Table 22: OpenCall partners demographics	65
Table 23: Observation and Feedback from the Heraklion workshop.....	66
Table 24: Survey results	66
Table 25: SME 1 interview results	71
Table 26: SME 2 interview results	72
Table 27: SME 5 interview results	73
Table 28: SME7 interview results	74
Table 29: SME8 interview results	75
Table 30: Perceived CYSEC usefulness based on survey and interview results (5 - fully agree, 4 - agree, 3 - neither agree nor disagree, 2 - disagree, 1 - fully disagree)	76
Table 31: Missing knowledge and capabilities	77
Table 32. Impact after using CYSEC	78

List of Figures

Figure 1. Important Open Call Dates	19
Figure 2. Evaluators(invited) Distribution among EU	23
Figure 3. Evaluators' Profiles	24
Figure 4. Screenshot of test results for malware downloading process on a Linux OS (Ubuntu 16.04) laptop with installed BitDefender “end-point” protection.....	35
Figure 5. Screenshot of BitDefender dashboard correctly identifying the Linux test laptop with installed BitDefender “end-point” protection	35
Figure 6. Screenshot of BitDefender “end-point” scanning action on Windows 10 machine.....	36
Figure 7. Screenshot #1 of BitDefender (GravityZone) dashboard and threat detection on a Windows 10 machine	36
Figure 8. Screenshot #2 of BitDefender (GravityZone) dashboard and threat detection and correction on a Windows 10 machine	37
Figure 9. Screenshot #1 of BitDefender scan status on a Windows 10 machine and detection of attacker’s address.....	37
Figure 10. Screenshot #2 of BitDefender (GravityZone) dashboard with scan status of “end-point” test machines (Windows 10) and detection of attacker’s address.....	38
Figure 11. Screenshot of CySEC dashboard showing an issue to connect to the system.....	38
Figure 12. Firewall-Malware- Phishing test.....	43
Figure 13. BitDefender dashboard, successfully blocked of malicious url	43
Figure 14. SMESEC SIEM dashboard.	44
Figure 15. Detection of port scanning	45
Figure 16. Honeypot DDOS Attack	46
Figure 17. SSH Brute Force Attack.....	46
Figure 18. Reports from XL-SIEM	46
Figure 19. CYSEC results #1	47
Figure 20. CYSEC results #2	47
Figure 21. XL-SIEM general report graphs.	48
Figure 22. Alerts as received by XL-SIEM agent	49
Figure 23. Results of EWIS testing as appear in SMESEC framework.	49
Figure 24 - AEGIS log sent to SMESEC	50
Figure 25 - AEGIS log received by SMESEC	51
Figure 26- AfterTech log sent to SMESEC.....	51
Figure 27- AfterTech log received by SMESEC.....	52
Figure 28- RKL log sent to SMESEC	52
Figure 29 - RKL log received by SMESEC	52
Figure 30. Detailed Numbers from CEO’s Shares on LinkedIn.....	53
Figure 31. Detailed Numbers from CCO’s Shares on LinkedIn	54

Document name:	D5.5 Open Call Design, Implementation and Results Report			Page:	7 of 115	
Reference:	D5.5	Dissemination:	PU	Version:	1.0	Status: FINAL

Figure 32. Examples of Follow-up Emails.....	55
Figure 33. SMESEC Training Courses and Awareness Platform	57
Figure 34: Answers from the 8 SMEs on Overall Experience (Score from 0 to 10).....	58
Figure 35: Answers Whether the Objectives of the Courses Were Met.....	59
Figure 36 : Answers on Whether it was Easy to Apply What Was Learnt	59
Figure 37: Answers on Whether SMEs Would Recommend the Courses to Colleagues.....	60
Figure 38: CYSEC dashboard and work area.....	61

Document name:	D5.5 Open Call Design, Implementation and Results Report			Page:	8 of 115
Reference:	D5.5	Dissemination:	PU	Version:	1.0
				Status:	FINAL

List of Acronyms

Abbreviation / acronym	Description
API	Application Program Interface
CVE	Common Vulnerabilities and Exposures
CSRF	Cross-Site Request Forgery
DDOS	Distributed Denial of Service
EWIS	Early Warning Intrusion Detection System
HTTP	Hypertext Transport Protocol
IDS	Intrusion detection System
IoT	Internet of Things
IT	Information Technology
ROP	Return-oriented Programming
SME	Small and Medium Enterprises
SSI	Server Side Includes
SQL	Structured Query Language
TaaS	Test as a Service
TRL	Technology Readiness Level
URL	Uniform Resource Locator
XML	eXtensible Markup Language

Executive Summary

SMESEC project's main objective is improving the level of security and protection against cyber-security threats, the contemporary smart services and products provided from SMEs to their end-users (big companies, infrastructure, citizens, public administration, etc.). To address the challenges that SMEs and entities with limited budget are facing today, the overall concept of SMESEC is organized around the following distinct 5 concepts: i) Definition & Recommendations, ii) Discovery & Solutions, iii) Protection & Response, iv) Extensive validation and v) Training & Awareness. These concepts represent the phases of a complete lifecycle for cyber-security protection and each one of them is realized through a set of processes offered by SMESEC framework.

This deliverable outlines the work completed in the context of Task 5.5 “*SMESEC open call organization, execution and result collection/evaluation*”. This task consists of the validation of the SMESEC solution by means of external SMEs. The selection of these SMEs happened by means of an Open Call. The result of this validation was supplemental to the one performed in Task 5.3. The objective of this task was to demonstrate that SMESEC is able to cover security needs in existing solutions (products and/or services) provided by the SMEs selected during the Open Call process in a range of market sectors, which can strengthen their operation by means of enhanced security features.

The task 5.5 consists of three general and different stages. The first stage, to begin with, included all the preparatory activities for the setup of the SMESEC open call. This action implements the basic principles that were specified in WP1 and moves forward to build up the rules and review process of the open call for SMEs to evaluate the SMESEC security framework. In the first stage, all the organizational issues of the open call realization were addressed, the formulation of the feedback to be collected from SMEs participating in this call was specified and the technical, business and management procedures to be followed during the execution phase were decided. The outcome of this task was the call for participation in the extended validation phase of the SMESEC security framework for SMEs, that could offer diverse applications compared to the ones that the consortium pilots provide. The second stage of this task included all activities involved in the execution of the SMESEC open call starting from the open call review process implementation that led to the selection of the most appropriate SMEs that fitted the SMESEC vision. This phase, after appropriate SME selection, involved all communication activities with the selected SMEs, the technical guidance for realizing the SMESEC security framework, the overview of the framework realization by the selected SMEs and the reporting guidance of the evaluation procedures on the SMESEC framework leading to the final stage (third stage) of this task. The third stage of this task included two main activities. The first activity was focused on the collection of evaluation results of the SMESEC security framework realization by the selected open call SMEs. The second activity is focused on the processing of the collected results and their analysis to extract evaluation conclusion regarding the final SMESEC security framework.

Document name:	D5.5 Open Call Design, Implementation and Results Report			Page:	10 of 115		
Reference:	D5.5	Dissemination:	PU	Version:	1.0	Status:	FINAL

1 Introduction

1.1 Purpose of the document

The purpose of this document is to present all the work done for materialisation of the SMESEC Open Call, namely all the work in the context of “Task 5.5 SMESEC open call organization, execution and result collection/evaluation” of WP5. It will present in detail all the efforts for the creation of the Open Call namely: The application procedure, the evaluation process and the rationale / respective documents of the evaluation process, the execution plan along with its execution details, the Open call evaluation results and the selected SMEs for the Open Call. The execution of the Open Call and the Evaluation results as reported from the participants. We summarise and present the lessons learnt and the overall conclusions on the SMESEC framework and provide some additional information about the social-economic and business model of SMESEC as perceived by the participants.

Additionally, at the closing of this document there is an Annex section containing all the relevant documents and procedures followed during the realisation of the task. Note that, since this is a public document, the SMESEC Security Advisory Board requested that only templates and documents that do not present private information are depicted here all other relevant information and documents with all other details to be included in the internal “SMESEC annual report on project management (Year 3)” Deliverable namely D7.4.

1.2 Relation to other project work

The work of this task and presented here is used for the augmenting the evaluation of the SMESEC framework by means of external SMEs. Thus, the results produced during the Open Call process were distributed and used by the all the tool providers to revise the framework, providing feedback back to main development work package of the project namely WP3. Additionally, the we received useful feedback for the Training component of SMESEC and the CySec tool that studied the security awareness prior and after the use of SMESEC.

Moreover, all the evaluation reports provided additional input to task T5.4 that will report overall assessment of the framework. The internal evaluation trials that were designed in T5.1 and the demos and evaluation of T5.3 provided the template for the trials that took place in the context of SMESEC Open Call. The results of T5.1 and T5.3, along with the evaluation results of T5.5 will allow the creation of the final evaluation report of SMESEC in D5.4. of T5.4.

Furthermore, as the Open Call gave us the opportunity to receive feedback on the Business Plan of SMESEC and assist on the social-economic analysis of the SME plane we the results of these analysis will be presented in D6.4[2] and D5.4[3] respectively.

1.3 Structure of the document

The document is divided in two parts. The main document and the Annexes part. The main document is structured as follows

Chapter 1 presents an introduction of the deliverable;

Chapter 2 presents the initial design and the dissemination activities of the Open Call;

Chapter 3 depicts the applications and evaluation process that we followed;

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	11 of 115				
Reference:	D5.5	Dissemination:	PU	Version:	1.0	Status:	FINAL

Chapter 4 summarises the main outcomes of the open call procedure: The Open Call Results;

Chapter 5 concludes the document;

Chapter 6 presents all the references used in the document

Finally, the Annexes section includes:

Annex I presents the contractual technical tasks for open call Category 1

Annex II presents the contractual technical tasks for open call Category 2a

Annex III presents the contractual technical tasks for open call Category 2b

Annex IV presents the contractual technical tasks for open call Category 3

Annex V includes templates used for the evaluation of open call applicants

Annex VI includes the questionnaire that was provided to the open call participants

Document name:	D5.5 Open Call Design, Implementation and Results Report			Page:	12 of 115		
Reference:	D5.5	Dissemination:	PU	Version:	1.0	Status:	FINAL

2 Open Call Initial Design and Dissemination

2.1 Introduction

In this section, we are describing the initial design of the Open Call and all the Dissemination actions taken in order to promote the Open Call and receive as many applications as possible. The main objective of the open call was the validation of the SMESEC solution with SMEs outside the SMESEC consortium. The validation provided feedback and insights to the project to produce a product that is closer to the market's needs with a high TRL (Technology Readiness Level). Moreover, through the open call, we were able to demonstrate that SMESEC can cover security needs in existing solutions (products and services) provided by these SMEs in a range of market sectors, which can strengthen their operation using enhanced security features.

For the interested participants, the open call consists of 2 stages:

- First stage: collection of applications and selecting of participating third-parties. After the external partner selection, a hands-on workshop was performed with the selected partners, guidance for using the SMESEC security framework provided, and instructions shared for reporting about the experience using the SMESEC evaluation procedures.
- Second stage: collection of the results of evaluating the SMESEC security framework by the selected open call partners. These collected results will be analysed to extract conclusions for evolving the SMESEC framework.

In the initial design the open call, work consisted of three distinct phases (i) [M20-M24) All preparatory activities, (ii) [M24-M30) Execution of the Open Call (ii) [M30-M36] Collection and analysis of Open Call results. This timeline was revised as these phases, in proposal phase, were considered as distinct phases without interconnection. But this was not the case in the real execution of the open call, some of these actions could be performed in parallel. During the execution phase the tool providers of the consortium as well as the leader of the evaluation WP5, participated in bi-weekly calls with the Open call participants directly receiving the feedback for the tools and the framework and providing updates/guidance to the participants.

The time plan that was finally followed had minor deviation from the one that was presented during the second project technical review meeting in Barcelona, to the project reviewers. The plan was executed in whole, retrieving all the results from the Open Call participants, feeding the evaluation process WP5 and the process of finalizing SMESEC Framework and Training and Awareness platform of WP3. The key activities that took place during the open call design and initiation process were the following:

- Initiation of the Open Call consortium committees
- Internal discussion through regular meetings for the categories of the open call and the publication of the call
- Open Call publication (12/03/2019)84
- Selection of the Evaluation Committee. More information is presented in section 3
- Dissemination of the Open Call
- Applications gathering (12/03-15/05/2019)
- Evaluation of applications (09-16/05/2015)
- Notification to the selected applicants (June 2019)
- First online meeting with the Open Call participants and kick off of the Open Call (16/07/2019)
- First F2F meetings between the Consortium and the Open Call participants (9-10/09/2019)

Document name:	D5.5 Open Call Design, Implementation and Results Report			Page:	13 of 115		
Reference:	D5.5	Dissemination:	PU	Version:	1.0	Status:	FINAL

More information on these activities and key decisions are discussed in this section and in Section 3, whilst the feed and the analysis of the open call results are presented in Section 4.

2.2 Open Call Categories

There was a broad discussion inside the consortium about the different categories that will be supported by the Open Call. We wanted to evaluate all the major functionalities introduced by SMESEC, thus we focused on different SMEs' categories to provide a broad and in-depth evaluation of the developed Framework. In the process, we also followed the comments of the PO and reviewer from the 1st technical meeting and for the AB members, including one red team category to evaluate the framework. Since SMESEC is dedicated to SMEs we wanted to include all flavours of SMEs. More in information of the specific all the criteria can be found in Section 3.

To realize the decided broad validation of all the features provide by the SMESEC Framework we have defined three different categories that are furthered described in sections 2.2.1, 2.2.2, 2.2.3 and 2.2.4 respectively:

- Category 1: Red Team/ Tiger Team
- Category 2a. Full Integration and testing
- Category 2b: External API Integration
- Category 3: SME Association

Based on the available funds and local legislation for procurements in the scope of the project, we have decided the following number of accepted proposals and funding per category:

- For category 1, a maximum one proposal will be funded with € 20.000,00 (excl. VAT)
- For category 2a, a maximum of five proposals will be funded with € 15.000,00 (excl. VAT)
- For category 2b, a maximum of three proposals will be funded with € 12.000,00 (excl. VAT)
- For category 3, a maximum of one proposal will be funded with € 7.000,00 (excl. VAT)

Also, based on the partners' internal procedures and national legislation, it was agreed that financing of the selected proposal will be performed in a single deposit, upon the delivery and acceptance of the evaluation report. All logistics and funding of the selected SMEs were handled by two partners FORTH and UU. In the reminder of Section 2.2, you can find a general description for every category and the rationale behind the creation of each category.

2.2.1 Category 1. Red Team

Following the comments from the 1st technical review, our internal consortium discussion and after receiving the approval of the PO, we included a Red Team category to the open call process. The rationale behind this category was that a red team will be able to assist on the evaluation of the security status of the framework, as well as the added security value imposed by the SMESEC framework to our pilots. In that sense one of our pilots was selected to be examined prior and after the installation of SMESEC in the pilot. The detailed technical tasks of the contract signed with Red Team can be found at ANNEX I

Description as Published in the Call:

“Category 1: 1 Red Team will assess the security level of the involved SMEs before and after the deployment of the SMESEC Framework. The applicants will be evaluated based on the proved experience in assessing systems for cyber-threat, their cybersecurity expertise and overall IT experience.”

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	14 of 115
Reference:	D5.5	Dissemination:	PU
	Version:	1.0	Status:
			FINAL

2.2.2 Category 2a. Full Integration and testing

This is the main category of the Open Call. It is the category that used all the features of the SMESEC framework to protect their day to day operations from cybersecurity incidents. The evaluation of the framework was divided in five categories which are based on the five pillars of features provided by the SMESEC framework, namely: (i) “Detection and Response”, (ii) “Protection and Response”, (iii) “Capability and Awareness”, (iv) “Training Courses & Material”, (v) “Lessons Learned” and (vi) “Business model and the market acceptance”. Each participated SME was obliged to perform specific actions for each of the evaluation categories as described in the technical annex of the contracts that were signed between the consortium and the selected SMEs. Specific Tasks for category 2a can be studied in ANNEX II

In order to broaden our diversity and coverage, we looked for a distinct set of SMEs with multiple capabilities. For this category, all applicants were placed into three sub-categories (high, medium, low) based on the expertise on IT and the adoption level of ICT to their day-to-day operations.

Description as Published in the Call:

“Category 2a: up to 5 SMEs that will incorporate SMESEC framework taking advantage of all the features provided by SMESEC, e.g. threat protection and response tools, security awareness and training, testing and recommendation tools. As we are seeking for a diverse set of SMEs for this category, all applicants will be placed into three categories (high, medium, low) based on the expertise on IT and the adoption level of ICT to their day-to-day operations. Then 2 applicants will be selected from the high category, 2 from the medium category, and 1 from the low category.”

2.2.3 Category 2b: External API Integration

The scope of this category was to test and evaluate the External API of the SMESEC. This API allows external cybersecurity solution provider to attach their solutions to the SMESEC Framework promoting the overall capabilities of SMESEC, adding more events resources. This also creates a cybersecurity Ecosystem based on the SMESEC platform where solutions providers can offer their solutions to a broader audience. Finally, it promotes the business opportunities both for the SMESEC as well as the involved external solution provider. We decided to fund up to three SMEs from providing cybersecurity solutions that will test the external integration API, incorporating their cybersecurity solutions to the SMESEC framework. We sought for experienced SMEs with a strong background in cybersecurity. The technical tasks that were performed by the SMEs of Category 2b can be found at ANNEX III

Description as Published in the Call:

“Category 2b: up to 3 SMEs from providing cybersecurity solutions that will test the external integration API, incorporating their solutions to the solutions of the SMESEC framework. We seek experienced SMEs with a strong background in cybersecurity.”

2.2.4 Category 3: SME Association

The rationale behind involving a SME Association in the SMESEC Open Call was backed on the following grounds: (i) To promote the cybersecurity awareness to the SMEs’ of the association and in general (ii) To receive feedback from a community of SMEs on particular tools (iii) To provide feedback on the overall approach chosen by SMESEC (iv) To organize collective actions and provide feedback about KPIs and SME practice improvements recommended by the SMESEC tools to improve our

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	15 of 115
Reference:	D5.5	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

solutions. We were focused on applicants that involve a large number of SMEs and events. The description of the tasks that were requested and agreed with the SME Association of Category 3 can be found at ANNEX IV

Description as Published in the Call:

“Category 3: 1 SME association, community, or ecosystem to help increase awareness on SMEs cybersecurity issues by using and validating the SMESEC framework. As the project provides a comprehensive framework of tools for cybersecurity, we look for feedback from a community of SMEs in particular on the tool’s acceptance, on the overall approach chosen including usefulness and easiness to use the tools, etc. We look for applicants helping to organise collective actions and provide feedback about KPIs and SME practice improvements recommended by the SMESEC tools to improve our solutions. The applicants will be evaluated on the number of SMEs involved and on the potential impact of the SMESEC framework to increase SMEs’ cybersecurity protection.”

2.3 Open Call Dissemination Activities

The whole consortium pushed the dissemination of Open Call to their countries, SME associations and directly to their work contacts. A list of the dissemination activities as presented at the 2nd SMESEC technical review meeting are depicted in the following table.

Table 1 Dissemination activities for the Open Call (per partner)

Partner	Activity	Activity	Activity	Activity
@ATOS	Repost/retweet of original post	Dissemination using corporate tools of social media	Promoted Via Cyberwatching.eu	Contacted ECSO and promoted through their network. Contacted EU SBA and Funding Box
@BD	Promoted through Local SME Association	Repost/Retweets of original post		
@CITRIX	Post/tweet of open call announcement	Repost/retweet of official post/tweet	Shared with Patra’s Science Park (https://www.psp.org.gr/) which hosts ~30 SMEs	Shared with Orange Grove Patra’s (http://orangegrovepatras.biz/), a local incubator with 20+ start-ups
@EGM	Promoted through Local SME Association	Repost/Retweets of original post		
@FHNW	Permanent banner to the web page	Promoted through Local SME Association	Promoted to Swiss SME association	Published all material via smesec.eu site
@FORTH	Repost/Retweets of original post Post via the official ICS-	invitation in Greek and Disseminated via Praxi Network (SME Association)	Invitations via a local incubator	Contacted ECSO and promoted through their network. Contacted EU SBA and Funding Box

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	16 of 115
Reference:	D5.5	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

	FORTH media accounts			
@GRIDP	Poster in Technological Park in Koszalin	Disseminated during Koszalin Fair conference	poster on Gridpocket booth during Koszalin Fair	
@UOP	Post/tweets in social media	Dissemination in PatrasIQ event	Dissemination through POS4Work, a coworking space in Patras connected with multiple startups, SMEs, VCs etc.	Dissemination through other EU projects that UOP is participating.
@UU	Likes on LinkedIn for Open Call related posts.	Tweet/Retweets of Open Call related posts on Twitter.	Disseminated the Open Call through LinkedIn to several SMEs which provide security tools and/or provide penetration testing.	Likes on LinkedIn for Open Call related posts.
@SCYTL	Repost/retweet of original post			

3 Applications and Evaluation Process

3.1 Introduction

In this section, the application process for SMESEC Open Call and the evaluation process that took place for the applicants are described. In addition, after the selection process, SMESEC organised several meetings (face to face or online) with the selected parties to facilitate the process. The actions taken regarding these efforts are also described in this section.

3.2 Application Process

To invite and select SMEs, the SMESEC consortium had disseminated the opportunity to join the SMESEC projects as a third-party. The call described the aims of the project, what the consortium offered to the participants, the categories of SMEs sought for, the eligibility requirements, and the important dates.

Objectives:

- High-quality cybersecurity solutions attractive to SMEs with a restricted budget
- Provide cybersecurity training and awareness for SMEs and all type of employees
- Test and validate our solution with four initial use cases and have an open call when the solution is more mature

What SMESEC offered to the SMESES:

- Improving security and reducing the risk of cyber-attacks.
- Increasing security awareness for employees.
- Providing up to €20.000 of funds per participant.

To achieve a broad validation of all the features provided by the SMESEC framework, the consortium had defined three different categories:

- Category 1: 1 Red Team will assess the security level of the involved SMEs before and after the deployment of the SMESEC Framework. The applicants will be evaluated based on the proved experience in assessing systems for cyber-threat, their cybersecurity expertise and overall IT experience.
- Category 2a: up to 5 SMEs that will incorporate SMESEC framework taking advantage of all the features provided by SMESEC, e.g. threat protection and response tools, security awareness and training, testing and recommendation tools. As we are seeking for a diverse set of SMEs for this category, all applicants will be placed into three categories (high, medium, low) based on the expertise on IT and the adoption level of ICT to their day-to-day operations. Then 2 applicants will be selected from the high category, 2 from the medium category, and 1 from the low category.
- Category 2b: up to 3 SMEs from providing cybersecurity solutions that will test the external integration API, incorporating their solutions to the solutions of the SMESEC framework. We seek experienced SMEs with a strong background in cybersecurity.
- Category 3: 1 SME association, community, or ecosystem to help increase awareness on SMEs cybersecurity issues by using and validating the SMESEC framework. As the project provides a comprehensive framework of tools for cybersecurity, we look for feedback from a community of SMEs in particular on the tool's acceptance, on the overall approach chosen including usefulness and easiness to use the tools, etc. We look for applicants helping to organise

Document name:	D5.5 Open Call Design, Implementation and Results Report			Page:	18 of 115		
Reference:	D5.5	Dissemination:	PU	Version:	1.0	Status:	FINAL

collective actions and provide feedback about KPIs and SME practice improvements recommended by the SMESEC tools to improve our solutions. The applicants will be evaluated on the number of SMEs involved and on the potential impact of the SMESEC framework to increase SMEs' cybersecurity protection.

Eligibility requirements for participating SMEs:

- Proposals will only be accepted from parties that are eligible for participation in EC H2020-projects.
- All applying parties must be compatible with the EU definition of SMEs and must provide a signed 'Model Declaration Form' (application documents)
- All proposal must be submitted in the English language, strictly before the due date and through the SMESEC web portal by using specific proposal template (mandatory).
- Access to the proposal templates and application documents is available through the SMESEC website.
- Proposers' organisations can submit multiple proposals, but only one proposal per single organisation might be selected for funding in this Open Call.

Expected contributions, part of the eligibility requirements. All selected SMEs must:

- Participate actively in all workshops: two physicals in a country of the EU and two virtual meetings via teleconferencing.
- For category 2 applicants must have enough IT expertise and suitable infrastructure to support the full (cat. 2a) or partial (cat. 2b) deployment and validation of the SMESEC framework.
- The consortium will provide full technical support for the deployment and detailed guidelines for the evaluation reporting for each category.
- Deliver a final report, using the respective report template that will be provided by SMESEC, either for security findings (cat. 1), full validation (cat. 2a), integration process (cat. 2b) or provide feedback about KPIs and SME practice improvements (cat. 3) in due time and proper manner.
- Present their evaluation results to the consortium during the final physical workshop.

The important dates were as follows:



Figure 1. Important Open Call Dates

The advertisement of the Open Call and the achieved results of the campaign were described in detail in D6.3, Section 3.3.

Applications could be submitted by registering in the SMESEC framework. Upon registration, the participants received proposal templates and application documents.

3.3 Evaluation Process

Regarding the evaluation of the applicants, several criteria have been set for all applications and also per each application category (Category 1, 2a, 2b and 3). These criteria have been announced before the applications. The criteria set were divided into two types: Eligibility Criteria and Evaluation Criteria.

3.3.1 Eligibility Criteria

Table 2 Eligibility Criteria and their applicability to the categories.

Eligibility Criteria	Category
SME is eligible for participation in the EC Framework Programme H2020.	All
SME conforms to the SME definition used by the EC.	All
Single parties (no consortia are allowed).	All
Declaration by the applicant is in conformity with the supporting documents requested.	All
Being GDPR compliant.	All
Having the required technical infrastructure in place to deploy the SMESEC framework.	2a
Do you have a cybersecurity solution that fits in at least one the categories: detection, alerting, protection and response for network or host-based security incidents?	2b

If the examination of the application reveals that the applicant does not meet the eligibility criteria stated in the corresponding tables, the application would have been rejected on this sole basis.

The eligibility assessment was done by SMESEC project responsible partners.

The applications that pass the eligibility criteria were then subject to the evaluation process by the external evaluators.

3.3.2 Evaluation Criteria

The evaluation criteria were established and announced before the applications. 10 general evaluation criteria were established applicable to all categories. All evaluation criteria used in the evaluation process is presented in Table 3. In addition, in several internal meetings, SMESEC consortia members involved in Open Call task (5.5) have assigned weight factors for each evaluation criteria

Table 3 Evaluation Criteria and Their Applicability to the Categories

Evaluation Criteria	Category
Express your number of years of experience in IT security.	All
Ability to deploy SMESEC Framework in the live environment with the help of SMESEC partners (preferable).	All
Ability to deploy SMESEC Framework in test environment with the help of SMESEC partners.	All
The SME is part of a SME association that can provide feedback and participate in other SMESEC activities. (A letter of support from the SME association is preferable).	All
Total number of employees.	All
Having a person appointed as cybersecurity manager.	All
Number of IT technical staff and software developers.	All

Evolution of the SME in the last five years (prices, funding, rate of growth, etc.).	All
The number of years that the SME has been legally constituted for.	All
Describe how your participation in the Open Call will benefit SMESEC in terms of experience, technology.	All
Experience in assessing systems for cyber threats.	1
Express your number of years of experience in external software deployment and validation on premises servers.	2a
# of SMESEC features planned to be exploited with the SME.	2a
Having the required technical infrastructure in place to deploy the SMESEC framework.	2a
Typical types of assets used by the SME (e.g. Cloud Services, Databases, IoT sensors).	2a
Being experienced in with IT cybersecurity (Express your number of years of experience in IT security).	2b
Having a cybersecurity solution that fits in at least one the categories: detection, alerting, protection and response for network or host-based security incidents.	2b
The SME's product is able to provide security information (raw data, incident logs, events description) via an API.	2b
Having the required technical infrastructure in place to deploy the SMESEC framework.	2b
# of SMEs associated with the SME association.	3
# of events with member SMEs per year.	3
Potential impact of SMESEC to increase SMEs' cybersecurity protection.	3

3.3.3 Marking Guideline

In an online meeting with the external evaluators, the eligibility criteria, evaluation criteria and the evaluation process were presented. External evaluators were also provided with a guideline for giving their final evaluation marks for the applicants. This guideline is presented in Table 4.

Table 4 Marking Guideline for the Evaluation Process

Mark	Definition
0	The SME cannot be judged due to missing or incomplete information.
1 - 2 Very poor	Criterion is addressed in an unsatisfactory way.
3 - 4 Poor	There are serious weaknesses related to the criterion in question.
5 - 6 Fair	The criterion is addressed broadly, but there are important weaknesses that need to be corrected.
7 - 8 Good	The criterion is addressed well although several improvements are possible.
9 - 10 Excellent	All significant aspects of the criterion in question are addressed successfully. Any possible defect found is minor.

3.3.4 Calculating the Scores

The external evaluators were provided with an Excel file to facilitate their evaluation process. This excel file can be found in Annex IV.

The final score for every applicant for each evaluator was calculated using the following formula.

Calculate the total score for the general criteria

$$\sum_{general} mark * weight$$

Calculate the total score for the category specific criteria

$$\sum_{category\ specific} mark * weight$$

Calculate final score for the application

$$\sum_{final\ score} general\ total\ score + category\ specific\ score$$

3.3.5 Criteria for Profiling the Category 2a Applicants

Additional profiling was done for the category 2a applicants. Since SMESEC framework's target is all types of SMEs, we wanted to include high, medium and low-profile SMEs according to their evaluation results. To guarantee the diversity amongst the selected SMEs we applied the following profiling criteria given in Table 5.

Table 5 Criteria for Profiling for Category 2a Applications

Criteria	High	Medium	Low
Express your number of years of experience in IT security	>5	2-5	0-1
Express your number of years of experience in external software deployment and validation on premises servers.	>5	2-5	0-1
# of SMESEC features planned to be exploited with the SME.	5	3-4	1-2
Number of IT technical staff and software developers.	>5	2-5	0-1
Total number of employees.	101-250	26-100	0-25
The number of years that the SME has been legally constituted for.	>8	3-7	0-2

As we were seeking for a diverse set of SMEs for this category, all applicants were placed into one of the three categories (High, Medium, Low) based on the expertise on IT and the adoption level of ICT to their day-to-day operations. Then two applicants will be selected from the High and Medium category and 1 from the Low.

The following guideline in Table 6 were applied according to the answers given to the profiling criteria in Table 5.

Table 6 Guideline for Profiling Category 2a Applicants

Guideline	Final Profile
Number of High >= 3 and Medium <3 and Low <3	High

Number of Medium ≥ 3 and High < 3 and Low < 3	Medium
Number of Low ≥ 3 and High < 3 and Medium < 3	Low
Number of High = 3 and Medium = 3 and Low = 0	High
Number of Medium = 3 and Low = 3 and High = 0	Medium
Number of High = 3 and Low = 3 and Medium = 0	Medium
Number of High = Medium = Low = 2	Medium

The external evaluators applied the following procedure to assign the final profiles to the applicant SMEs.

For each category 2a applicant,

- Count the number of the criteria answered as High in Table 5,
- Count the number of the criteria answered as Medium in Table 5,
- Count the number of the criteria answered as Low in Table 5,

Apply the guideline in Table 6 to profile the SME as either High or Medium or Low.

3.4 Evaluation Committee

The role of the evaluation committee was to use the criteria and grading process, designed by the consortium and presented in section 3.3, in order to elicit the most fitting applicants. We asked the evaluators, expect from using the provided criteria, to focus on applicants that seem to exhibit the Ability and Professionalism to complete the validation of the framework. We aimed for diversity and coverage of the SMEs ecosystem as described in the evaluation criteria section.

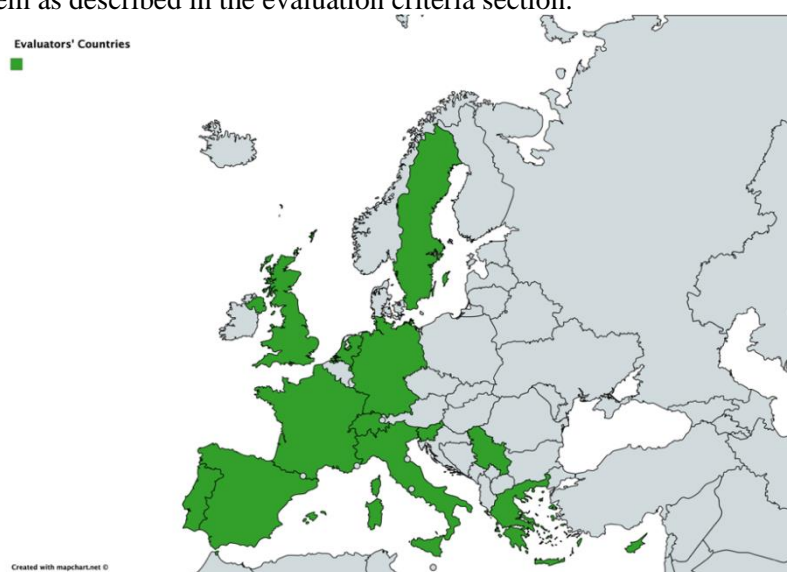


Figure 2. Evaluators(invited) Distribution among EU

For the external evaluation committee, we created a shared inside the consortium and asked all partners to suggest potential candidates for the Evaluation Committee. We invited all **Twenty-eight (28) proposed experts**. The distribution of the location of the experts in the EU can be found in Figure 1. Based on the time plan and the evaluation and their work engagement eleven (11) accepted to join the evaluation committee, seven (7) of them originated from Industry and four (4) of them, from Research Institutes/Academia. The profiles of the evaluators are depicted in Figure 3 and the Institute/Company

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	23 of 115
Reference:	D5.5	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

and country of origin of each member of the evaluation committee is presented in Table 7. The full details of the evaluators can be found in the appendix of D7.4[4]

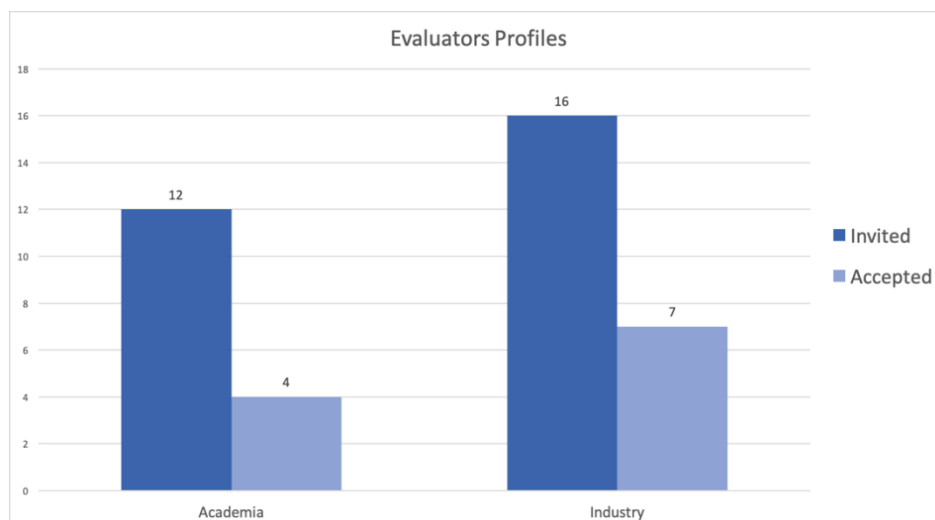


Figure 3. Evaluators' Profiles

Table 7. Institute/Company of each Committee Member

Institute/Company	Country
Freelancer working for CGI Germany	Germany
Blekinge Institute of Technology	Sweden
HP Italy	Italy
University of Novi Sad	Serbia
Harokopio University of Athens	Greece
SAP France	France
XLAB	Slovenia
SolentHub	UK
ThinkSilicon	Greece
Gradient	Spain
u. maastricht	Netherlands

We have held an Introductory meeting with the evaluators on the 9th of June 2019, where we described in depth the evaluation procedure and the scoring system of the applications. Also, we provided access to a shared folder of the consortium where we uploaded the Open Call applications, that fulfilled the eligibility criteria and all the reference material that would be used for the evaluation. We completely randomly distributed all the applications to the evaluators and asked for conflicts of interested, after receiving their input we did the appropriate changes and each application was evaluated by three evaluators.

Based on the scores from each evaluator we calculated an average score per application/per category. Based on this score we held a final consensus meeting, on the 16th of June 2019, finalizing the list of the selected SMEs. The results we received during that consensus meeting are presented in the next section 3.5 From that point on consortium started contacting the selected SMEs and the validation procedure (stage 2) of the framework in the context of the Open Call had begun.

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	24 of 115
Reference:	D5.5	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

3.5 Evaluation Results (@FORTH)

In this section, we present the received applications and the results as proposed by the evaluation committee and agreed upon within the consortium. The data presented in the following section are sanitized and only personal information we have received approval are disclosed. The full information of the application evaluation results can be found in the appendix of Deliverable 7.4.

Twelve distinct application were received during the Open Call and the countries of origins for the SMEs that applied are presented in Table 8.

Table 8. Open call applicants' origin country per category

Category	Country
Cat 1	France
Cat 2a	France, Greece (2), United Kingdom, Italy (2)
Cat 2b	United Kingdom (2), France, Spain
Cat 3	Denmark

The Consortium held two meetings with the committee to explain the evaluation goals, the process, to appoint, each one of the received applications, to three evaluators and a final consensus meeting for the final selection of the SMEs to be funded and participate in the evaluation of the SMESEC Framework. The final results from the review process are depicted in Table 9:

Table 9. Reviewers' final scores

Application ID	Reviewer 1 Score	Reviewer 2 Score	Reviewer 3 Score	Average	Result
Cat1: Montimage	333	328	363	341,3	ACCEPT
Cat2a: AESSE.NET	357	309	320	328,7	ACCEPT
Cat2a: BLACBOXSECU	275	369	243	295,7	ACCEPT
Cat2a: CareAcross	322	328	291	313,7	ACCEPT
Cat2a: Fraud Line	408	290	339	345,7	ACCEPT
Cat2a: ITML	321	353	237	303,7	ACCEPT
Cat2a: -----	270	227	219	238,7	REJECT
Cat2b: AEGIS	458	460	350	422,7	ACCEPT
Cat2b: RKL	443	328	401	390,7	ACCEPT
Cat2b: AfterTech	189	447	288	308,0	ACCEPT
Cat3: It-forum	308	303	278	296,3	ACCEPT

Out of the **twelve (12) received applications**, **eleven (11)** were evaluated as one SME, Montimage, initially had applied for two categories (categories cat1and cat2b), but at a later point withdrew its application for category 2b.

The SMESEC consortium accepted the evaluation results and funded the SMEs presented in Table 9. Additionally, based on the Grant Agreement of SMESEC (contract no740787), the costs for the evaluation from the SMEs, along with all the required procedures for payment of the SMEs will be realized by two Consortium Partners, namely Foundation for Research and Technology Hellas (FORTH) and University of Utrecht (UU). Based on GA of SMESEC (contract no 740787), four SMEs will be paid by FORTH and six from UU. The appointment to of each application to the responsible partner for the payment, is also presented in Table 10.

Table 10. Accepted SMEs to be funded by SMESEC

Selected SME/Assoc	Category	Country	Maximum Budget	Payment By
Montimage	Cat 1	FR	20.000€	UU
BLACKBOXSECU	Cat 2a	FR	15.000€	UU
ITML	Cat 2a	GR	15.000€	FORTH
CareAcross	Cat 2a	UK	15.000€	UU
AESSE.NET	Cat 2a	IT	15.000€	UU
Fraud Line	Cat 2a	GR	15.000€	FORTH
AfterTech	Cat 2b	UK	12.000€	FORTH
AEGIS	Cat 2b	UK	12.000€	FORTH
RKL	Cat 2b	ES	12.000€	UU
IT-Forum	Cat 3	DK	7.000€	UU

3.6 Summary of Execution Plan

In this section, we present the whole execution plan of the Open Call without including the evaluation process details as it was thoroughly described in the previous sections. We will focus on the actions that took place for the materialization of the open call. We provide a summary of the actions and more information can be found in the respective sections.

The overall plan is depicted in Table 11

Table 11. Open Call Execution Plan

Actions	Initial Plan	Actual date	Details
Inform the selected SMEs	Jun' 19	7-Jun-19	After the selection procedure, all SMEs were contacted with an official letter from the SMESEC consortium and we received a signed later of acceptance from each external partner.

1st Online meeting with the SMEs	Jul'19	16-Jul-19	Preparatory meeting with the SMEs provided all information, tools and plan for the Open Call.
Creation of a technical Mailing list	Jul'19	18-Jul-2019	A technical mailing list for realization of the Open Call was created and all involved parties were added to it.
Installation guides / training material tools /testing scenarios	Jul'19	Jul'19	All tool owners provided instructions and installation guides for their tools through the smesec.eu platform
Provide tools to the SMEs	Jul'19	Jul'19	The tools were made available through smesec.eu and all SMEs had access to them after successfully registering to the web site
Amendment II	-	Jul'19	An amendment was submitted and accepted in order to distribute the funds between FORTH and UU that were responsible for funding the SMEs that participated in the Open Call.
Template Contracts for each Category	Aug'19	Sep'19	FORTH and UU created the templates for the contracts to be signed by each SME in the Open Call. Moreover specific technical tasks, required for the completion of the undertaken work, were described in the technical annex of the contracts, with the help of all partners involved.
Integration with SMEs	Jul'19 Oct'19	Sept'19 Nov'19	The whole integration phase was divided to integration of cat 2a, cat2b with different dates for each of the categories.
Progress tracking meeting and shared files	Sept'19 Jan'20	Bi-Weekly	All external SMEs were invited to participate in the Consortium's pre-existing Bi-weekly meetings for the Open Call so to discuss and resolve any integration issues. Also, unofficial progress tracking files were created and shared with the participants.
Planning & Integration 2a	Jul'19	Sept'19 Nov'19	The integration phase was originally planned to last for two weeks but it varied greatly from SME to SME spanning until the start of M30
1st Physical Meeting	Sept'19	9-Sept-19	The first physical meeting took place on the 9 th and 10 th of September 2019, in Heraklion, Greece. A detailed discussion on the SMESEC's Technical details took place. The first integration issues were addressed for Category 2a. The first specification for the category 2b was presented and remarks on how the external tools to be integrated to the SMESEC framework were extensively discussed. Finally, the plan of the red team was presented and agreed upon with the consortium
Provide API specification	Sept'19	9-Sept-19	The specification of the external API was discussed during the 1 st physical meeting with the SMEs. The final version of the API was delivered in Oct-19.
Category 1 planning	Sept'19	10-Sept-19	The Red Team presented during the physical meeting the initial plan for the penetration testing of the SMESEC platform and the SMEs involved in this category validation activities.
Run the provided test	Sept'19 Oct'19	Sept'19 Jan'19	A list of tests based on the evaluation process and tests that were created during task 5.1. This list was shared with the Open Call SMEs and based on the solutions applicable to their case. The run of the tests lasted longer than based on the availability and the provided timeslots of some of the

			pilots as well as the adaptations made to SMESEC tools to be compatible with the SMEs environments.
Use the platform to their day-to-day business	Sep'19 – Nov'19	Sept'19 – Jan'20	After the integration process was successfully concluded to the external SMEs they had the chance to use the system to their day to day activities. Initially it was planned to provide free access to the system until the end of planned testing period, but we decided to extend this period until the end of the Open Call activities.
Provide reporting template and guidelines	Oct'19	31-Oct-2019	The reporting templates were created and shared with the Open Call participants as Planned. We also devoted the next bi-weekly telco to provide a walk-through and specific guideline to the SMES. As the reports of Category 1 and Category 3 were not in the same format of
Integration and testing of Cat2b (external API)	Oct'19- Nov'19	Nov'19 – Jan'20	The first version of the external API was released on Oct'19 and the final version was released on Nov'19 and was used for the integration and testing of the Open Call. A final release that will accommodate changes based on the comments received during this process will be released publicly in May'20 in github.
Category 1 testing	Oct'19- Nov'19	Nov'19 – Jan'20	The penetration testing started and the largest part of it was concluded in Nov'19. The original plan was executed as discussed and even more tests were conducted against specific parts of the Platform e.g. the Training Service. Both the framework and the e-voting pilot were examined and valuable information was extracted from the process.
Reports finalisation and delivery	Dec'19	Dec'19 – Jan'19	All final reports were delivered before our deadline 31-Jan-20. The initial versions of the reports were delivered earlier, but at some cases the consortium requested additional input or clarifications resulting to the final version of the reports.
Open call process and reporting conclusion	Jan'19	4-Feb-20	All the reports and the takeaways of the Open Call process were presented during our final physical meeting with the SMEs in Netherlands. There the results of the Open Call process were presented to the consortium and all reports were accepted.
Provide input to other tasks	Feb'20- Mar'20	Dec'19 – Apr'20	As we held bi-weekly tele-conferences and had all the necessary collaboration tools (e.g. mailing lists, shared areas) in place the feedback to the consortium and the input to the related tasks was a continuous process spanning from the start of the integrations until the finalisation of the Open Call process. All tool providers were actively updating their tools based on the feedback of the integration process and the evaluation experiments.
Deliverable writing, Q&A, Submission	Apr'20- May'20	Mar'20 – Apr'20	The final phase of Task 5.5 was the writing of this deliverable. This started after we have received all the reports and had had the final meeting with the Open Call reporting all the activities that took place for the materialisation of the SMESEC Open Call.

4 Open Call Results

In order to create a solid evaluation strategy, we derived the five pillars based on the objectives of the project on which the evaluation was built upon. The five pillars defined are:

- (i) Detection & Alerting
- (ii) Protection & Response
- (iii) Training Courses & Material
- (iv) Capability & Awareness
- (v) Lessons Learnt

Complementary to this to these five pillars all participants filled in a questionnaire about the market acceptance of SMESEC proposition and the proposed business plan. Results from these questionnaires can be found in respective section in D5.5. and in D5.4[3]

4.1 “Category 1. Red Team”—Technical Results and Findings

4.1.1 Security Findings

This section contains information that can be used for malicious purposes against the SMESEC framework or the pilots so it has been moved to D3.9[5] that is not a public deliverable.

4.1.2 SMESEC Recommendations

The report provided in category 1 did not find any major issues regarding the SMESEC Framework, as can be seen in the Annex section of D7.4[4] since it contains private information that cannot be presented in this public deliverable.. Most of the findings, however, were fixed in subsequent releases, and were documented in deliverable 3.7.

Beside the framework, also the Scytl application and the Training Platform were audited.

For Scytl’s application, no issues were reported. This was justified because Scytl’s application was heavily audited before for security vulnerabilities, resulting in a properly secured application.

However, major vulnerabilities were discovered in the training platform, that allowed possible attackers to completely take over the system. These findings lead to an extensive revise of the training platform, solving all the critical security vulnerabilities. Another audit, performed after the open call, demonstrated the work done in this area. More information on this can be found in 4.5 and in deliverable D3.7.

4.2 “Category 2a: Full Integration and testing” Technical Results

4.2.1 Provided Tests

Table 12 summarizes the full list of tests that was provided to the SMEs and were used for the evaluation of the SMESEC framework. The complete list of the tests was defined in the task T5.1 to evaluate the components integrated in the SMESEC framework.

Document name:	D5.5 Open Call Design, Implementation and Results Report			Page:	29 of 115
Reference:	D5.5	Dissemination:	PU	Version:	1.0
				Status:	FINAL

Table 12. List of tests for the Open Call evaluation process

Test-Codes	I/ J	Provider	Description
IT_01_XL-SIEM	Individual	ATOS	General test of relevant alerts
IT_01_2_XL-SIEM	Individual	ATOS	Test of test plugin
IT_01_3_XL-SIEM	Individual	ATOS	Test of SSH plugin
IT_01_4_XL-SIEM	Individual	ATOS	Test of FORTH EWIS plugin
IT_01_5_XL-SIEM	Individual	ATOS	Test of ADC plugin
IT_02_1_GravityZone	Individual	Bitdefender	Malware detection in clients and servers, deployment and detection of test malware, alerts in relation to detected malware send and represented in GravityZone
IT_02_2_GravityZone	Individual	Bitdefender	Detection of downloaded malware
IT_02_3_GravityZone	Individual	Bitdefender	Accessing a blacklisted URL
IT_02_4_GravityZone	Individual	Bitdefender	Inserting an USB stick with a malicious file
IT_02_5_GravityZone	Individual	Bitdefender	Detection of port scanning
IT_03_1_Honeypot	Individual	FORTH	Detection of DDoS attack
IT_03_2_Honeypot	Individual	FORTH	Detection of SQL-Injection attack
IT_03_3_Honeypot	Individual	FORTH	Detection of brute force attacks
IT_04_1_AntiROP	Individual	IBM	Validate that antiROP unique copies do not change executable functionality
IT_04_2_AntiROP	Individual	IBM	Validate that antiROP unique copies defend against ROP attack
IT_05_1_TaaS	Individual	EGM	Lora testing
IT_05_2_TaaS	Individual	EGM	API testing
IT_05_3_TaaS	Individual	EGM	Check if user is authorized to access the TaaS platform
IT_05_4_TaaS	Individual	EGM	Show all reports
IT_06_CITRIX-ADC	Individual	CITRIX	Detects malicious or improper network traffic and blocks it before reaching the backend application servers, potentially causing service downtime. stops it
IT_07_1_IDS	Individual	FORTH	Scanning detection
IT_07_2_IDS	Individual	FORTH	DDoS attack detection
IT_08_1_Virtual_Patching	Individual	IBM	Validate that the predictive model provides reasonable FPR/TPR rates on input-samples
IT_08_2_Virtual_Patching	Individual	IBM	Validate that the Integration into custom log file analysis produces the same results as in T_08_01_Virtual_Patching
IT_09_1_CYSEC	Individual	FHNW	Validation of the installation and login functionality of the CYSEC tool

IT_09_2_CYSEC	Individual	FHNW	Validation of the on boarding, assessment, learning, control and practice implementation, reporting, and recommendation functionalities of the CYSEC tool
IT_09_3_CYSEC	Individual	FHNW	Validation of CYSEC coaches
IT_09_4_CYSEC	Individual	FHNW	Validation of the insight stream functionality of the CYSEC tool
IT_10_1_ExpliSAT	Individual	IBM	Validate that testing platform does not produce false alerts
IT_10_2_ExpliSAT	Individual	IBM	Validate that testing platform covers common vulnerability families
JT_01_XL-SIEM_GravityZone	Joint	ATOS & Bitdefender	Malware detection, reporting on the XL-SIEM system and alerts rising
JT_02_XL-SIEM_Honeypot	Joint	ATOS & FORTH	Possible attacks on the honeypot reported on the XL-SIEM system
JT_03_CITRIX-ADC_Honeypot_XL-SIEM	Joint	CITRIX & FORTH & ATOS	Citrix ADC is deployed in front of an application server and intercepts all inbound traffic. Traffic is inspected based on predefined policies and discarded if found inappropriate. Inappropriate traffic is forwarded to the Honeypot while generic reports are issued to the XL-SIEM.
JT_04_XL-SIEM_IDS_Honeypot	Joint	ATOS & FORTH	The Cloud-IDS and Honeypot detect a DoS attack and reports the XL-SIEM about it

4.2.2 Summary of tests for Category 2a

In this section we provide a matrix of all the tests run by each SME, based on their infrastructure and the assets they wanted to protect, along with a mark denoting whether this test was successful(✓), partially successful(✓-) or dropped/failed(✗). Each SME selected a different flavour of the SMESEC platform that was suited for its case. In order to get better feedback and improve all aspects of SMESEC, the provided tests' granularity was based on each tool present in the SMESEC framework. The tests were either designed to be either individual or joint between different tools.

The following sections (4.2.3-4.2.7) include the detailed technical information on the evaluation trials as reported by the external SMEs in their submitted reports. The full reports can be found in the Annex of D7.4 for the sake of keeping personal information confidential. As depicted in Table 13, the majority of the tests were successful, proving the successful integration with the external SMEs. There was one test, IT_02_3_GravityZone, that failed for a specific SME participant namely ITML, but this functionality "URL-blacklisting" is not possible on Linux OS as Bitdefender is not offering a Content Control component for Linux OS. The malicious file can be downloaded but cannot be executed locally. Additionally, another test IT_06_CITRIX-ADC was dropped for Fraudline, as their network topology as deployed in their cloud infrastructure, had certain limitations which rendered the combination of Citrix ADC and ADC Aggregator nodes not functional. Several iterations were conducted with numerous reconfiguration attempts, however radical redesign was necessary to ensure seamless operation. Finally, some tests were marked as partial successes mostly because the SMEs running the tests did not have the expertise to interpret the results as successful or not.

Table 13. Category 2a Tests' Summary

Test-Codes	Provider	BLACK SECU	CareAcr oss	AESSE .NET	ITML	FRAU DLINE
IT_01_XL-SIEM	ATOS	✓	✓	✓	✓	✓
IT_01_2_XL-SIEM	ATOS	✓			✓	✓
IT_01_3_XL-SIEM	ATOS	✓			✓	✓
IT_01_4_XL-SIEM	ATOS	✓		✓		✓-
IT_01_5_XL-SIEM	ATOS	✓				✓-
IT_02_1_GravityZone	Bitdefende r	✓		✓	✓	
IT_02_2_GravityZone	Bitdefende r	✓		✓	✓	
IT_02_3_GravityZone	Bitdefende r	✓		✓	X	
IT_02_4_GravityZone	Bitdefende r	✓		✓		
IT_02_5_GravityZone	Bitdefende r	✓		✓	✓	
IT_03_1_Honeypot	FORTH	✓			✓	✓
IT_03_2_Honeypot	FORTH					✓
IT_03_3_Honeypot	FORTH	✓			✓	✓
IT_05_2_TaaS	EGM		✓-			
IT_05_3_TaaS	EGM		✓			
IT_05_4_TaaS	EGM		✓			
IT_06_CITRIX-ADC	CITRIX					X
IT_09_1_CYSEC	FHNW	✓	✓			
IT_09_2_CYSEC	FHNW	✓	✓			
IT_09_3_CYSEC	FHNW	✓	✓			
IT_09_4_CYSEC	FHNW	✓	✓			
JT_01_XL-SIEM_GravityZone	ATOS & Bitdefende r	✓		✓		
JT_02_XL-SIEM_Honeypot	ATOS & FORTH	✓				
JT_03_CITRIX-ADC_Honeypot_XL-SIEM	CITRIX & FORTH & ATOS					

JT_04_XL-SIEM_IDS_Honeypot	ATOS & FORTH	✓				
-----------------------------------	--------------	---	--	--	--	--

4.2.3 BLACKBOXSECU

Based on the tools that BLACKBOXSECU has installed in its premises a subset of these tests were used for the evaluation of the technical aspects of the detection and response pillars of the SMESEC framework.

Table 14. List of tests executed from BLACKBOXSECU

Test-Codes	Description	Success	Date	Remarks / Execution details
IT_01_XL-SIEM	General test of relevant alerts	✓	10/09/2019	
IT_01_2_XL-SIEM	Test of test plugin	✓	29/10/2019	
IT_01_3_XL-SIEM	Test of SSH plugin	✓	29/10/2019	
IT_01_4_XL-SIEM	Test of FORTH EWIS plugin	✓	29/10/2019	
IT_01_5_XL-SIEM	Test of ADC plugin	✓	29/10/2019	
IT_02_1_GravityZone	Malware detection in clients and servers, deployment and detection of test malware, alerts in relation to detected malware send and represented in GravityZone	✓	19/11/2019	
IT_02_2_GravityZone	Detection of downloaded malware	✓	19/11/2019	(2)
IT_02_3_GravityZone	Accessing a blacklisted URL	✓	19/11/2019	(3)
IT_02_4_GravityZone	Inserting an USB stick with a malicious file	✓	19/11/2019	(4)
IT_02_5_GravityZone	Detection of port scanning	✓	19/11/2019	(5)
IT_03_1_Honeypot	Detection of DDoS attack	✓	29/10/2019	
IT_03_3_Honeypot	Detection of brute force attacks	✓	29/10/2019	
IT_09_1_CYSEC	Validation of the installation and login functionality of the CYSEC tool	✓	17/01/2020	(6)

IT_09_2_CYSEC	Validation of the on boarding, assessment, learning, control and practice implementation, reporting, and recommendation functionalities of the CYSEC tool	✓	17/01/2020	(6)
IT_09_3_CYSEC	Validation of CYSEC coaches	✓	12/12/2019	
IT_09_4_CYSEC	Validation of the insight stream functionality of the CYSEC tool	✓	12/12/2019	
JT_01_XL-SIEM_GravityZone	Malware detection, reporting on the XL-SIEM system and alerts rising	✓	19/11/2019	(1)
JT_02_XL-SIEM_HoneyPot	Possible attacks on the honeypot reported on the XL-SIEM system	✓	19/11/2019	
JT_04_XL-SIEM_IDS_HoneyPot	The Cloud-IDS and HoneyPot detect a DoS attack and reports the XL-SIEM about it	✓	19/11/2019	

Remarks

- (1) *Ok for Windows OS but problems with Linux OS were observed. At the beginning this test failed due to lack of reporting events to the XL-SIEM. This was an issue related to the package creation. The “epag” service was trying to reach the “smesec.bitdefender.com” on the internal ip address: 192.x.x.x. This was however not reachable as the Bitdefender’s GravityZone server is placed in AWS and therefore the correct address was: 34.x.x.x.*

On the Linux side, BitDefender team has provided initially a wrong location for the agent. It would have to be in “/opt/bitdefender/etc/epag.js” The problems were resolved by the BitDefender team in our package.

- (2) *Initially this test failed due to the following reasons:
 #1: The event was not detected by the Dashboard of our company:
 #2: The infected file could be downloaded under Linux (Ubuntu 16.04) (the machine had Bit Defender installed as shown at the screenshot below).*

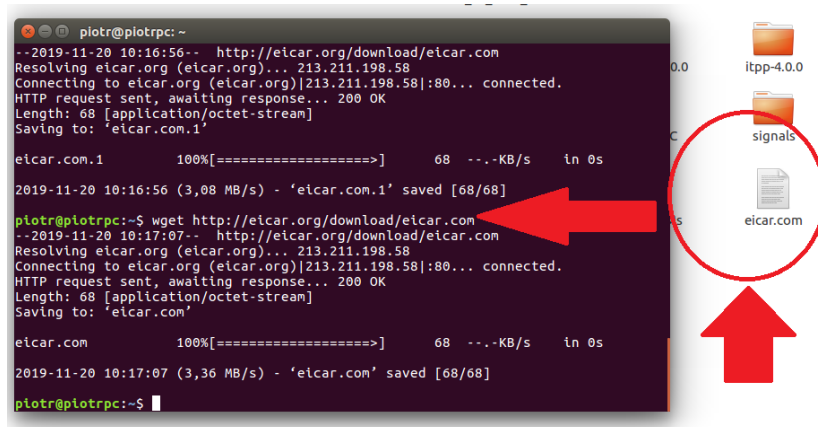


Figure 4. Screenshot of test results for malware downloading process on a Linux OS (Ubuntu 16.04) laptop with installed BitDefender “end-point” protection

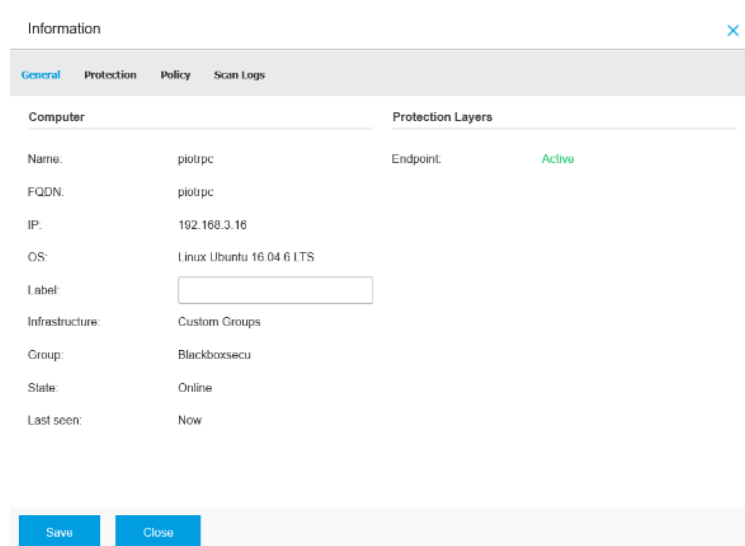


Figure 5. Screenshot of BitDefender dashboard correctly identifying the Linux test laptop with installed BitDefender “end-point” protection

According to BitDefender, this is a correct behaviour, because there is no “Content Control” feature for Linux, there so “no way to do URL filtering and ant phishing within the Linux OS”.

(3) *Ok for Windows OS but problems with Linux OS. Initially this test failed due to the following reasons for Linux machine:*

#1: The event was not detected by the Dashboard of our company

#2: Blacklisted URL could be accessed from Linux “end-point” machine (Ubuntu 16.04) or we could download the malware from USB stick (the machine has BitDefender installed as shown at the screenshot below).

According to BitDefender, this is a correct behaviour, because there is no “Conent Control” feature for Linux, there is “no way to do url filtering and antiphishing within the Linux OS”.

Also, according to BitDefender some requirements for using on-access scanning with DazukoFS are needed:

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	35 of 115
Reference:	D5.5	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

“For DazukoFS and on-access scanning to work together, a series of conditions must be met. The SELinux policy must be either disabled or set to permissive. To check and adjust the SELinux policy setting, edit the /etc/selinux/config file.”

- (4) *Ok for Windows OS but problem with Linux OS seen. Initially this test failed due to the following reasons for Linux machines:*
- #1: The event was not detected by Dashboard of our company*
 - #2: Malware file could be downloaded from USB stick on the “end-point” Linux machine (Ubuntu 16.04). Worked well for Windows 10 (Please see the screenshot below):*

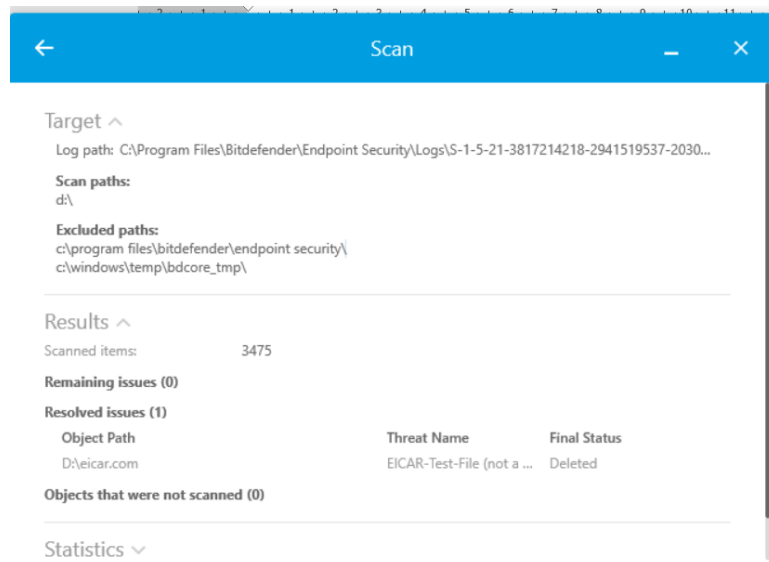


Figure 6. Screenshot of BitDefender “end-point” scanning action on Windows 10 machine

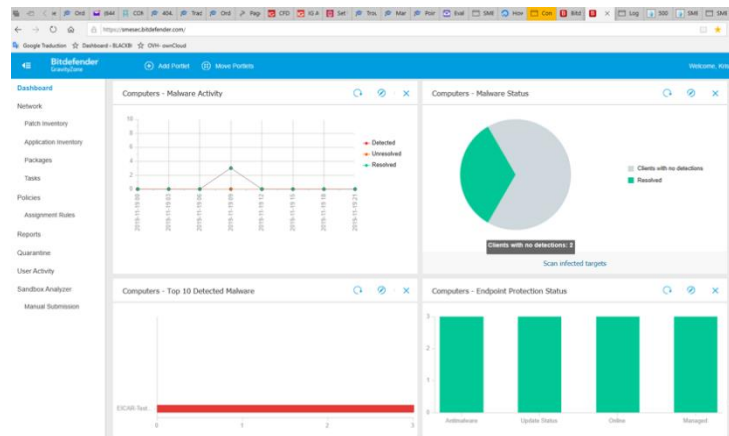


Figure 7. Screenshot #1 of BitDefender (GravityZone) dashboard and threat detection on a Windows 10 machine

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	36 of 115
Reference:	D5.5	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

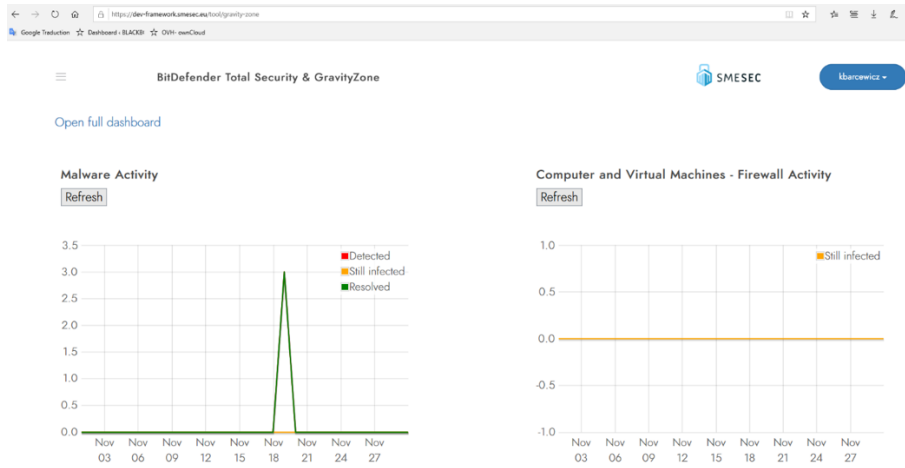


Figure 8. Screenshot #2 of BitDefender (GravityZone) dashboard and threat detection and correction on a Windows 10 machine

According to BitDefender, this is a correct behaviour, because there is no “Content Control” feature for Linux, so there is “no way to do URL filtering and ant phishing within the Linux OS”.

- (5) Initially this test failed for the following reasons:
 - The attack detection was not reported in the XL-SIEM dashboard
 (The port scanning attack was detected, and the detection was reported in the GravityZone dashboard)

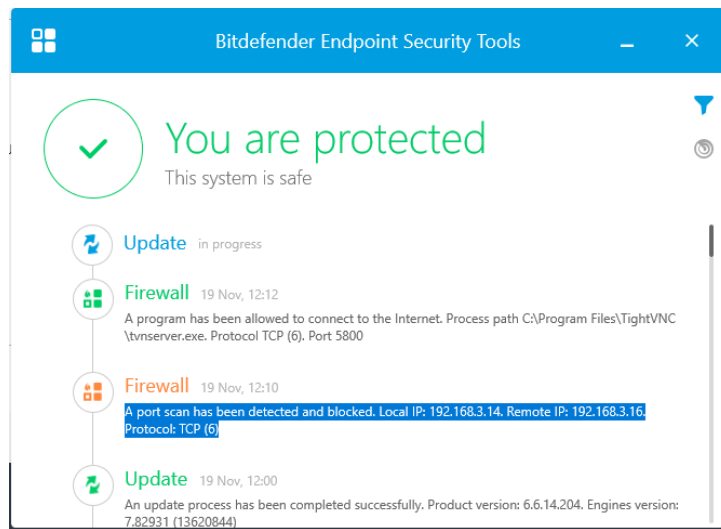


Figure 9. Screenshot #1 of BitDefender scan status on a Windows 10 machine and detection of attacker’s address

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	37 of 115
Reference:	D5.5	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

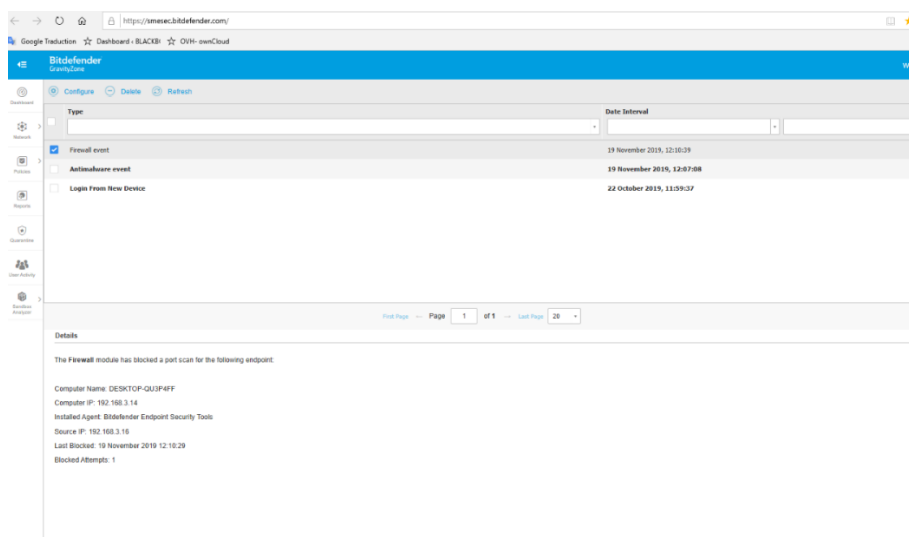


Figure 10. Screenshot #2 of BitDefender (GravityZone) dashboard with scan status of “end-point” test machines (Windows 10) and detection of attacker’s address

The reporting problem in XL-SIEM was corrected by ATOS team after signalling the issue.

(6) Some CySEC Dashboard access problems faced that prevented us to perform recommended coaches. Problems were fixed by the FHNW team. See below:



Figure 11. Screenshot of CySEC dashboard showing an issue to connect to the system

4.2.4 CareAcross

Based on the tools that CareAcross has installed in its premises a subset of these tests will be used for the evaluation of SMESEC.

Table 15. List of tests executed from CareAcross

Test-Codes	Description	Success	Date	Remarks / Execution details
IT_01_XL-SIEM	General test of relevant alerts	✓	January 2020	(1)
IT_05_2_TaaS	API testing	Partial	December 2019	(2)

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	38 of 115
Reference:	D5.5	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

IT_05_3_TaaS	Check if user is authorized to access the TaaS platform	✓	September-December 2019	(3)
IT_05_4_TaaS	Show all reports	✓	September-December 2019	(4)
IT_09_1_CYSEC	Validation of the installation and login functionality of the CYSEC tool	✓	September-December 2019	(5)
IT_09_2_CYSEC	Validation of the on boarding, assessment, learning, control and practice implementation, reporting, and recommendation functionalities of the CYSEC tool	✓	September-December 2019	(6)
IT_09_3_CYSEC	Validation of CYSEC coaches	✓	September-December 2019	(7)
IT_09_4_CYSEC	Validation of the insight stream functionality of the CYSEC tool	✓	September-December 2019	(8)

Remarks

1. Rationale:

This is the fundamental tool provided the within the SMESEC framework. Since the other tools selected were not directly integrating with the XL-SIEM tool, this is the only relevant and applicable test done for this tool.

Execution Details:

Many attempts were made to install the XL-SIEM agent in the same environment/system/virtual machine that hosts our application (Heroku). However, this was proven not possible, because of the following reasons:

- i. Installing non-default app packages is not supported on Heroku*
- ii. Heroku does not support sudo*
- iii. Modifying system files is not possible*
- iv. The Heroku infrastructure does not allow to open up ports.*

Therefore, we opted to use alternative cloud providers, and with the Consortium's help we identified Amazon EC2 as a viable option. Once this was identified, the initial setup was relatively smooth. However, storage/capacity problems prevented the installation to be completed, and the general test to be performed.

Comments:

The principles of the XL-SIEM offering are very relevant and important. Its functionality would be a welcome addition to a DevOps team. However, the realities of cloud infrastructure come with the following "side-effects":

- i. Each cloud service provider has its own approach regarding the architecture, its openness, access, etc. Consequently, custom toolkits may not be available everywhere.*

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	39 of 115
Reference:	D5.5	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

- ii. *Teams and DevOps leaders are accustomed to light-touch, single-click, fast provisioning of modules or services. Consequently, and despite their experience with high-touch multi-step components, they tend to favour processes that are simpler to execute and maintain.*
- iii. *Despite the openness of the cloud platforms overall, it is inevitable that the tools built, procured, brokered, or otherwise made available in these ecosystems are very specific and relatively limited (hence making them somewhat closed, in some critics' eyes). Consequently, other tools are disadvantage by incompatibilities and limited availability of community and corresponding knowledge.*

The above are even more pronounced and important among startup companies or small enterprises, which favour speed, agility, community over custom implementations, no matter how high quality.

2. Rationale:

Our web applications make this test suite quite applicable.

Execution Details:

With the help of the Consortium, we received the necessary details to set up and access the tool, and perform the corresponding testing.

The testing itself was straightforward, but the presented results of the testing were not always clear. Some tests would have a "Test Verdict: PASS" despite an error message of "Please check your API: Entry point not available"; similarly, tests with wrong/invalid METHOD would also pass; and in some cases the Test Results page would appear blank.

Comments:

The tool is useful, but not easy to use, and inconsistent. This is mostly due to some issues with the UI/UX and not necessarily with the underlying functionality. However, given the increasing competition from similar test suites, it faces an uphill battle. Perhaps the Lora testing is more consistent and thus offers a competitive advantage, being a less contested space.

3. Rationale:

Fundamental test case for a web-based tool.

Execution Details:

The online access to this tool was established without much trouble (although the tool was unavailable at times).

Comments: *Straightforward test.*

4. Rationale:

This is an applicable test for such a web-enabled API testing tool, since it is very likely that the testing needs of an organisation will comprise multiple such individual tests.

Execution Details:

The "Test Reports" page was loaded without problems. It would accurately display the results of the previously conducted tests.

Comments:

This is a useful page but can be improved. For example, additional metadata (e.g. test details) or functionality (e.g. re-running of tests) would be welcome.

5. Rationale:

A fundamental test.

Execution Details:

There were some periodic issues with accessing the tool.

Comments:

Useful tool but in some cases not tailored to SMEs.

6. Rationale:

Document name:	D5.5 Open Call Design, Implementation and Results Report			Page:	40 of 115	
Reference:	D5.5	Dissemination:	PU	Version:	1.0	Status: FINAL

Fundamental test

Execution Details:

Although it was not clear what was to be expected, the execution was relatively smooth.

Comments:

There were some very valid points in the learning objectives. However, they were not always tailored to the needs, capabilities and priorities of SMEs. It may be useful to provide a qualitative analysis of the priorities and their corresponding impact.

7. Rationale:

Useful concept as it connotes some level of tailoring.

Execution Details:

Was done throughout the CYSEC process.

Comments:

While there were elements of coaching, the context was not clear and felt more instantaneous as opposed to longitudinal. It may be a matter of naming, more than anything else.

8. Rationale:

Useful concept.

Execution Details:

Was done throughout the CYSEC process.

Comments:

The insights were mostly interesting, although not necessarily useful. The nature of the service, of course, will inevitably “suffer” from the limitations of the underlying insights, which is perfectly understandable. It would be very useful to tailor the stream across multiple parameters. This way, it would not feel as if it compounds the information overload and the attention-grabbing nature of many such passive tools.

4.2.5 AESSE.NET

Based on the tools that AESSENET has installed in its premises a subset of these tests will be used for the evaluation of SMESEC.

Table 16. List of tests executed from AESSE.NET

Test-Codes	Description	Success	Date	Remarks / Execution details
IT_01_1_XL-SIEM	Test whether the XL-SIEM agent is well connected to the XL-SIEM server	✓	November, December 2019	Aesse tested the connection between XL-SIEM agent installed in house and the XL-SIEM server. Snapshot of XL-SIEM dashboard is enclosed below (Image 4.2.4.1) Image 4.2.4.3 shows Syslog file (two pages) that reports communication among different agents and servers
IT_01_4_XL-SIEM	Test whether the Gravity Zone plugin is well configured	✓	November, December 2019	Logger program has been used to generally test the connection. Image 4.2.4.2 enclosed below The BD events are shown in the dashboard panel of XL-SIEM on line server. Image 4.2.4.5 and 4.2.4.6

IT_02_1 _Gravity Zone	Detect the presence of malware within one of the protected hosts. Provide appropriate reaction to the attack, send alert to GravityZone	✓	November, December 2019	BD works on all the testing environments. Snapshot is enclosed. (Image 4.2.4.4, 4.2.4.5)
IT_02_2 _Gravity Zone	Test if the endpoints are protected from malware downloaded from the Internet.	✓	November, December 2019	BD works on all the testing environments. Snapshot is enclosed. (image 4.2.4.4)
IT_02_3 _Gravity Zone	Test if Bitdefender prevents the protected endpoints from accessing blacklisted URLs.	✓	November, December 2019	BD works on all the testing environments.
IT_02_4 _Gravity Zone	Test if the endpoints are protected from malware distributed through USB drives.	✓	November, December 2019	USB drivers with malware are blocked directly by Operating Systems malware protections. We had to simulate the attack.
IT_02_5 _Gravity Zone	Test if port scanning attacks are detected by Bitdefender	✓	November, December 2019	
JT_01_ XL- SIEM_G ravityZo ne	Malware detection, reporting on the XL-SIEM system and alerts rising	✓	November, December 2019	It has been the most expected result (Image 4.2.4.6), we did many tests seeing the results in the syslog file without seeing them in the dashboard of XL-SIEM, at the end the system was configured in the correct way.

Remarks

The following Images 4.2.4.6 show the events reported, in particular image 4.2.4.1 shows the local BitDefender agent, the image 4.2.4.4 shows the BitDefender agent and the XL-SIEM panel reporting the events the image 4.2.4.6 the XL-SIEM dashboard.

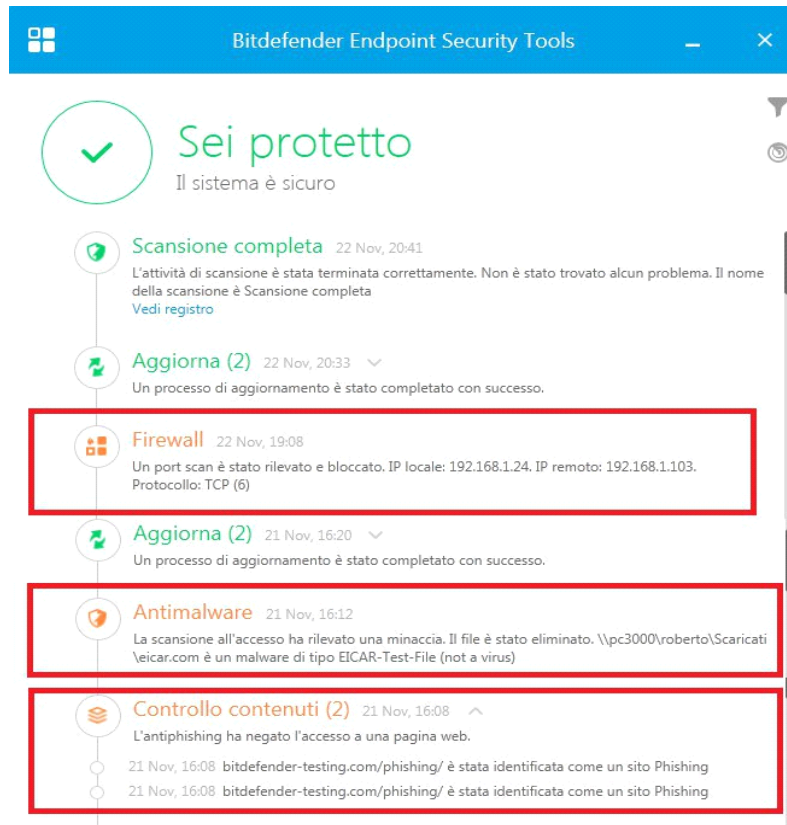


Figure 12. Firewall-Malware- Phishing test

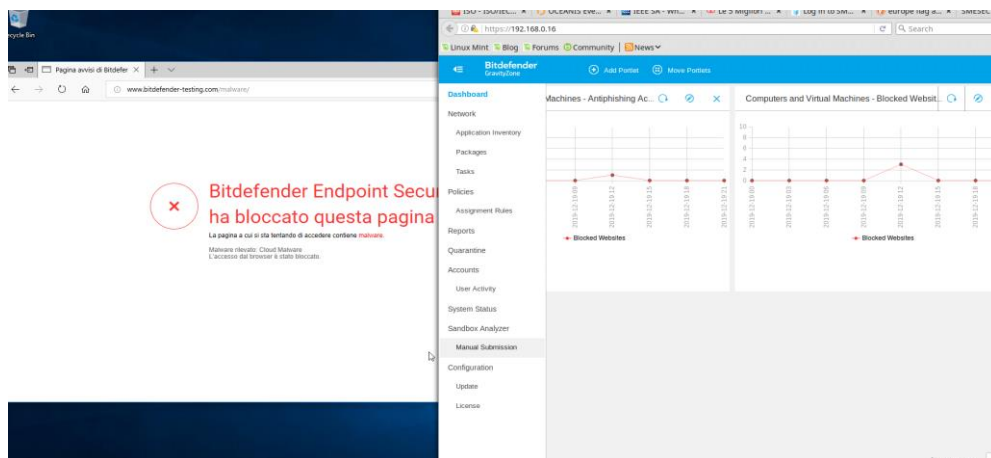


Figure 13. BitDefender dashboard, successfully blocked of malicious url

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	43 of 115
Reference:	D5.5	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

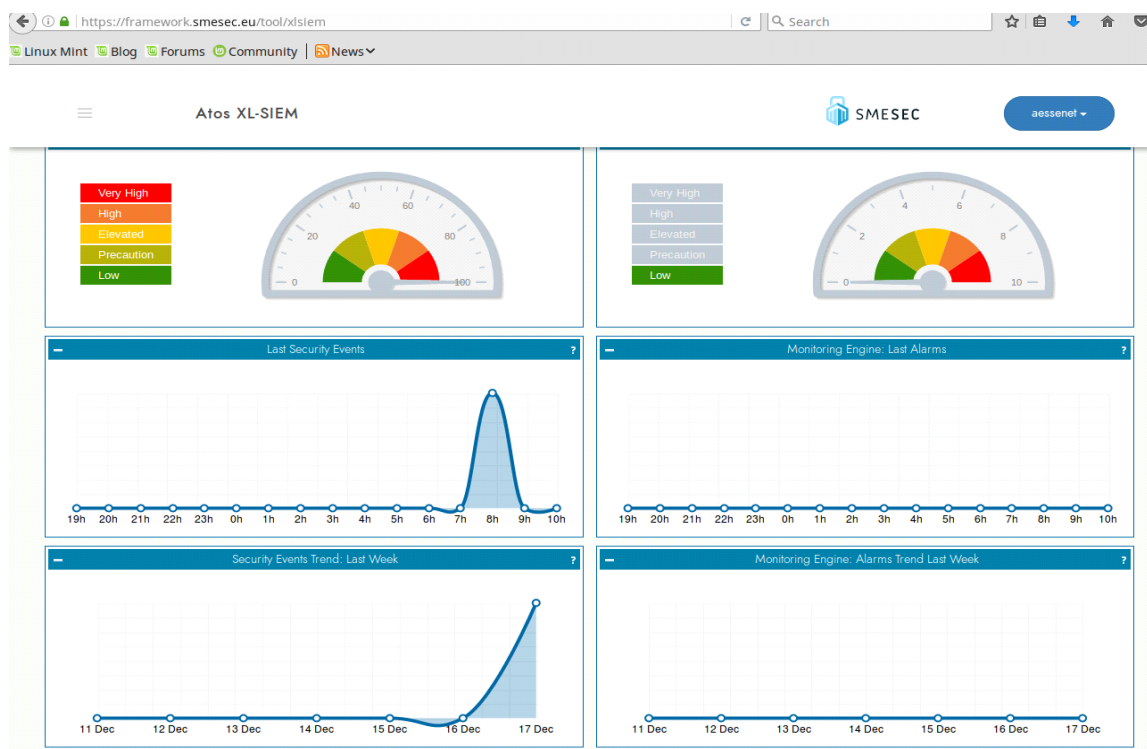


Figure 14. SMESEC SIEM dashboard.

4.2.6 ITML

Based on the tools and applications that ITML uses in its premises a subset the proposed tests were used for the evaluation of SMESEC.

Table 17. List of tests executed from ITML

Test-Codes	Description	Success	Date	Remarks / Execution details
IT_01_XL-SIEM	General test of relevant alerts	✓	30/01/2020	
IT_01_2_XL-SIEM	Test of test plugin	✓	30/01/2020	
IT_01_3_XL-SIEM	Test of SSH plugin	✓	30/01/2020	
IT_02_1_GravityZone	Malware detection in clients and servers, deployment and detection of test malware, alerts in relation to detected malware send and represented in GravityZone	✓	30/01/2020	

IT_02_2_GravityZone	Detection of downloaded malware	✓	30/01/2020	
IT_02_3_GravityZone	Accessing a blacklisted URL	✗	30/01/2020	Though we followed the instruction to the letter we were still able to visit the blacklisted URL from a Linux machine
IT_02_5_GravityZone	Detection of port scanning	✓	30/01/2020	
IT_03_1_HoneyPot	Detection of DDoS attack	✓	28/11/2019	
IT_03_2_HoneyPot	Detection of SQL-Injection attack	-	30/01/2020	We were not able to perform the test because we did not have any web server/service installed to test/apply it to
IT_03_3_HoneyPot	Detection of brute force attacks	✓	28/11/2019	

Remarks

A few images from the above tests



Figure 15. Detection of port scanning

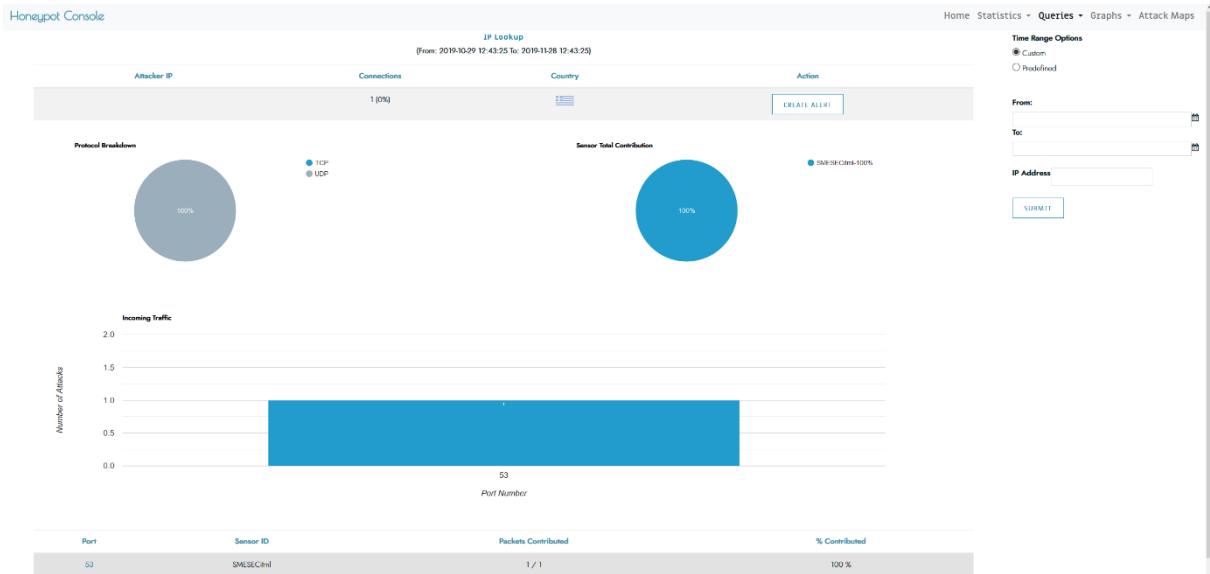


Figure 16. Honeypot DDoS Attack

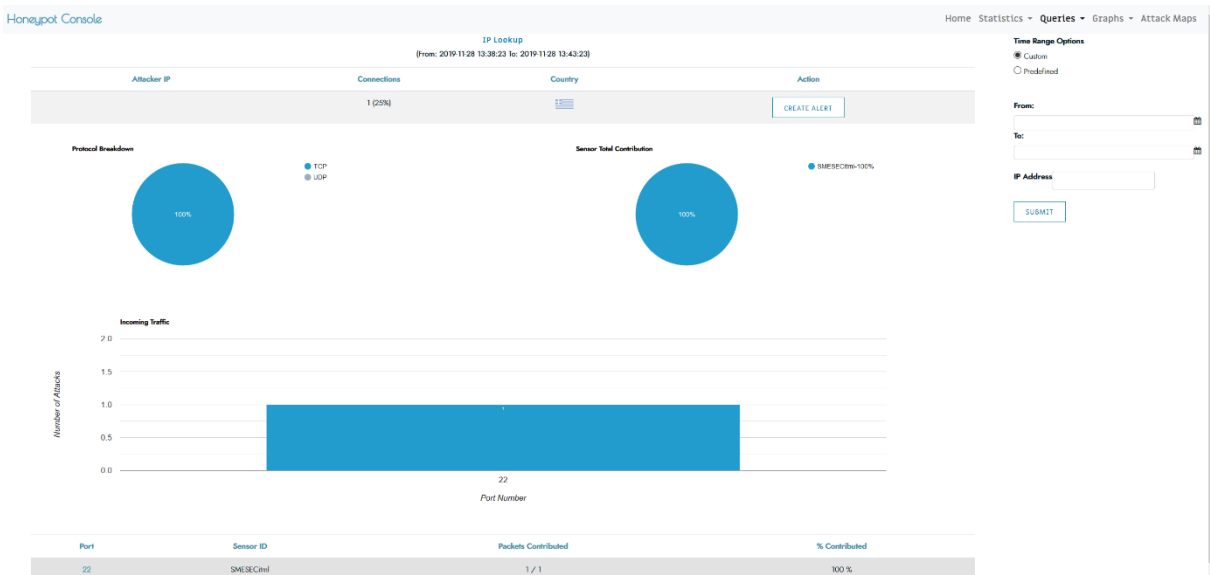


Figure 17. SSH Brute Force Attack

Time frame selection GMT+1:00: | Timeline analysis:

Unique addresses: Source | Destination | Source Port: TCP | UDP | Destination Port: TCP | UDP | Taxonomy: Product Types | Categories | Unique IP links [FQDN] | Unique Country Events

Today | Last 24h | Last 2 days | Last Week | Last 2 Weeks | Last Month | All | [Custom Views](#)

Displaying events 1-11 of about 11 matching your selection.

<input type="checkbox"/>	Signature	Date GMT+1:00	Sensor	Source	Destination	Asset S → D	Risk
<input type="checkbox"/>	SSHd: Generic SSH Event	2020-01-31 08:56:57	itml-agent			5 → 5	0
<input type="checkbox"/>	SSHd: Received disconnect	2020-01-31 08:56:57	itml-agent			5 → 5	0
<input type="checkbox"/>	SSHd: Input userauth request invalid user	2020-01-31 08:56:57	itml-agent			5 → 5	0
<input type="checkbox"/>	SSHd: Invalid user	2020-01-31 08:56:57	itml-agent			5 → 5	1
<input type="checkbox"/>	SSHd: Generic SSH Event	2020-01-31 08:56:33	itml-agent			5 → 5	0
<input type="checkbox"/>	SSHd: Received disconnect	2020-01-31 08:56:33	itml-agent			5 → 5	0
<input type="checkbox"/>	SSHd: Generic SSH Event	2020-01-31 08:56:29	itml-agent			5 → 5	0
<input type="checkbox"/>	SSHd: Received disconnect	2020-01-31 08:56:29	itml-agent			5 → 5	0
<input type="checkbox"/>	SSHd: Connection closed	2020-01-31 08:55:28	itml-agent			5 → 5	0
<input type="checkbox"/>	SSHd: Input userauth request invalid user	2020-01-31 08:55:28	itml-agent			5 → 5	0
<input type="checkbox"/>	SSHd: Invalid user	2020-01-31 08:55:28	itml-agent			5 → 5	1

Figure 18. Reports from XL-SIEM

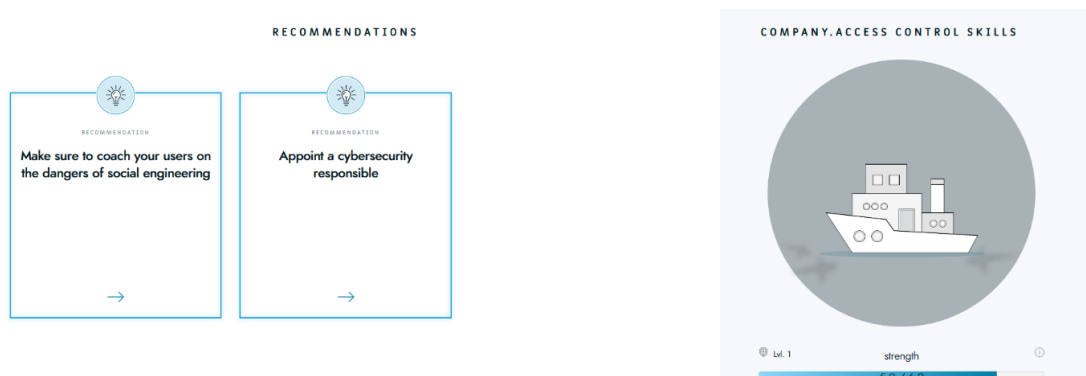


Figure 19. CYSEC results #1

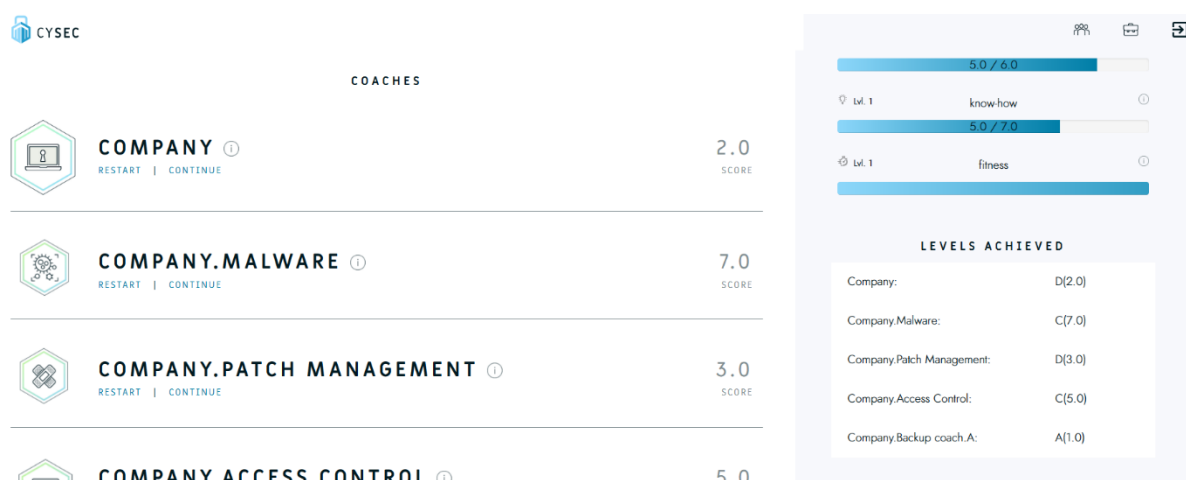


Figure 20. CYSEC results #2

4.2.7 Fraud Line

Based on the tools that Fraud Line has installed in its premises a subset of these tests will be used for the evaluation of SMESEC.

Table 18. List of tests executed from ITML

Test-Codes	Description	Success	Date	Remarks / Execution details
IT_01_1_XL-SIEM	Test whether the XL-SIEM agent is well connected to the XL-SIEM server	Partial	24/01/2020	There was partial success. While we integrated the service we are not certain whether the output observed was because of actual attacks or other reasons. We also failed to see consistently the EWIS output on the SIEM Dashboard.
IT_01_2_XL-SIEM	Test of test plugin			
IT_01_3_XL-SIEM	Test of SSH plugin			
IT_01_4_XL-SIEM	Test of FORTH EWIS plugin			
IT_01_5_XL-SIEM	Test of ADC plugin			

IT_06_CITRIX-ADC	Detects malicious or improper network traffic and blocks it before reaching the backend application servers, potentially causing service downtime. stops it	✗	19/12/2019	The test was not successful since we failed to properly implement the service on Azure. We tried to use the documentation for AWS and apply it for Azure. We spent a lot of time on this, but the attempt was not successful.
IT_03_1_Honeypot	Detection of DDoS attack	✓	24/01/20	All results were successful after installing the service and running the test codes. We used a virtual machine to attack the honeypot and we saw the response on the EWIS dashboard.
IT_03_2_Honeypot	Detection of SQL-Injection attack			
IT_03_3_Honeypot	Detection of brute force attacks			

Remarks

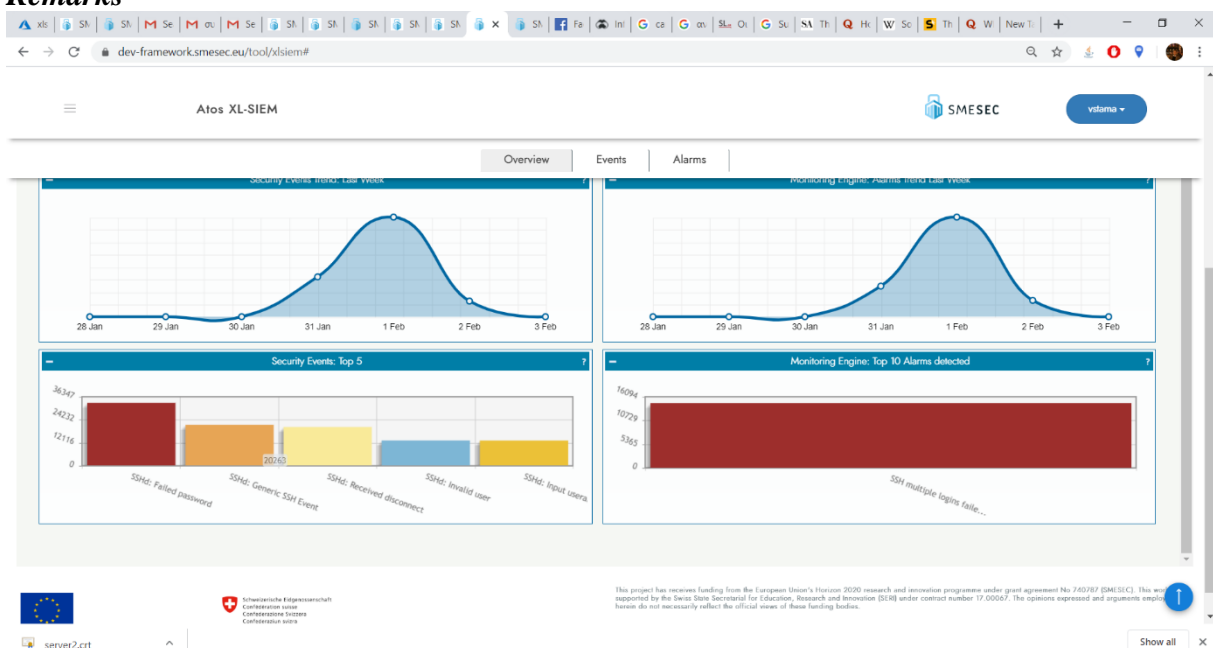


Figure 21. XL-SIEM general report graphs.

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	48 of 115
Reference:	D5.5	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

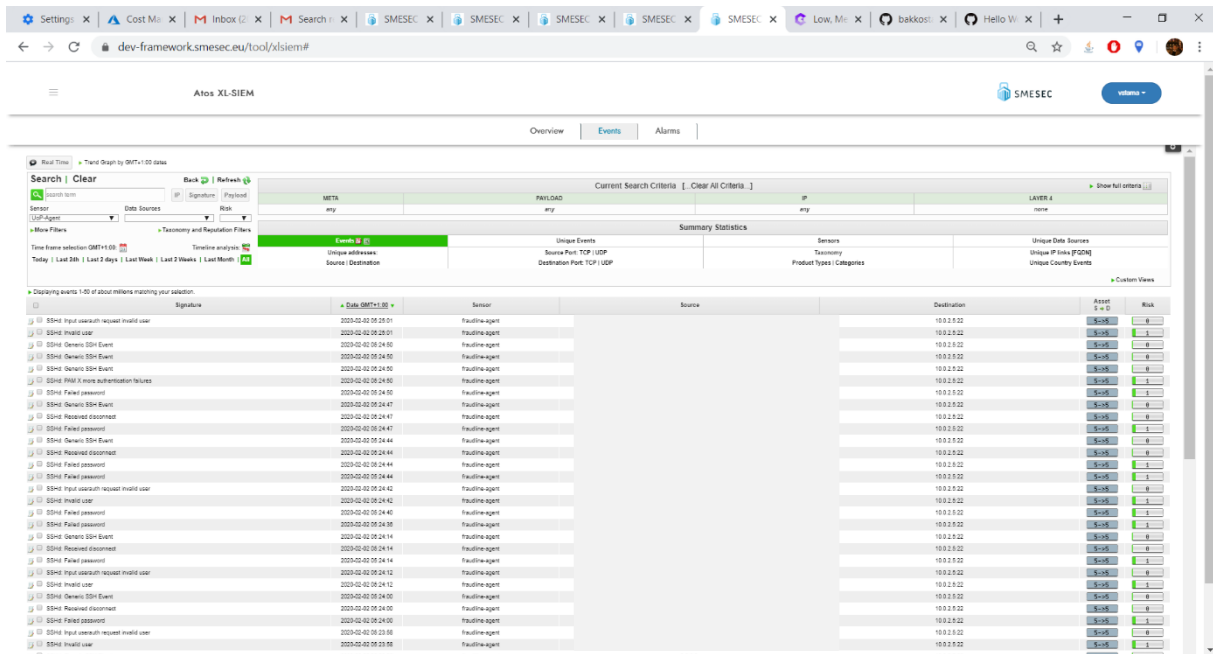


Figure 22. Alerts as received by XL-SIEM agent



Figure 23. Results of EWIS testing as appear in SMESEC framework.

4.3 “Category 2b: External API Integration” Technical Results

In order to mark the integration between the external SMEs and SMESEC successful, we tested if information coming from the external SMEs arrived our internal infrastructure. All the involved SMEs successfully completed the test. For each of the external companies, the following procedure was followed:

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	49 of 115
Reference:	D5.5	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

- Creation and distribution of the external API code.
- Creation of a public documentation page with usage instructions[6].
- Transformer function implemented by AEGIS, After Tech and RKL.
- Certificate distribution by the SMESEC Consortium for communicating with the SMESEC Framework.
- Testing of the external API, by:
 - Sending messages from the external tool to the external API.
 - Checking in the SMESEC internal infrastructure that messages are arriving to it.

The results for each individual company are presented in the following subsections below.

As a result of the external API, and following some recommendations received by the partners of the open call, a new version of the external API have been developed, providing a default transformation function that expects the input to be in the correct format of the messages.

This allows to external tools to rely on internal modifications, without need to have any kind of knowledge of the external API architecture or implementation details.

4.3.1 AEGIS

In this subsection, evidence of the integration with AEGIS are provided. In Figure 24, the logs of the external API tool deployed on AEGIS side show information about the information sent by their tool to SMESEC. Then, in Figure 25, a screenshot of the RabbitMQ queue used for receiving the data is shown.

```

2020-01-24 11:20:25,573 INFO [main] [eu.smesec.framework.external.api.core.communication.CommunicationService] - Sending data from organization AEGIS IT RESEARCH to rabbitMQ.
2020-01-24 11:20:25,648 INFO [main] [com.aegis.netflowreader.NetflowReader] - SMESEC Object sent - Critical Connections Count:{"description": "Abnormal number of Network Connections", "timestamp": {"date": {"year": 2020, "month": 1, "day": 24}, "time": {"hour": 11, "minute": 18, "second": 0, "nano": 0}}, "attackRecipient": "192.168.1.82", "severity": 6, "validity": 1579861224987, "organization": "AEGIS IT RESEARCH", "additionalAttributes": {"Number_Connections": 17}}
2020-01-24 11:20:25,656 INFO [main] [com.aegis.netflowreader.NetflowReader] - 192.168.1.82; Network Connections;CRITICAL;Network Connections 17 at 2020-01-24 11:18
Nfdump CSV file processed: /root/NetFlowAgent/nfdumpCSVs/nfcapd.202001241115.csv
  
```

Figure 24 - AEGIS log sent to SMESEC

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	50 of 115
Reference:	D5.5	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

```

exchange test-exchange
Routing
  Key
  elivered 0
  operties
Payload
  262 bytes
  Encoding:
  string
{"externalData":{"description":"Abnormal number of Network Connections","timestamp":"2020-01-24T11:16:00","attackRecipient":"192.168.1.82","severity":6,"validity":1579861223642,"organization":"AEGIS IT RESEARCH","additionalAttributes":{"Number_Connections":125}}}

rge 472
erver reported 2 messages remaining.

exchange test-exchange
Routing
  Key
  elivered 0
  operties
Payload
  262 bytes
  Encoding:
  string
{"externalData":{"description":"Abnormal number of Network Connections","timestamp":"2020-01-24T11:17:00","attackRecipient":"192.168.1.82","severity":6,"validity":1579861224987,"organization":"AEGIS IT RESEARCH","additionalAttributes":{"Number_Connections":411}}}

rge 473
erver reported 1 messages remaining.

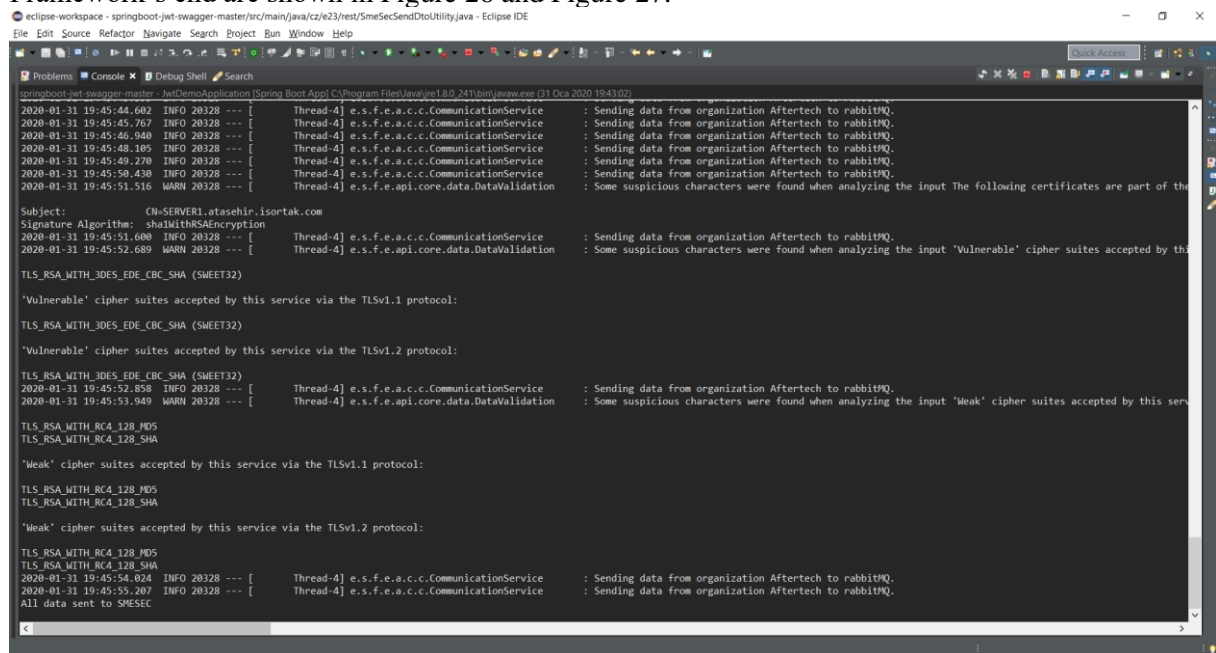
exchange test-exchange
Routing
  Key
  elivered 0
  operties
Payload
  262 bytes
  Encoding:
  string
{"externalData":{"description":"Abnormal number of Network Connections","timestamp":"2020-01-24T11:18:00","attackRecipient":"192.168.1.82","severity":6,"validity":1579861224987,"organization":"AEGIS IT RESEARCH","additionalAttributes":{"Number_Connections":17}}}

```

Figure 25 - AEGIS log received by SMESEC

4.3.2 After Tech

The proofs of a working integration with After Tech are presented in this subsection. As in the previous subsection, logs of the external API running on After Tech’s side and a screenshot of the SMESEC Framework’s end are shown in Figure 26 and Figure 27.



```

springboot-jwt-swagger-master - JarDemoApplication [Spring Boot App] C:\Program Files\Java\jre1.8.0_241\bin\java.exe (31 Oct 2020 19:43:02)
2020-01-31 19:45:44.602 INFO 20328 --- [ Thread-4] e.s.f.e.a.c.c.CommunicationService : Sending data from organization Aftertech to rabbitMQ.
2020-01-31 19:45:45.767 INFO 20328 --- [ Thread-4] e.s.f.e.a.c.c.CommunicationService : Sending data from organization Aftertech to rabbitMQ.
2020-01-31 19:45:46.940 INFO 20328 --- [ Thread-4] e.s.f.e.a.c.c.CommunicationService : Sending data from organization Aftertech to rabbitMQ.
2020-01-31 19:45:48.105 INFO 20328 --- [ Thread-4] e.s.f.e.a.c.c.CommunicationService : Sending data from organization Aftertech to rabbitMQ.
2020-01-31 19:45:49.270 INFO 20328 --- [ Thread-4] e.s.f.e.a.c.c.CommunicationService : Sending data from organization Aftertech to rabbitMQ.
2020-01-31 19:45:50.430 INFO 20328 --- [ Thread-4] e.s.f.e.a.c.c.CommunicationService : Sending data from organization Aftertech to rabbitMQ.
2020-01-31 19:45:51.516 WARN 20328 --- [ Thread-4] e.s.f.e.a.c.c.core.data.DataValidation : Some suspicious characters were found when analyzing the input The following certificates are part of the
Subject: CN=SERVER1.atasehir.isortak.com
Signature Algorithm: sha1withRSAEncryption
2020-01-31 19:45:51.608 INFO 20328 --- [ Thread-4] e.s.f.e.a.c.c.CommunicationService : Sending data from organization Aftertech to rabbitMQ.
2020-01-31 19:45:52.689 WARN 20328 --- [ Thread-4] e.s.f.e.a.c.c.core.data.DataValidation : Some suspicious characters were found when analyzing the input 'Vulnerable' cipher suites accepted by the
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SMEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SMEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SMEET32)
2020-01-31 19:45:52.858 INFO 20328 --- [ Thread-4] e.s.f.e.a.c.c.CommunicationService : Sending data from organization Aftertech to rabbitMQ.
2020-01-31 19:45:53.949 WARN 20328 --- [ Thread-4] e.s.f.e.a.c.c.core.data.DataValidation : Some suspicious characters were found when analyzing the input 'Weak' cipher suites accepted by this ser
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
2020-01-31 19:45:54.024 INFO 20328 --- [ Thread-4] e.s.f.e.a.c.c.CommunicationService : Sending data from organization Aftertech to rabbitMQ.
2020-01-31 19:45:55.207 INFO 20328 --- [ Thread-4] e.s.f.e.a.c.c.CommunicationService : Sending data from organization Aftertech to rabbitMQ.
All data sent to SMESEC

```

Figure 26- AfterTech log sent to SMESEC

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	51 of 115
Reference:	D5.5	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

```

Exchange test-exchange
Routing Key
Redelivered 0
Properties
Payload 1202 bytes
Encoding string
{"externalData":{"timestamp":"2020-01-23T12:08:20.823","attacker":"127.0.0.1","attackRecipient":"192.168.10.10","severity":5,"validity":"1579778500015","organization":"AfterTech","additionalAttributes":{"VulnName":"DCE/RPC and MSRPC Services Enumeration Report:
...
Message 97
The server reported 257 messages remaining.
Exchange test-exchange
Routing Key
Redelivered 0
Properties
Payload 612 bytes
Encoding string
{"externalData":{"timestamp":"2020-01-23T12:08:20.824","attacker":"127.0.0.1","attackRecipient":"192.168.10.10","severity":4,"validity":"1579778500024","organization":"AfterTech","additionalAttributes":{"VulnName":"Git Privilege Escalation Vulnerability - Wind
...
Message 98
The server reported 256 messages remaining.
Exchange test-exchange
Routing Key
Redelivered 0
Properties
Payload 612 bytes
Encoding string
{"externalData":{"timestamp":"2020-01-23T12:08:20.824","attacker":"127.0.0.1","attackRecipient":"192.168.10.10","severity":7,"validity":"1579778500024","organization":"AfterTech","additionalAttributes":{"VulnName":"MS Windows HID Functionality (Over USB) Code I

```

Figure 27- AfterTech log received by SMESEC

4.3.3 RKL

As in the previous subsections, evidences of the integration between RKL and the SMESEC Framework are presented in Figure 28 and Figure 29.

```

@id@ps@87191:/var/log
rk1@ps@87191:/var$ ls
backlog  cron  local  log  opt  snap  tmp
cronlog  lib  lock  mail  run  spool  www
rk1@ps@87191:/var$ cd log
rk1@ps@87191:/var/log$ ls
alternatives.log  cloud-init-output.log  kern.log.1  syslog.1
alternatives.log.1  dconf-gsettings-cache.log  landiscope  syslog.2.gz
apt  apt-get.d  apt-get.log.1  apt-get.log.2.gz  apt-get.log.3.gz  apt-get.log.4.gz
auth.log  auth.log.1  auth.log.2.gz  auth.log.3.gz  auth.log.4.gz
auth.log.1  fail2ban.log  fail2ban.log.1  fail2ban.log.2.gz  fail2ban.log.3.gz  fail2ban.log.4.gz
auth.log.2.gz  fail2ban.log.1  mail.err  mail.err.1  mail.log  maillog
auth.log.3.gz  fail2ban.log.2.gz  mail.log.1  mysql  wtmp
btm  fail2ban.log.4.gz  mysql  wtmp
cron  cronlog  cronlog.1  cronlog.2.gz  cronlog.3.gz  cronlog.4.gz
cloud-init.log  kern.log  kern.log.1  kern.log.2.gz  kern.log.3.gz  kern.log.4.gz
rk1@ps@87191:/var/log$ tail -f /opt/smesec-agent/agent/agent.log
2019-12-28 07:08:00.873 INFO 1579 --- [io-8080-exec-1] e.s.f.a.a.c.c.CommunicationService : Sending data from organization rk1 to rabbitmq.
Incoming data: {"severity":9,"organization":"rk1","attacker":"49.91.240.176","attackRecipient":"192.168.2.12","validity":"1577515201","timestamp":"2019-12-28T07:08:00.873"}
type: class org.json.JSONObject
organization rk1, type: class java.lang.String
severity 9, type: class java.lang.String
validity 1577515201, type: class java.lang.String
timestamp 2019-12-28T07:08:00.873, type: class java.lang.String
attacker 49.91.240.176, type: class java.lang.String
attackRecipient 192.168.2.12, type: class java.lang.String
2019-12-28 07:08:01.821 INFO 1579 --- [io-8080-exec-2] e.s.f.a.a.c.c.CommunicationService : Sending data from organization rk1 to rabbitmq.
Incoming data: {"severity":7,"organization":"rk1","attacker":"192.151.209.12","attackRecipient":"192.168.4.13","validity":"1577516793","timestamp":"2019-12-28T08:05:01.752"}
type: class org.json.JSONObject
organization rk1, type: class java.lang.String
severity 7, type: class java.lang.String
validity 1577516793, type: class java.lang.String
timestamp 2019-12-28T08:05:01.752, type: class java.lang.String
attacker 192.151.209.12, type: class java.lang.String
attackRecipient 192.168.4.13, type: class java.lang.String
2019-12-28 08:01:02.420 INFO 1579 --- [io-8080-exec-3] e.s.f.a.a.c.c.CommunicationService : Sending data from organization rk1 to rabbitmq.
Incoming data: {"severity":7,"organization":"rk1","attacker":"144.40.182.96","attackRecipient":"192.168.5.3","validity":"1577517001","timestamp":"2019-12-28T08:10:01.703"}
type: class org.json.JSONObject
organization rk1, type: class java.lang.String
severity 7, type: class java.lang.String
validity 1577517001, type: class java.lang.String
timestamp 2019-12-28T08:10:01.703, type: class java.lang.String
attacker 144.40.182.96, type: class java.lang.String
attackRecipient 192.168.5.3, type: class java.lang.String
2019-12-28 08:10:02.544 INFO 1579 --- [io-8080-exec-2] e.s.f.a.a.c.c.CommunicationService : Sending data from organization rk1 to rabbitmq.
Incoming data: {"severity":9,"organization":"rk1","attacker":"164.246.28.140","attackRecipient":"192.168.1.0","validity":"1577517811","timestamp":"2019-12-28T08:15:01.801"}
type: class org.json.JSONObject
organization rk1, type: class java.lang.String
severity 9, type: class java.lang.String
validity 1577517811, type: class java.lang.String
timestamp 2019-12-28T08:15:01.801, type: class java.lang.String
attacker 164.246.28.140, type: class java.lang.String
attackRecipient 192.168.1.0, type: class java.lang.String
2019-12-28 08:15:02.544 INFO 1579 --- [io-8080-exec-1] e.s.f.a.a.c.c.CommunicationService : Sending data from organization rk1 to rabbitmq.
Incoming data: {"severity":6,"organization":"rk1","attacker":"83.47.47.236","attackRecipient":"192.168.1.7","validity":"1577519441","timestamp":"2019-12-28T08:50:01.907"}
type: class org.json.JSONObject
organization rk1, type: class java.lang.String
severity 6, type: class java.lang.String
validity 1577519441, type: class java.lang.String
timestamp 2019-12-28T08:50:01.907, type: class java.lang.String
attacker 83.47.47.236, type: class java.lang.String
attackRecipient 192.168.1.7, type: class java.lang.String

```

Figure 28- RKL log sent to SMESEC

```

Message 1
The server reported 0 messages remaining.
Exchange test-exchange
Routing Key
Redelivered 0
Properties
Payload 198 bytes
Encoding string
{"externalData":{"timestamp":"2019-12-28T07:40:01.684","attacker":"49.91.240.176","attackRecipient":"192.168.2.12","severity":9,"validity":1577515201,"organization":"rk1","additionalAttributes":{}}}


```

Figure 29 - RKL log received by SMESEC

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	52 of 115
Reference:	D5.5 Dissemination: PU	Version:	1.0
		Status:	FINAL

4.4 “Category 3: SME Association”—Activities and Results

From the open call, an SME association was selected to help promoting SMESEC at larger scale and give feedback on SMESEC framework from multiple users perspective.

 The selected association was the IT Forum in Denmark. It-forum is a membership-based network for more than 470 companies from private and public organizations, colleges, and local, regional and state authorities in Region Midtjylland and Southern Denmark. They represent in total close to 20.000 IT people in all positions from CEOs to programmers.

Their members share an interest in adopting smart ICT technologies for innovating purposes and in order to improve their businesses. The it-forum headquarter is based in the heart of the Aarhus University campus, IT research, and innovation center. From the headquarter and its nine local offices around the region of Middle Jutland and Southern Denmark, it-forum is close to the cluster of members and all local authorities in the major cities in the region.

4.4.1 SMESEC promotion and engagement

It-forum has helped disseminating the SMESEC training platform by promoting cybersecurity awareness to all our approx. 450 Danish membership companies. We decided to expand the target group and offer access to the online “public questionnaire” to all subscribers of our monthly newsletter as well. Over 92% of the receivers are either responsible for or employee in a Danish SME. This means that the total number of receivers (from two mailing lists) where: $2.421 + 291 = 2.712$

IT forum also push access to the questionnaire and awareness about SMESEC through our personal networks also. The largest personal network belongs to it-forum’s CEO Bo Sejer Frandsen and CCO Karsten Dehler. Both shared a personal post dedicated to this task. Please see Figure 30 and 2.6 for LinkedIn statistics.

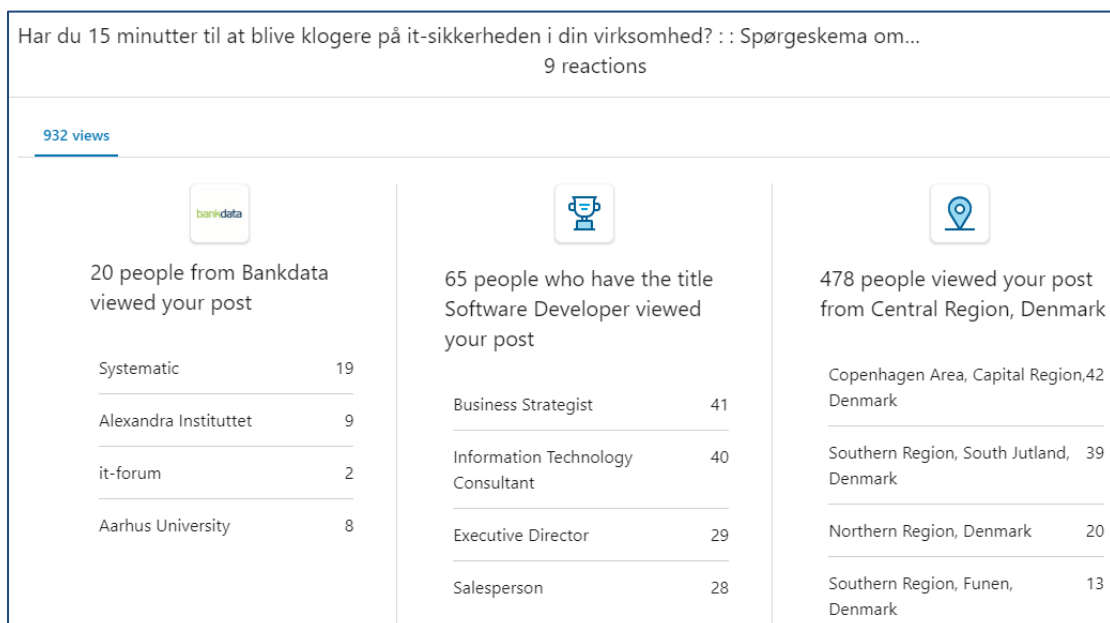


Figure 30. Detailed Numbers from CEO’s Shares on LinkedIn

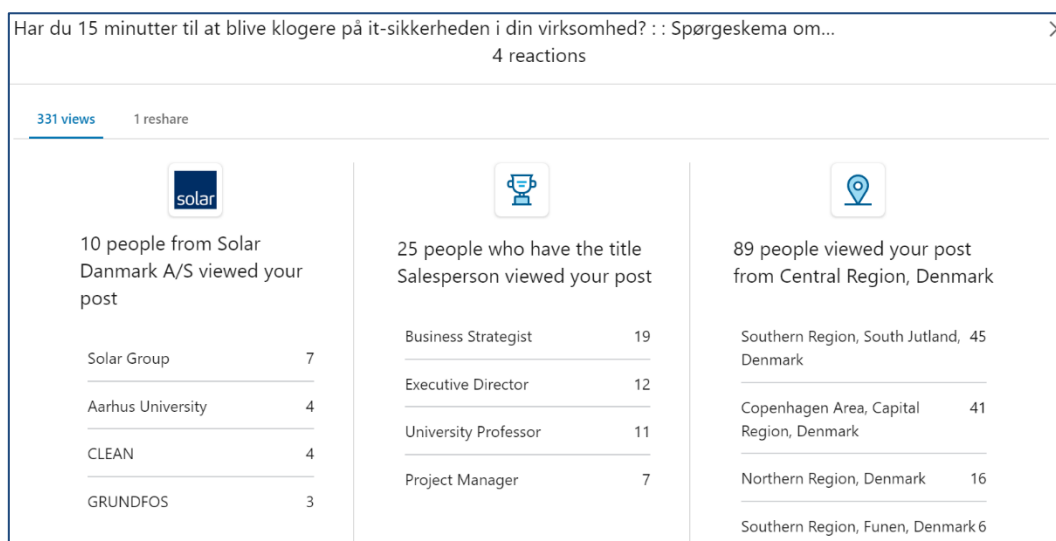


Figure 31. Detailed Numbers from CCO's Shares on LinkedIn

Total number of views for the two posts was 1.263

After having shared access to the online form and information about SMESEC several times in November and December 2019 the number of completed questionnaires was quite limited.

Final list of actions taken:

- Two newsletters/direct mails in November 2019
- Two dedicated LinkedIn post in December 2019
- Two physical events in Vejle and Aarhus in January 2020

4.4.2 SMESEC Promoting Security Awareness

In January 2020 we had two physical events where CEOs, CTOs and other “strategic decisionmakers” were invited. The events were in Vejle (21st in the Southern Region of Denmark) and in Aarhus (23rd in the Middle Region of Denmark). [Pictures from the two events can be found in Appendix 1].

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	54 of 115
Reference:	D5.5	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

Both the presentation and link to the online questionnaire was shared to all participants in the “Follow up”/”Thank you for participating” emails after each event [please see screenshots below]. The deadline for completion was set to Friday the 24th and Monday the 27th of January.

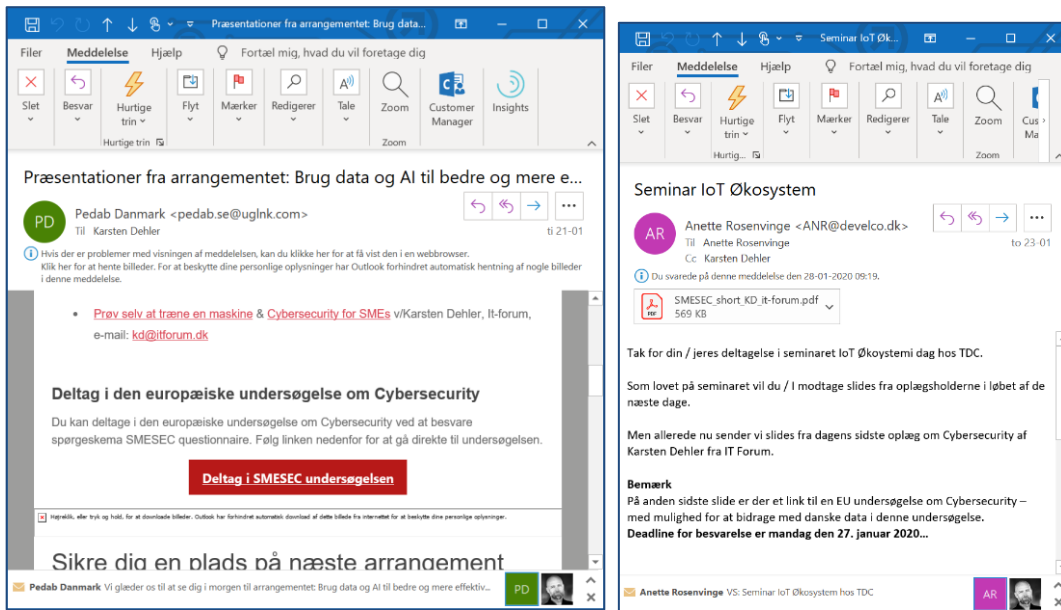


Figure 32. Examples of Follow-up Emails

In both events other presenters were talking about the potential of Digital Transformation and my expectation was that adding the Cyber Security aspect here would create interest from the participants as they got the “all-around image” of the whole AI/IoT ecosystem. Addressing non-technical matters did not meet our expectations unfortunately.

The people we have spoken to have all been advised to go to the SMESEC website to create a profile and to log on so that we could look at the training platform together. No one has succeeded in this task and for me personally I have tried to create a user without any luck. Therefore, the personal interviews have not been carried out as planned.

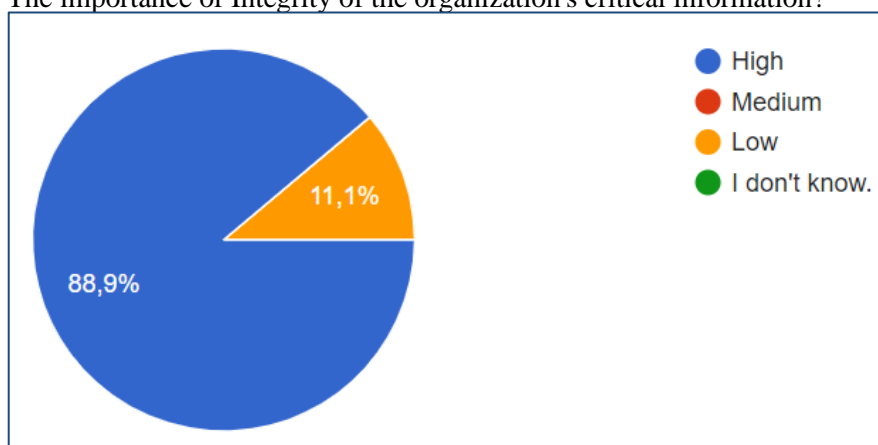
4.4.3 Feedback on SMESEC

Access to online survey has been broadcasted as mentioned above. The introduction and background have been in Danish but info about SMESEC and the online questionnaire in English also asking the participants to please give their replies in English

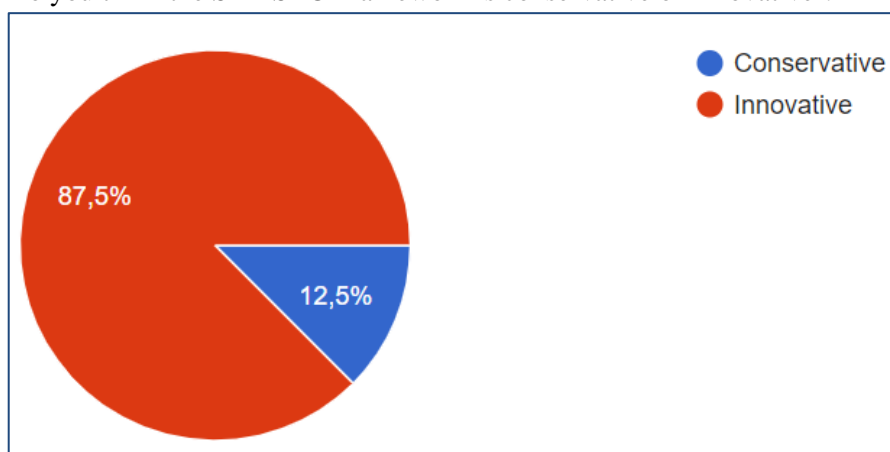
The clearest answers are the following two questions from the survey:

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	55 of 115
Reference:	D5.5	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

1) The importance of Integrity of the organization's critical information?



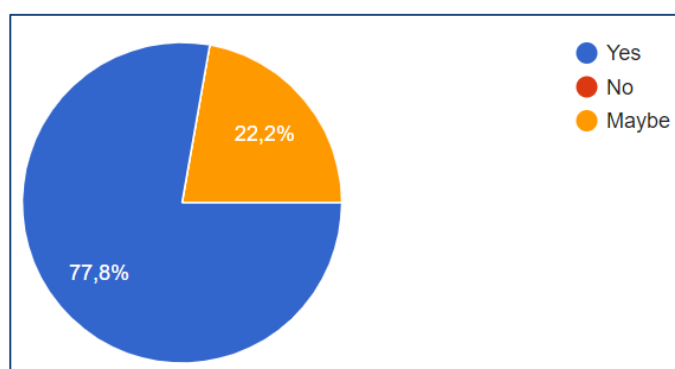
2) Do you think the SMESEC Framework is conservative or innovative ?



So, a vast majority of the participants are rating the Integrity of the organization's critical information as high (89,9%) and 87,5% of the participants finds SMESEC Innovative.

Even though we must be careful not to conclude too much on this Danish surveys "thin" results, as we can't be certain that the results are representative for the general population of SME's, there is also a clear believe among the respondees that ".. information security standards or cybersecurity standards may improve the quality of their products or services" (77,8%).

Q: Do you believe that information security standards or cybersecurity standards may improve the quality of your services or products?



4.5 Training and Awareness -- Results

4.5.1 Training Courses and Material

During the open call evaluation phase all participants were given access to the training service of SMESEC. The service, among others, makes use of an external platform which hosts a list of courses created by SMESEC partners. The external platform is called securityaware.me and is designed and hosted by University of Patras (Figure 33)

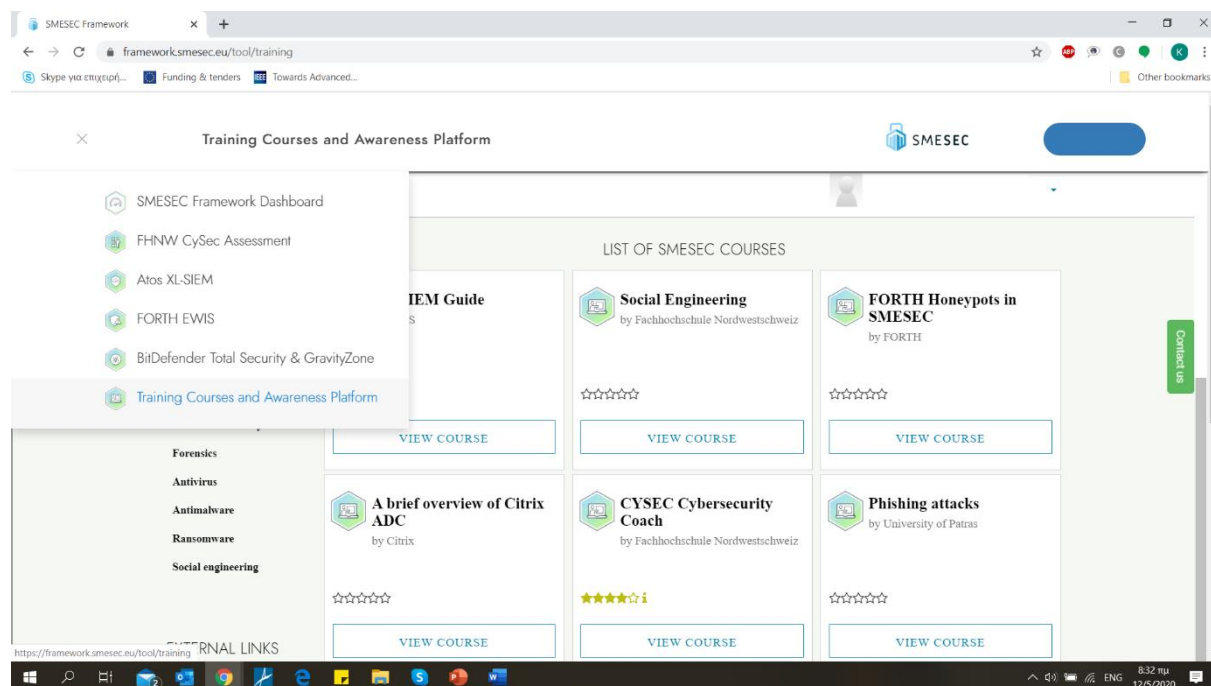


Figure 33. SMESEC Training Courses and Awareness Platform

The courses created by SMESEC partners and hosted in the securityaware.me platform include general security courses (e.g. Social Engineering) as well as tool specific trainings (e.g. FORTH Honeypots in SMESEC). A menu on the left side of the main page, allows the user to filter courses based on his preference.

Inside the context of the project, the securityaware.me platform was integrated with the SMESEC framework to present a seamless experience to the end user. In particular:

- A new -SMESEC alike- webpage was created to present the training courses of SMESEC project. This webpage (Figure 33) follows the design patterns, icons and colour pallets of the SMESEC framework.
- SMESEC users are automatically identified by the securityaware.me platform as SMESEC users, without the need any additional registration actions.

The courses provided to the open call SMEs, were highly diverse. We included courses on general security aspects (designed for people with little background in security) as well as more complicated courses with highly technical details for more experienced users. Our goal was to investigate the “type of users” SMESEC platform is likely to have and what should the level of complexity for SMESEC training material be. The results of the evaluation demonstrated that there were many comments in favor of the general-purpose courses, but also some arguing against them, stating that SMESEC training should be more technical-oriented and based on its provided tools.

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	57 of 115
Reference:	D5.5	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

Considering the overall evaluation of the SMESEC training we requested from all open call participants to evaluate the training service and the courses material they selected to do. More specifically each participant had to at least complete 3 training courses and then a) answer a list of questions considering the whole experience, any problems they experienced etc. b) complete a “score board” (template) for at least 2 of these courses.

The good news that the 8 SMEs succeeded to run 30 training courses and globally like the experience. The success rate of the experience scored from 1 to 10 is 64%

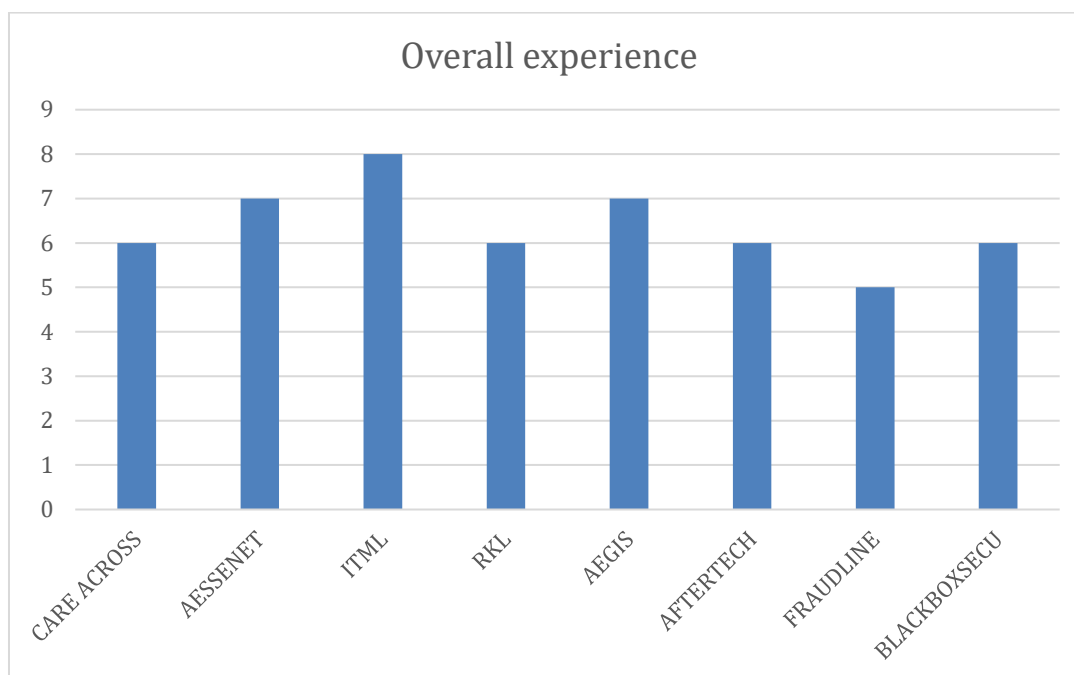


Figure 34: Answers from the 8 SMEs on Overall Experience (Score from 0 to 10)

Although, there were different expectations 65% of them agreed that the objectives of training were met

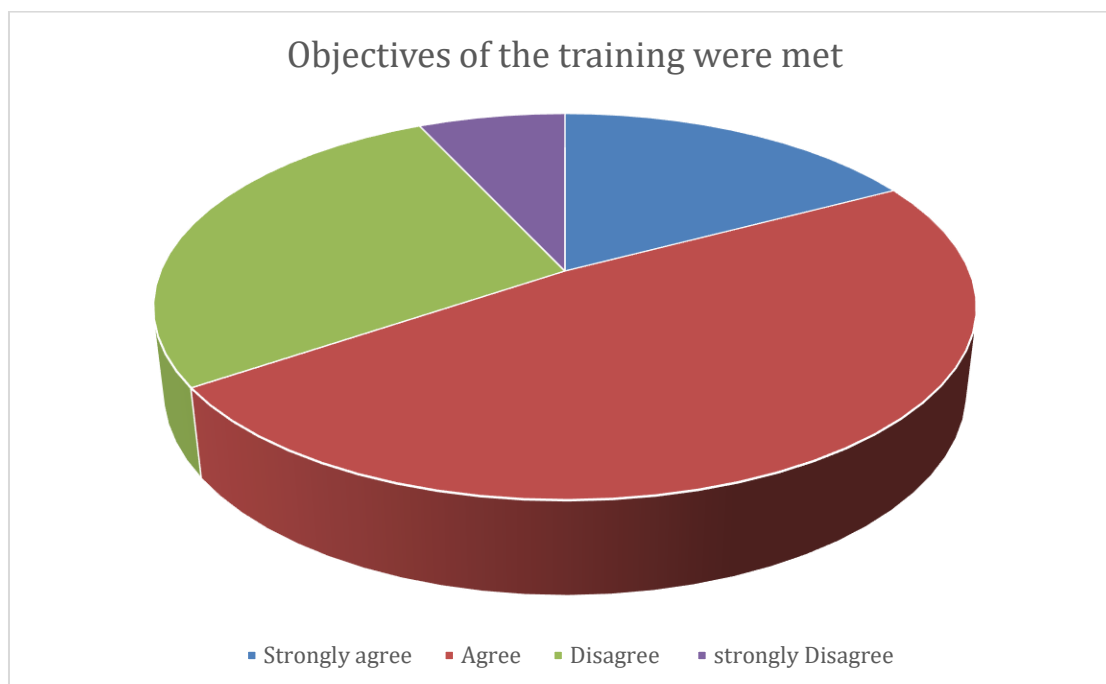


Figure 35: Answers Whether the Objectives of the Courses Were Met

64% agreed that the courses brought skills that was easy to apply on what they learnt

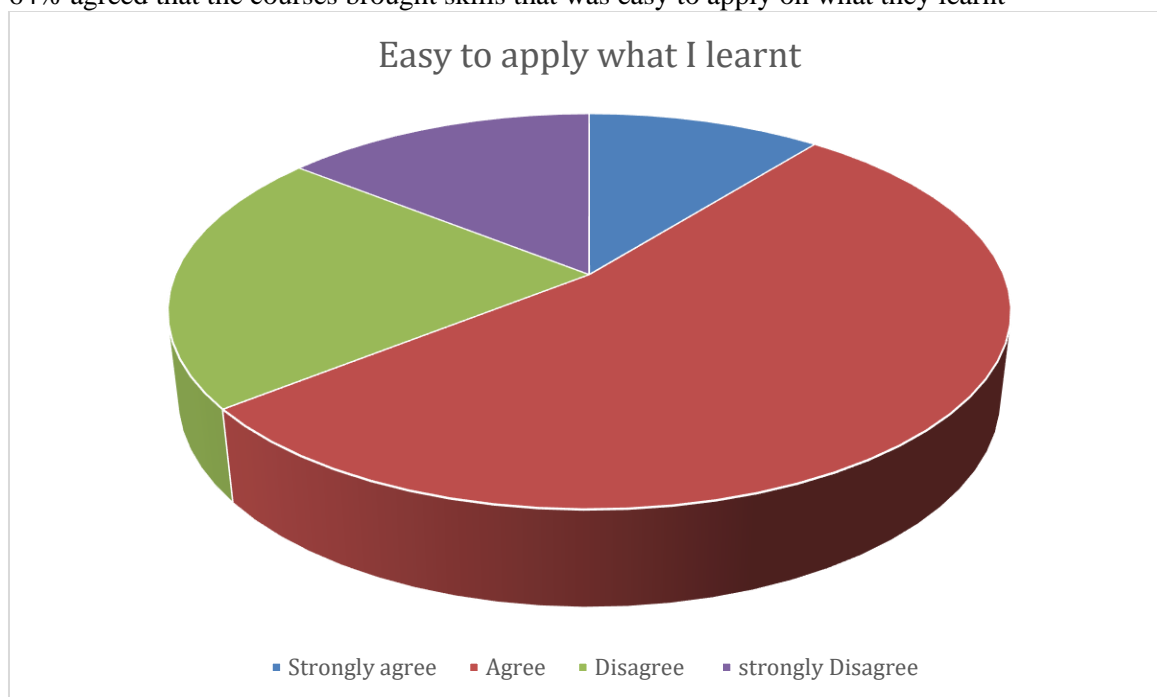


Figure 36 : Answers on Whether it was Easy to Apply What Was Learnt

The best conclusion on the usefulness on the course could summary in the question : would you recommend these courses to colleagues ? 70% of courses got a yes

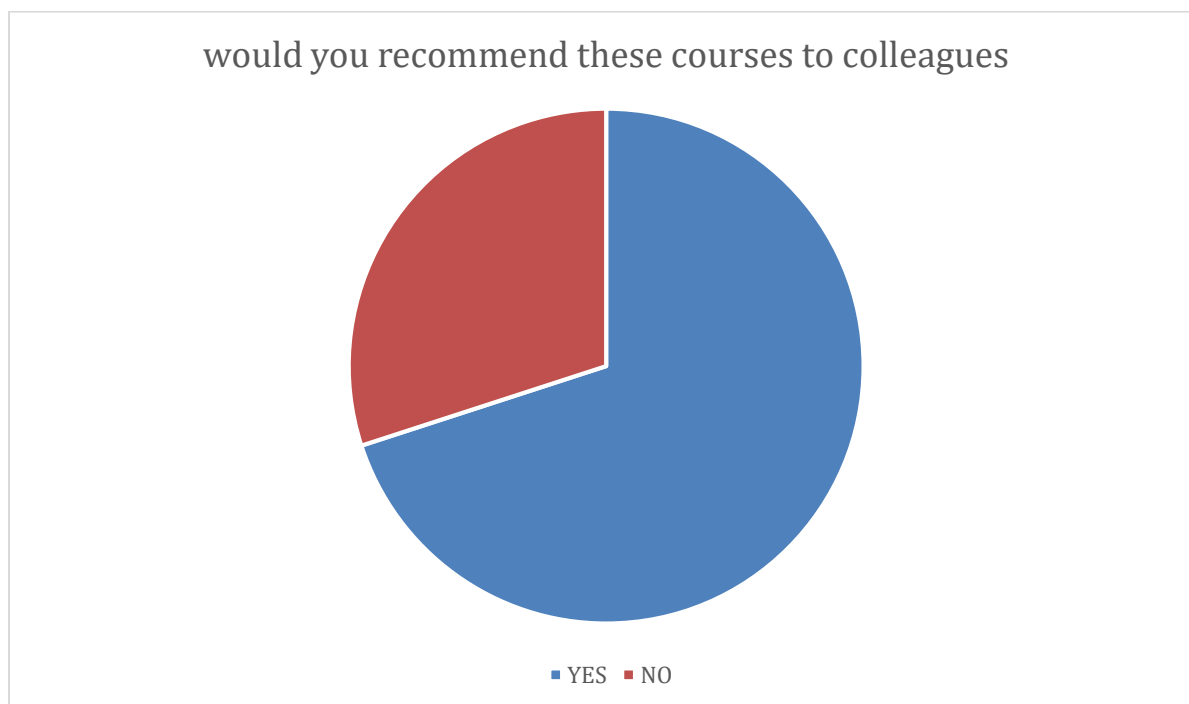


Figure 37: Answers on Whether SMEs Would Recommend the Courses to Colleagues

The comments received for technical issues or suggestions about the training platform and how we addressed them are presented below.

- Filter menu on the left was not working properly: UOP identified what was the problem and fixed it. Now the left filter menu is working properly.
- SMEs would like to have a view of the percentage of the course completion: SMESEC framework and UOP have designed and implemented a feature which allows the training platform (securityaware.me) monitor the percentage of a course that has been completed by a specific user. This information is then sent to SMESEC framework and is presented in the main dashboard.
- Personalization of the suggested training: SMESEC framework now allows an authorised user (e.g. the administrator of a company) to select the list of courses that are relevant for its users. Also, the CYSEC tool now provides recommendations for training courses after the completion of coaches.
- Categorize trainings based on proficiency and levels: Since the training service is a part of SMESEC solution, we focused on creating tools for personalization of trainings at the SMESEC framework. Under this approach, we decided to treat the training platform as a hosting service which should not interfere with the organization of SMESEC training courses and service.

Apart from the evaluation of the course material, during the open call, SMESEC requested from Montimage, the participating company in Category 1 (red team) to also perform a penetration testing to the external platform used for the SMESEC training platform (securityaware.me). The reason behind this request was because the platform was created by a University and had not been extensively tested like a company would do if this was a market product. Also, we wanted to make sure that all the components and tools used inside the SMESEC framework are secure and do not pose any threat to the system and its potential customers.

The initial pen test during the open call revealed severe vulnerabilities to the securityaware.me platform. Such vulnerabilities allowed the red team to launch successful attacks to the website. In total of 22 vulnerabilities were found with at least 4 of them been critical. Based this evaluation report, University

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	60 of 115
Reference:	D5.5	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

of Patras communicated with Montimage and agreed on the following. University of Patras team would work to address the identified vulnerabilities and specifically the critical ones. Then Montimage would perform a second penetration testing and report its findings.

After the security updates and fixes, the second pen test was a success. The red team was not able to replicate any of the major attacks of the first round and also confirmed that all critical security fixes that were suggested after the first pen test were applied. A detailed report on this activity can be found in Annexes of the deliverable D7.4 (private).

4.5.2 Impact on Awareness (CYSEC tool used by the OpenCall SMEs)

In this section, we describe the CYSEC features offered to the SMEs and explain how we planned these features to affect the SMEs’ awareness of threats, controls, practices, and tools. In the next section, we will describe how we evaluated the impact of CYSEC on awareness and report the results of the evaluation.

4.5.2.1 CYSEC training and awareness features

To supporting effective security communication with users and improving awareness, CYSEC has two main interfaces: the dashboard and the work area. The dashboard is shown in the top left of Figure 38, the work area at the bottom right.

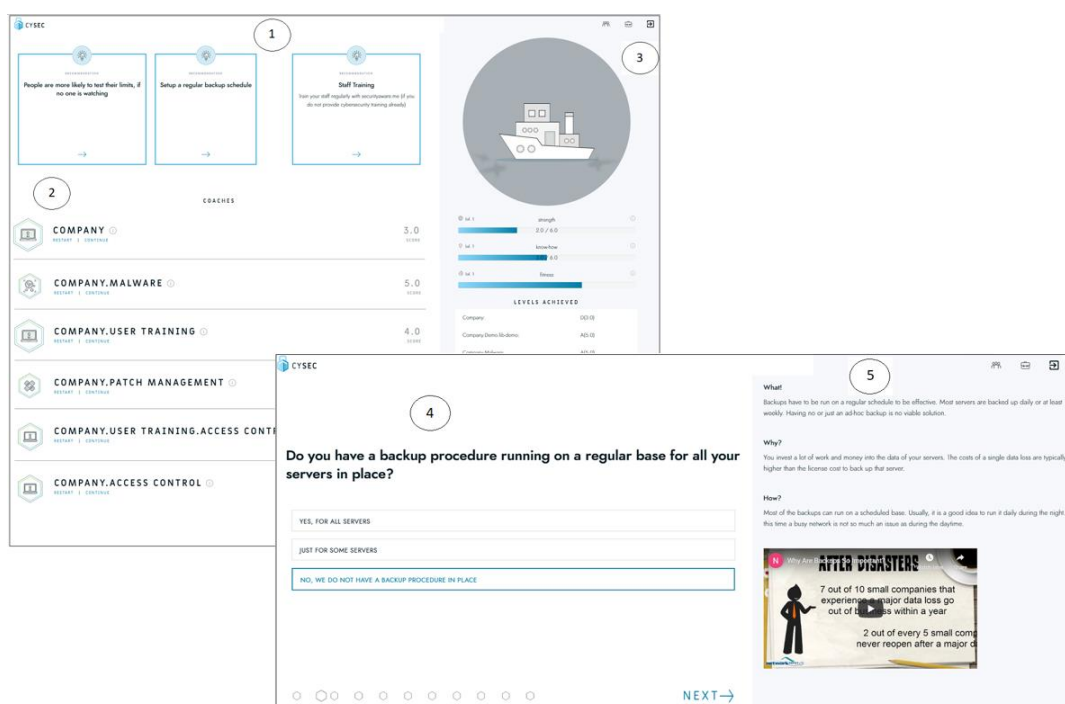


Figure 38: CYSEC dashboard and work area

The aim of the dashboard is to provide the SME end-user with an overview of capability areas of relevance for the SME, offer recommendations about the next steps, and show KPIs about how well the SME is doing in cybersecurity. In the dashboard, there are (1) recommendations for next improvements, (2) access to capability areas, and (3) KPI-based summary information about the company progress based on the SME’s answers to the self-assessment questions (strength), the number of visited questions (know-how), and the amount of user interaction with the tool during the last month (fitness).

The aim of the work area is to guide the SME end-user step-by-step through self-assessment and recommended good practices, controls, and tools for improving the SME’s awareness of threats and how these threats can be countered. In the work area, CYSEC offers (4) self-assessment and, (5) and

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	61 of 115
Reference:	D5.5	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

embedded security awareness and training content, including awareness-raising videos, pictures, and texts for educating threats, vulnerabilities, and countermeasures. Training content indicates the threats or vulnerability, why it is important, and how the use case can take a countermeasure.

Table 19 shows the scope of cybersecurity threats, vulnerabilities, controls, and practices that was supported by the CYSEC tool in use by the SMEs. This scope was offered through thematic coaches that corresponded to the capability areas company, malware scanning, user training, patch management, access control, and backup.

Table 19: A detailed list of threat, vulnerabilities, and security controls for refreshing interviewees' minds

Threats
Disaster, malicious insider, Downloading App from a not-trusted store, Ransomware, using just a simple password, no backup procedure (regular backup), phishing emails, not encrypted password communication (client-server)
Vulnerabilities
Shared password, [Malware] Scanning ALL files/software (Windows, Mac, iOS, Linux), disabling anti-malware, forget monitoring anti-malware signature, forget software with manual patching, giving admin rights to all, forget reboot after patching, using weak passwords, forget clearing access permission for offboarding employees, lack of spare parts for critical systems
Selected controls and practices
Blocking malicious websites, updating malware scan regularly (Windows, Mac, iOS, Linux) Scanning emails on server (for anti-malware) Training [protection against malware, what to do after detection] [Training for all staff] [GDPR][Evaluation] Having a checklist of threats Having a list of authorized software, having a store, monitoring anti-malware signature /policies Having a CISO, having a data protection officer Having a CSIRT (cybersecurity incident response team) Enabling automated patching for ALL servers/application Inventory of patching, newly produce devices patching, automated patch management, having a rollback plan schedule patch days, Enabling 2FA, implement the principle of least privilege, password policy, review access permissions, log access attempts, remote access policy, monitor network traffic, verifying created backup, multiple copies of backup files

4.5.2.2 Proposed impact of CYSEC on SME awareness

Albrechtsen [7] indicates that security awareness is *the extent to which organisational members understand the importance of information security, the level of security required by the organisation and their individual security responsibilities*. Based on Bulgurcu et al. [8], information security awareness (ISA) has two key dimensions and is defined as *an employee's general knowledge about information security and his cognizance of the information security policies (ISP) of his organization*. General information security awareness is *an employee's overall knowledge and understanding of potential issues related to information security and their ramification*. ISP awareness is *an employee's knowledge and understanding of the requirements prescribed in the organization's ISP and the aims of those requirements*. Also, we considered perceived usefulness (PU) as an antecedent of cybersecurity adoption in each use case's company. PU is defined as *the degree to which a person believes that using a particular system would enhance his/her job performance* [9]

To evaluate CYSEC, we focused on the tool's awareness-raising impact along with the following awareness-impact propositions.

- (1) The display of capability areas relevant for the SME provided users with a holistic view of the important cybersecurity capabilities to build. This display was expected to increase the SME end-user general knowledge about information security.
- (2) Self-assessment questions introduce security concepts and capture users' attention to important security threats, vulnerabilities, and practices. These questions were expected to increase the

SME end-users understanding of the importance of cybersecurity and general knowledge about information security.

- (3) Embedded training content described, and explained good cybersecurity practices, presented the importance of security threats and matching countermeasures. Training content included videos, statistics, pictures, and links to relevant websites, training courses offered in SMESEC securityaware.me, and quick self-assessment tools. This training content was expected to influence the SME end-user general knowledge about cybersecurity and the individual's security responsibilities. While CYSEC did not offer immediate support for communicating the SME's self-designed security policies, it communicated broadly established policy recommendations adapted to SMEs.
- (4) The KPI-based summary information in the dashboard gave a general overview of the company's progress. It offered continuous feedback and motivation to persist in pursuing the capability and manageability improvement journeys. This feedback was expected to influence the SME end-user understanding of the level of security still required by the organisation.
- (5) Recommendations based on the users' answers to the self-assessment questions allowed dynamic tailoring the steps followed along the SMEs' capability and manageability improvement journeys. This tailoring was expected to increase the perceived usefulness of CYSEC in comparison to static recommendations.

4.5.2.3 Evaluation of CYSEC impact of SME awareness

Based on the presented awareness-impact propositions, we evaluated the impact of CYSEC by collecting data about the SMEs' cybersecurity awareness and studied how CYSEC changed the awareness. Also, we reflected with these SMEs how usefulness and impact of CYSEC could be even further enhanced, paving the way towards future market-readiness of CYSEC as a product.

This section presents the impact of CYSEC on the OpenCall SMEs' awareness improvement and cybersecurity adoption. The presented results were gathered using three methods: 1) observation in the first workshop meeting with six OpenCall SMEs, 2) paper-based survey reported by eight OpenCall SMEs, and 3) structured interviews with five OpenCall SMEs. The names of the companies have been kept anonymous to ensure confidentiality.

4.5.2.4 Method

The aim of the here presented study was to evaluate if CYSEC enhanced use case partners' awareness. The study sought to answer the following research questions.

RQ1: How do the SMEs build cybersecurity awareness improvement when assisted with the CYSEC cybersecurity coach? RQ1 reflects the impact of actual usage of the CYSEC on cybersecurity awareness improvement. This question wants to assess how the tool helps SMEs in the journey of cybersecurity awareness improvement and if the tool usage has made any changes in the organisation awareness improvement process.

RQ2: How should the CYSEC method be adapted to maximise impact on SMEs? RQ2 evaluates the users' needs and missing features in the context of security awareness improvement after experiencing the tool's actual usage. This question wants to discover users' needs after using the tool. In fact, to find out how CYSEC can effectively facilitate the security awareness-raising process in SMEs.

RQ3: Do the SME end-users perceive CYSEC to be useful as a tool assisting cybersecurity assessment and awareness improvement? RQ3 aims at understanding the users' attitudes about tool acceptance and usefulness. This question wants to know users' attitudes by evaluating the acceptance and perceived usefulness of the tool. Usefulness is a significant factor for tool adoption.

For answering the research questions, we allowed the SMEs to use the CYSEC tool over a prolonged time (September 9, 2019 - January 31, 2020).

Three data collection methods have been used: a) observation at the beginning of the OpenCall period, b) questionnaire-based survey after the SMEs' extended use of the CYSEC tool in the SME's operational

Document name:	D5.5 Open Call Design, Implementation and Results Report			Page:	63 of 115
Reference:	D5.5	Dissemination:	PU	Version:	1.0
				Status:	FINAL

environment, and c) structured interviews after the SMEs' extended use of the CYSEC tool in the operational environment. The survey data was collected in February 2020, and all subjects confirmed that they had applied the tool. The final interview used for data collection about CYSEC impact was in May 2020.

Observation. The first data source is based observation method on the initial open call workshop in Heraklion, Greece (FORTH_Hellas), on September 9-10. Six OpenCall SMEs participated in the meeting and used the CYSEC (four the available coaches at that time with limited recommendations and questions). In the workshop, each SME representative characterised their companies, and later, the FHNW member introduced the tool, run a short training, and explained the meeting's objectives. Then the subjects had time to use the tool. During the meetings, the FHNW member observed the tool usage and took some notes and subjects' comments.

Survey. The second data source is based on the SMEs' answers to the final paper-based survey questionnaire. The survey included 12 questions, and the SMEs could reflect their experience during the open call period (September 9, 2019 - January 31, 2020) and explain the advantages and disadvantages of the CYSEC. Eight SMEs answered the survey. Table 20 illustrates the survey questions.

Structured Interview. The third data source is based on structured interviews with five OpenCall SMEs. The interviews conducted based on the preliminary analysis of the gathered data (sources 1 and 2) and after the open call period. A request for the final online interview has been sent to all OpenCall SMEs, and five SME accepted. All interviewees could find a suitable time. In the interviews, the screen of the interviewer's computer was shared, and the interviewees were able to see and read the content and had enough time to think about the answers. Moreover, they could see the interviewer's notes and correct them (if needed). All the interviews were conducted without distraction.

Each interview started with an explanation of the objectives. Then the interviewer explained the topics for the interview, the questions, and two lists of security threats, vulnerabilities, and security controls that have been introduced in CYSEC. The lists of threats and controls helped interviewees to refresh their minds and provide the interviewer precise answers. All interviewees used the lists during the interviews. To collecting honest responses, the interviewer emphasised that the collected data would be applied anonymously for academic purposes or deliverable D5.5 and obtained the subjects' consent. Table 20 presents the questionnaire for the interviews.

Table 20: CYSEC evaluation survey questionnaire

ID	Questions
S1	Have you been aware of the threats and vulnerabilities identified in the CYSEC? <i>Low, Rather low, Medium, Rather high, High</i>
S2	Which questions were difficult to understand even after reading the training content part (right-hand side of each question)?
S3	For which questions (and in which coaches) is the relevant training content complicated (non-practical, challenging to implement, difficult to understand)?
S4	How many questions did provide you with the security controls you have not implemented in your company?
S5	How do you evaluate the quality of the information in the training content? <i>Low, Rather low, Medium, Rather high, High</i>
S6	(based on question #5) Please delineate your reasons?
S7	What problems did you encounter while using CYSEC?
S8	Does the training content send a clear message about the severity and vulnerability of threats? <i>Low, Rather low, Medium, Rather high, High</i>
S9	How easy is applying CYSEC? <i>Low, Rather low, Medium, Rather high, High</i>
S10	How useful is applying CYSEC to improve your security awareness and capability? <i>Low, Rather low, Medium, Rather high, High</i>
S11	What are the main advantages and disadvantages of CYSE?

S12	Which parts of training content in the right-hand side of the questions (video, text, statistics, more information link, integrated training content links) are practical? Why?
-----	---

Table 21: The questionnaire template for the structured interview with the use case partners

Impact of CYSEC	
<i>Threats and Vulnerabilities</i>	
1	What threats or vulnerabilities have not you been aware <u>before</u> using CYSEC?
2	What threats or vulnerabilities have you been aware <u>before</u> using CYSEC?
3	What threats or vulnerabilities are missing in CYSEC?
4	What threats or vulnerabilities are irrelevant to your company but still suggested by CYSEC?
<i>Controls and Practices</i>	
5	What security controls and practices have you implemented now and not before CYSEC?
6	What security controls and practices have you already implemented before using CYSEC?
7	What security controls and practices are missing in CYSEC?
8	What security controls and practices are irrelevant to your company but still suggested by CYSEC?
Impact Creation	
9	In which situation or circumstances is CYSEC most useful?
10	How would you measure or assess the impact of CYSEC on your organisation?
11	To what extent do you agree with the following? CYSEC had a significant impact on the security of our company: 5 - fully agree, 4 - agree, 3 - neither agree nor disagree, 2 - disagree, 1 - fully disagree
12	Why, respectively, what should be done to improve?

4.5.3 Results

Table 22 gives an overview of the OpenCall SMEs' demographics. The SME identifiers are consistently used throughout the rest of the results' description.

Table 22: OpenCall partners demographics

ID	Size	Offices	Maturity (based on CYSEC security topics)	Subject cybersecurity experience	Structure
1	Small	3	IT industry and security (aware of all, implemented some)	Some years	Horizontal structure
2	Small	2	Health care (aware of some, implemented some)	Some years	CEO, chief medical officer, legal counsellor, head engineer, support engineers, community manager, behavioural scientist, designer
3	Small	1	IT industry (aware of all, implemented some)	Some years	CEO, employees
4	Small	2	Cybersecurity company (aware of all, implemented some)	Expert	CEO, developers, technical director, sales manager
5	Small	1	IT industry (aware of some, implemented some)	Some years	Horizontal structure

6	Small	1	IT industry (aware of all, implemented some)	Expert	CEO, technical director, project managers, developers
7	Small	1	IT service provider (aware of all, implemented some)	Some years	CEO, employees
8	Small	1	Security consulting company (aware of all, implemented some)	Expert	CEO, employees

Heraklion Workshop Results. The users selected coaches in different orders. The users referred to the training content when they were not able to understand the actual goal of the questions or only to find a specific issue. The users wanted each question to be answerable with suitable options for the response that explained their requirements precisely. Table 23 described the Heraklion workshop results, which we obtained from six of the SMEs.

Table 23: Observation and Feedback from the Heraklion workshop

ID	Observation, Feedback
SME 1	User scrolled through the training content part when they had a problem understanding some topics, questions, or options. The user moved between questions to compare the topics. <i>Some questions need more options.</i>
SME 2	<i>Privacy issues (data of patients) are more important for us than security topics.</i>
SME 3	The user scrolled through the training content part to understand some new concept (e.g., CSIRT) <i>I am aware of these threats/vulnerabilities, no new concepts. You can have some questions about security communication, Bluetooth, and mobile communication.</i> <i>It [CYSEC] should be more user friendly</i>
SME 4	The user had a problem with the language. He used Google translator several times
SME 5	User scrolled through the training content part to understand some new concepts. <i>I want that the tool automatically after each answer moves forward.</i> <i>We have security controls, but they are not documented</i>
SME 6	<i>The tool reminds us of what we need to do.</i> <i>You can improve the gamification elements.</i>

Survey Results. Table 24 demonstrates the collected data through the survey. We organised the answers based on the survey questions. Some of the questions are based on a five-level Likert scale (low, rather low, medium, rather high, high). One company (ID7) provided feedback with two perspectives: 1) the company itself [C] and 2) its standard customers [SC].

Table 24: Survey results

Question	SME	Feedback
S1: SMEs' Threat, Vulnerability Awareness	SME1	Rather High
	SME2	Medium
	SME3	Rather high
	SME4	High
	SME5	Medium
	SME6	High
	SME7	C: high SC: Rather low

	SME8	Rather high
S2: Complexity of the Coaches' Questions	SME 1	None. The training content was helpful to understand the not so clear questions
	SME 2	Almost none.
	SME 3	None
	SME 4	None
	SME 5	None
	SME 6	Few
	SME 7	C: no one SC: many. The training content part helps a lot; however, the SMEs people know ICT topics superficially only. Sometime the right-hand side is empty. For instance, the following questions are almost incomprehensible for not ICT experts. “Do you subscribe to a CVE website RSS”, “Do you implement the principle of least privilege” - The questions are understandable by ICT people only. - The questions are useful, but they should be more “decoded” into a normal language.
	SME 8	I would say that the 10% of the questions are not understood. Reasons: - Some questions take it for granted some issues (i.e. knowing about cybersecurity rules.) - Others in questions 9.
S3: Training Content (complicated, non-practical, difficult to understandable)	SME 1	None. It would actually be nice to have it in all questions. Even a short paragraph would be fine because when not available it gives the impression that the training is missing/broken
	SME 2	Many questions which were related to organisational processes were not practical and/or non-applicable.
	SME 3	We believe that question about a chief information security officer (CISO) and CSIRT in one of the coaches not relevant to a SME.
	SME 4	None.
	SME 5	None.
	SME 6	None in particular
	SME 7	C: none SC: Some topics are more known, for instance, malware, some others are more technical as, for instance, patching “Have you enabled automated patching for all services interfacing to the internet?” - SMEs entrepreneurs don't know DNS or DHCP and so on. Generally, in a “standard” micro and small company there are no one who is in charge to manage patching. The questions are useful, but they should be more “decoded” into a normal language (Fig. 6)
	SME 8	The course should define FIRST: - What Operating systems users define? - What characteristics, properties users define And according to that generate the questions. This is done because there are questions regarding some OS that the does not apply to the user.
S4: Security Controls have not	SME 1	Between 5-10
	SME 2	About 1/3 rd .
	SME 3	Dozen.

Implemented (introduced by CYSEC)	SME 4	Approximately 10 controls, which we can't or don't want to implement, because of our infrastructure or business we are doing.
	SME 5	7
	SME 6	Around 12
	SME 7	C: the company has implemented all applicable security controls directly or indirectly on Linux and Windows systems. It doesn't use iOS and Android OS. SC: most of the security controls are implemented by external ICT suppliers, in many cases the implementation level is rather low.
	SME 8	We would say the 30% for the questions were not implemented by us.
S5: Quality of Training Content	SME 1	Rather High
	SME 2	Rather high
	SME 3	Medium
	SME 4	High
	SME 5	Medium
	SME 6	Rather High
	SME 7	Rather High
	SME 8	Some errors (company): <ul style="list-style-type: none"> - Question in digital offering there is nothing being showed - Same for Operating systems in servers About questions and missing answers <ul style="list-style-type: none"> - Example: Does your company have an experienced CIRT? From possible answers we should add: It is outsourced. (Malware): <ul style="list-style-type: none"> - What if we don't have MAC? That should we select in multiple choice? "No, we do not" but it because we don't have, not because we don't scan...Same IOS - Questions of "Do you monitor..."? I have a third party subcontracted to monitor them (add this answer.) - When I click in the final question to NEXT button it doesn't work. (Access control) <ul style="list-style-type: none"> - Questions related to SMEs that develop software but most SMEs don't develop software. - "When do you force your users to change their passwords?" this question needs more answers - "Are passwords sent encrypted?" that can't be answered by a SME (at least in 95%)
S6: Detailed evaluation of the Training Content Quality	SME 1	N/A
	SME 2	The information appeared reliable, and generally interesting.
	SME 3	The content is suited rather for big organizations and not really for start-ups like ours.
	SME 4	It was all clear.
	SME 5	Information was generic and not always relevant.
	SME 6	There were suggestions included in ways to further mitigate security risks that not only are not incorporated in our company but that we never really thought of implementing.
	SME 7	All the selected topics are important, training contents are professional and well done from technical point of view.
	SME 8	Questions not understood <ul style="list-style-type: none"> - Do your android clients use only play store and your company store to download apps? Don't understand this question. - There are many questions related to Linux, windows, mac and the answers don't cover the option of saying that you are NOT using these machines...(example we don't have WServers. We select "NO WE DO

		<p>NOT?" → it is not correct, because when you select that you are referring that you don't scan, not that you don't have those devices.)</p> <ul style="list-style-type: none"> - "Did you consider the cybersecurity rules that apply for your company when you selected the training?" what cybersecurity rule are you referring to? Nobody in SMEs knows about cybersecurity rules (unless they work for cyber sector)
S7: CYSEC Usage Problem	SME 1	<ul style="list-style-type: none"> -Some questions didn't have all possible answers, e.g. for some a 'N/A' option should exist. -The percentages in results should have better formatting (e.g. no more than 2 decimals) and better checks when calculating (I had 200% of recommended actions in Company coach) (Fig. 7) -Some graphics (result bars) and images were broken in various coaches. -The score in the overall dashboard is a bit unclear. Initially it seems that higher is better (i.e. 5.0 is best) but looking carefully on the right side at the 'levels achieved' widget there are some A, B, C grades with no clear correspondence to numerical scores. (Fig. 7) -The 'Coach company, malware' didn't respect OS choices made in previous coach and displayed questions for all OS's, even though it was stated otherwise -Proof Reading would improve language of some questions -System performance unstable from time to time -Recommendation in main dashboard point to dead links -Unlocked badges section seems broken (Fig. 7)
	SME 2	Some intermittent problems with access and user interface/user experience.
	SME 3	Technical issue related to functionality of the system (Problem with Dashboard logging, not possible to complete the coaches, etc.)
	SME 4	Reading the content part. It is not easy to read all information by going other web pages for more info.
	SME 5	It was not working at the beginning. We needed to troubleshoot a couple of times to get it to work.
	SME 6	A few times we had trouble connecting (the site/page was timing out).
	SME 7	We didn't encounter any particular problems in using CYSEC tool.
	SME 8	<ul style="list-style-type: none"> - Problems with understanding some questions - Usability problems
S8: Training Content message of the Severity, Vulnerability of Threats	SME 1	Rather High
	SME 2	Rather low
	SME 3	Rather high
	SME 4	Rather high
	SME 5	Rather high
	SME 6	High
	SME 7	High
	SME 8	Rather high: the right part describing the questions is a very useful part defining examples of vulnerabilities and severity.
S9: CYSEC Ease of Use	SME 1	High
	SME 2	Medium
	SME 3	Rather high
	SME 4	High
	SME 5	Medium
	SME 6	High
	SME 7	Rather high
	SME 8	Rather high

S10: CYSEC Usefulness	SME 1	Rather High
	SME 2	Medium
	SME 3	Medium
	SME 4	High
	SME 5	Medium
	SME 6	Rather High
	SME 7	C: Low because we were already aware of the cyber risks and of cybersecurity issues. SC: Rather high, because mimicking our customers we became more aware of their vulnerability.
	SME 8	Rather high
S11: CYSEC Advantages, Disadvantages	SME 1	Advantages: Easy to use, one place concentrating introductory material and pointers for security-related issues, gamified approach Disadvantages: Tool lack stability and robustness, scoring and levels should be more self-explanatory- numerical scores, letter grades, levels, badges and properties (e.g. fitness) seem quite mixed and confusing.
	SME 2	It is a good reminder of basic principles and good practices. Its format is useful as it is interactive and non-imposing. On the other hand, it appears rigid and not always applicable or tailored to SMEs.
	SME 3	Advantage: gives a good overview of cyber threats. Disadvantage: content not correctly adapted to small companies.
	SME 4	It is good to reach from a framework and ensures awareness of the controls, even we did not implement willingly.
	SME 5	The advantage is that it gives you comprehensive information in holistic way. However, it is often too generic.
	SME 6	Main advantages are the complete manner that it addresses individual security risks and relative solutions.
	SME 7	Potentially CYSEC is a good tool to increase the awareness and improve the expertise of ICT professionals and ICT micro companies which supply ICT services and system/hardware maintenance to SMEs but that are not cybersecurity experts. It is less useful, perhaps no useful to cybersecurity experts and it is, somewhere too complex for ICT user SMEs. Maybe it could be useful to split CYSEC in two tools one for SMEs without internal IT experts and a second one for more structured companies with internal IT service.
	SME 8	Advantages: questions that must be answered make the SME to be aware of its own status. Disadvantages are that CYSEC doesn't expose a roadmap of how the SME should mitigate their vulnerabilities once the answers are completed.
S12: Effectiveness of the CYSEC Training Features	SME 1	The overall approach including intro, links and videos seems quite helpful. Following the same approach for all questions would rather make the user feel more comfortable and the tool look more smooth and complete.
	SME 2	For passive consumption (like a feed), statistics are quite practical because they alert us on various topics with simple ways. Videos and text may require more time, and it is natural for many not to be of interest – hence reducing the tendency for the average viewer/user to refer to them.
	SME 3	The text was more appreciate, as an easy and fast way to understand the first idea of the message.

	SME 4	Everything was practical other than the more info. It makes person to forget the main objective. They can be given as a reference instead.
	SME 5	Mainly text because I do not remember seeing any video.
	SME 6	The most practical and needed were explanations of abbreviations of terms we had never come across.
	SME 7	Videos are the most practical tools. A video conveys better the content, it is more emphatic and pleasant. The real problem of CYSEC videos is the language. English could not be a problem for ICT experts however it may be a real problem to disseminate information across Europe. In many cases the language is a great barrier.
	SME 8	Right part: -Very useful to include practical examples for answering the questions to be answered -Not too many videos which is ok (not very heavy) -I would include more significative graphics -In back-up coach there were not contents on right part.

Interview Results. In this part, we present the interview results for five OpenCall SMEs (SME 1, SME 2, SME 5, SME 7, and SME 8).

Interview results for SME 1. Table 25 gives an overview of the SME 1 opinions about the CYSEC impacts on cybersecurity awareness-raising in the company. The SME confirmed that it had worked with CYSEC. The interview lasted 23 minutes.

Table 25: SME 1 interview results

Impact of CYSEC		
<i>Threats and Vulnerabilities</i>		
#	Question	Subject Statement
1	Not aware before?	'- (we are working in the security context)
2	Aware before?	We knew all of them
3	Missing in CYSEC?	It is complete. I do not see that sth is missing,
4	Irrelevant but still suggested?	I do not see any irrelevant; I think some of them do not apply to our company. They are valid, but we are a small company and do not have, for example, a data protection officer.
<i>Controls and Practices</i>		
5	Implemented now and not before?	In some degree, I can say training, because it is almost in the plan, but using CYSEC boost us (Motivate) to implement these training
6	Already implemented before?	Blocking web, updating malware, scanning email on servers, list of authenticated software, monitoring, automatic patching for all servers, least privilege, password policy access control, access permission review, log access attempts, monitor net traffic, multi backup file, (specifically for us: we are not using a public file server, google drive, Dropbox, we use ours, we believe it is less risky, for privacy mostly and not security.)
7	Missing in CYSEC?	-
8	Irrelevant but still suggested?	some of them are not applicable (such as data protection officer), but relevant
<i>Impact Creation</i>		
9	CYSEC most useful?	Most useful for the new members of the company, it gives quick training and view of all threats, we let them know, do the CYSEC assessment we see their results, and we update them.
10	How would you measure the impact?	some of our employees proceeded secure password in all their accounts, we know that it should be fixed and after using the tool, we updated the passwords, for the password it was easy to measure and validate that it affected us

11	CYSEC impact rate.	3 , because we are in the context of cybersecurity and we are aware. <i>5 - fully agree, 4 - agree, 3 - neither agree nor disagree, 2 - disagree, 1 - fully disagree</i>
12	Why? What should be done?	Having a list of the latest threats and security vulnerabilities. The most recent things, to keep us update to be interesting for the company, for instance: to know a new list of password leaks, a list of website compromised, to be sure about our passwords, to change our password, to have it as soon as it is going to be published, and some example of attacks

The subject stated that CYSEC motivated them to plan for training and update the password, which can show the impact of the tool and both cybersecurity intention and actual behaviours. Moreover, the subject indicated that the tool is most useful for the new member to assess their awareness. Also, the subject suggested that the training content parts need to cover the most recent security threats news.

Interview results for SME 2. Table 26 gives an overview of the SME 2 opinions about the CYSEC impacts on cybersecurity awareness-raising in the company. The SME confirmed that it had worked with CYSEC. The interview lasted 29 minutes. Two interviewers participated in this interview.

Table 26: SME 2 interview results

Impact of CYSEC		
<i>Threats and Vulnerabilities</i>		
#	Question	Subject Statement
1	Not aware before?	Social engineering
2	Aware before?	We were aware of most of them, but not actively thinking of them; however, after it [CYSEC] we decided and have planned to improve the process of password recycling, the process of backups,
3	Missing in CYSEC?	Protection of computer screens
4	Irrelevant but still suggested?	-
<i>Controls and Practices</i>		
5	Implemented now and not before?	-
6	Already implemented before?	Patch mechanism, a trojan detection module, encryption at rest
7	Missing in CYSEC?	Password mechanism for cloud systems in a network level (cloud-based SMEs security), employees phone usage for emails and the email is not encrypted on the device,
8	Irrelevant but still suggested?	-
<i>Impact Creation</i>		
9	CYSEC most useful?	I think CYSEC is useful. It would be more useful and usable by SME if it included more about cloud-based SMEs (hardware is managed by others, the physical security is managed by others)
10	How would you measure the impact?	-
11	CYSEC impact rate.	Yes/No, more accurately depends (SMEs are very diverse) We are an SME with a very good understanding of technology, and we use cloud services 2.5 (slightly disagree), because it was not very applicable to us, the hardware that we use for the services they are managed by third parties and the network is also set up by them, so there is not something we can do. <i>5 - fully agree, 4 - agree, 3 - neither agree nor disagree, 2 - disagree, 1 - fully disagree</i>
12	Why? What should be done?	If CYSEC extended with a coach that focuses on managing the service delivery of third-party cloud providers and provides more personalised questions/content (e.g., cloud services, what kind of users have access to the service), then CYSEC becomes useful for the company Having reminder and capabilities but in a non-distracting way

The subject stated that CYSEC was not very applicable to the company because third-parties manage the hardware and network.

Interview results for SME 5. Table 27 gives an overview of the SME 5 opinions about the CYSEC impacts on cybersecurity awareness-raising in the company. The SME confirmed that it had worked with CYSEC. The interview lasted 27 minutes.

Table 27: SME 5 interview results

Impact of CYSEC		
<i>Threats and Vulnerabilities</i>		
#	Question	Subject Statement
1	Not aware before?	software automated patching
2	Aware before?	all of them (except for auto-patching)
3	Missing in CYSEC?	Coaches about physical security for servers, laptops, infrastructure, malicious insider, stealing, destroying
4	Irrelevant but still suggested?	“a spare part for critical systems” is not relevant now, since we use the cloud, however, maybe in future it is relevant to us, totally I think everything is relevant
<i>Controls and Practices</i>		
5	Implemented now and not before?	Semi-automatic update and training. Because of SMESEC in general, but I cannot say only because of CYSEC.
6	Already implemented before?	malware scanning, block malicious websites, scanning emails, 2FA, encryption of databased and laptops, backup, access management,
7	Missing in CYSEC?	Physical vulnerability, physical security controls, security event management, (Atos tool), automated vulnerability assessment, for cloud infrastructure and other things relevant to web
8	Irrelevant but still suggested?	-
Impact Creation		
9	CYSEC most useful?	It should be customizable (not general), giving specific suggestion based on our infrastructure, the specific suggestion about security solutions and their costs (free solution, paid solutions)
10	How would you measure the impact?	It made an impact, but at the beginning of the open call period, there were some problems. We did not have enough time to use. We supposed to have more time to go through the information, Also, we cannot quantify the impact because we do not have KPIs for cybersecurity measurement.
11	CYSEC impact rate.	2. Because firstly, the time was not enough to evaluate it, and the maturity of the tool was not enough, and the maturity of the organisation of cybersecurity was not high 5 - <i>fully agree</i> , 4 - <i>agree</i> , 3 - <i>neither agree nor disagree</i> , 2 - <i>disagree</i> , 1 - <i>fully disagree</i>
12	Why? What should be done?	I needed more time for the usage of the tool. The tool should provide some specific solutions and prioritisation, The tool should give most important suggestions and an action plan for the next six months

The subject indicated that the lack of time for the usage of the tool, general (not customised) solutions and training content, and the level of maturity of the tool had (usage problems) impacted on his evaluation.

Interview results for SME 7. Table 28 gives an overview of the SME 7 opinions about the CYSEC impacts on cybersecurity awareness-raising in the company. The SME confirmed that it had worked with CYSEC. The interview lasted 45 minutes. SME 7 answered some of the questions with two perspectives: 1) the company and 2) its customers

Table 28: SME7 interview results

Impact of CYSEC		
<i>Threats and Vulnerabilities</i>		
#	Question	Subject Statement
1	Not aware before?	The company: aware of all The company customers: almost not aware of all (since they are not working in the area of cybersecurity and ICT)
2	Aware before?	The company: all, antimalware, backup, patch management for OS, (we do not use Mac), block malicious website ..., The company customers: they are not focusing on IT dangers, problems at all, the tool could be used for them to understand different threats. External companies protect them.
3	Missing in CYSEC?	Physical security, both personal computer and server, network, mobile phone, and laptops, customers do not think about screen saver password, mobile password. They forget to protect the office physically (damage, stolen, network protection) the customer has a backup, but the backup is in the same office close to the servers.
4	Irrelevant but still suggested?	I do not think there is anything irrelevant in general. The questions can be irrelevant to some case, if I use Linux, mac is irrelevant to me, but it is important as general. We are network professionals; we do not have employees and do not use training for employees. However, in general, training is very important.
<i>Controls and Practices</i>		
5	Implemented now and not before?	We have not changed anything after using CYSEC.
6	Already implemented before?	We have the policy to protect against cyber threats. We review our policy 2-3 time a year in an internal meeting to change, for instance, the rules, our servers are protected by our providers.
7	Missing in CYSEC?	physical protection
8	Irrelevant but still suggested?	All is relevant, and we cannot see something is irrelevant but depends on the situation
Impact Creation		
9	CYSEC most useful?	CYSEC is useful to review and check if everything is OK or not, a complete review of cybersecurity issues, To be most useful, consider the completeness of the tool and provide for every topics training content and videos.
10	How would you measure the impact?	We have not received too much impact internally. We used your tool to review our policy. I do not think there was any impact. We used the tool as a list to review cybersecurity topics,
11	CYSEC impact rate.	3 , because the CYSEC has no impact on our company directly, we knew already all threats and controls <i>5 - fully agree, 4 - agree, 3 - neither agree nor disagree, 2 - disagree, 1 - fully disagree</i>
12	Why? What should be done?	in my opinion, we can answer from the customer point of view: CYSEC is useful for some ICT companies and some non-ICT, more than for us, 1-the tool should be complete, and all questions should have training content, 2-translate coaches in different languages because most SMEs have difficulty in using English and learn in English. To spread the tool and improve awareness, it is necessary to have it in different languages. 3-your target should not be cybersecurity and ICT companies,

The subject indicated that the tool was useful for them to review cybersecurity threats and issues. He explained that the coaches and content are relevant to SMEs in general; however, the tool should also satisfy the non-ICT SMEs' requirement. Moreover, to improve security awareness, having the coaches in different languages is important.

Interview results for SME 8. Table 29 gives an overview of the SME 8 opinions about the CYSEC impacts on cybersecurity awareness-raising in the company. The SME confirmed that it had worked with CYSEC. The interview lasted half an hour.

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	74 of 115
Reference:	D5.5	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

Table 29: SME8 interview results

Impact of CYSEC		
<i>Threats and Vulnerabilities</i>		
#	Question	Subject Statement
1	Not aware before?	-
2	Aware before?	All, we are experts in cybersecurity, we develop solutions for others
3	Missing in CYSEC?	Navigating through browsers bad behaviour to fight and report bad behaviour
4	Irrelevant but still suggested?	Disaster is difficult even though possible, do not use Mac or iOS in an industrial context
<i>Controls and Practices</i>		
5	Implemented now and not before?	Nothing, All applicable instead of automat patching
6	Already implemented before?	Backup, antivirus, anti-malware, patches, for the white list we have a policy, incidents handler is out-source, we have not enabled 2FA, but we have a policy, incidents handling is expensive
7	Missing in CYSEC?	Network segmentation, it is important for vulnerability management,
8	Irrelevant but still suggested?	Personal data protection officer
Impact Creation		
9	CYSEC most useful?	CYSEC is good for the prevention time, providing this tool before something happen,
10	How would you measure the impact?	It is not easy to navigate the impact, We had a test approach, first time, after one month we put test, some employees have been selected for the test, and after one month, we assess the employees, we are more prepared. We are aware of all these attacks, CYSEC increased employees' awareness
11	CYSEC impact rate.	4 , because CYSEC clarifies and reinforces the improvement in processes, technical issues and people. 5 - fully agree, 4 - agree, 3 - neither agree nor disagree, 2 - disagree, 1 - fully disagree
12	Why? What should be done?	Improve the usability of the tool, the examples and questionnaires should be more concrete and more motivating

The subject indicated that the tool clarified the issues and considered the improvement aspects (people, processes, and technical issues). However, the tool should be more concrete and motivating (e.g., considering the usability issue and motivating factors, providing practical examples).

4.5.4 Analysis

In this section, we study the impact of CYSEC on cybersecurity awareness improvement and answer the research questions indicated in the method section based on the three data sources.

How do the SMEs build cybersecurity awareness improvement when assisted with the CYSEC cybersecurity coach? (RQ1)

CYSEC had no significant impact on the SME's security awareness improvement for the companies that were experts in cybersecurity, and the subjects have already had expertise in security. *SME7: "the CYSEC has no impact on our company directly; we knew already all threats and controls. The company has implemented all applicable security controls directly or indirectly on Linux and Windows systems. All the selected topics are important."* *SME8: "Nothing [security control] has been implemented after using CYSEC. We are experts in cybersecurity; we develop solutions for others."* *SME1: "We are in the context of cybersecurity, and we knew all of them."* *SME3: "I am aware of these threats/vulnerabilities, no new concepts."* However, SME7 from its customer points of view indicated that: "CYSEC is useful

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	75 of 115
Reference:	D5.5	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

for some ICT companies and some non-ICT, more than for us. Your target should not be cybersecurity and ICT companies.” CYSEC increased awareness about social engineering threat in SME2 and the possibility for automated patching in SME5.

However, the tool provided a holistic view of threats and security controls for the SMEs (indicated by SME3, SME4, SME5, SME6, SME7) for review. In addition, CYSEC had an impact on cybersecurity activities in the SMEs that have knowledge and expertise in security. The tool could help them reassess the security policy, clarify the improvement in processes, motivate to have security practices, and use for new employees. SME7: “CYSEC is useful to review and check if everything is OK or not, a complete review of cybersecurity issues. We used your tool to review our policy.” SME8: “CYSEC clarifies and reinforces the improvement in processes, technical issues and people.” SME2: “We were aware of most of them [threats, vulnerabilities], but not actively thinking of them; however, after it [CYSEC] we decided and have planned to improve the process of password recycling and the process of backups.” SME1: “I can say training [implemented after using CYSEC] because it is almost in the plan but using CYSEC boost us (Motivate) to implement these training.” SME1: “[CYSEC is] most useful for the new members of the company, it gives quick training and view of all threats, we let them know, do the CYSEC assessment, we see their results, and we update them.”

Do the SME end-users perceive CYSEC to be useful as a tool assisting cybersecurity assessment and awareness improvement? (RQ3)

Users evaluated the tool’s impact by responding to five-level Likert scale questions about the tool impact (5 - fully agree, 4 - agree, 3 - neither agree nor disagree, 2 - disagree, 1 - fully disagree). Table 30 shows the users’ scores.

Table 30: Perceived CYSEC usefulness based on survey and interview results (5 - fully agree, 4 - agree, 3 - neither agree nor disagree, 2 - disagree, 1 - fully disagree)

	average	SME1	SME2	SME3	SME4	SME5	SME6	SME7	SME8
Usefulness (Survey)	3.4	4	3	3	5	3	4	(C) 1 (SC) 4	4
Usefulness (Interview)	2.9	3	2.5	-	-	2	-	(C) 3	4

Two factors influenced the subjects’ evaluation of the tool’s usefulness.

Stability and Completeness. Since the development team was working on the tool during the open call period, some features and functionalities were not stable or available. Moreover, the users wanted to have training content for all questions. So, the tool stability and completeness were indicated by users. SME5: “It made an impact, but at the beginning of the open call period, there were some problems. So, the time was not enough to evaluate it. I needed more time for the usage of the tool. The maturity of the tool was not enough, and the maturity of the organisation of cybersecurity was not high.” SME7: “the tool should be complete, and all questions should have training content.” SME1: “It would be nice to have it [training content] in all questions. Even a short paragraph would be fine because when not available, it gives the impression that the training is missing/broken.” SME8: “error, question in the digital offering; nothing is being shown.” SME1: “The percentages in results should have better formatting (e.g. no more than two decimals) and better checks when calculating (I had 200% of recommended actions in Company coach.” SME2: “Some intermittent problems with access and user interface/user experience.” SME6: “A few times we had trouble connecting (the site/page was timing out).”

Content. Users needed customised, applicable, and easier-to-understand content. SME1: “I think some of them do not apply to our company. They are valid, but we are a small company and do not have, for example, a data protection officer.” SME2: “Many questions which were related to organisational processes were not practical or non-applicable. [About the quality of the training content] The information appeared reliable, and generally interesting.” SME7: “[tool usefulness from two points of view; the SME (C), and its customers (SC)]: C: Low because we were already aware of the cyber risks

and cybersecurity issues. SC: *Rather high, because mimicking our customers, we became more aware of their vulnerability.*” SME7: *“SMEs entrepreneurs don’t know DNS or DHCP, and so on. Generally, in a “standard” micro and small company, there is no one who is in charge to manage patching.”* SME5: *“The advantage is that it [CYSEC] gives you comprehensive information in a holistic way. However, it is often too generic. It should be customizable (not general); giving specific suggestion based on our infrastructure. Also, we cannot quantify the impact, because we do not have KPIs for cybersecurity measurement.”* SME7: *“training contents are professional and well done from a technical point of view. Videos are the most practical tools. A video conveys better the content; it is more emphatic and pleasant.”* SME2: *“it [CYSEC] was not very applicable to us; the hardware that we use for the services they are managed by third parties, and the network is also set up by them. Privacy issues (data of patients) are more important for us than security topics”* SME8: *“the right part [training content] describing the questions is a very useful part defining examples of vulnerabilities and severity. I would say that 10% of the questions are not understood.”* SME3: *“We believe that question about a chief information security officer (CISO) and CSIRT in one of the coaches [Company] not relevant to an SME. Content not correctly adapted to small companies.”*

How should the CYSEC method be adapted to maximise impact on SMEs? (RQ2)

In the open call study, we had a variety of users who are expert in cybersecurity or have good general knowledge about security. Also, all of them have long experience in IT. If CYSEC wants to maximise its impact on this group of users and SMEs, it needs to provide fresh, advanced, and personalised knowledge, capabilities, and recommendations. SME3: *“You can have some questions about security communication, Bluetooth, and mobile communication.”* SME2: *“If CYSEC extended with a coach that focuses on managing the service delivery of third-party cloud providers and provides more personalised questions/content (e.g., cloud services, what kind of users have access to the service), then CYSEC becomes useful for the company.”* SME1: *“Having a list of the latest threats and security vulnerabilities. The most recent things, to keep us update to be interesting for the company, for instance: to know a new list of password leaks, a list of website compromised, to be sure about our passwords, to change our password, to have it as soon as it is going to be published, and some example of attacks.”* SME5: *“The tool should provide some specific solutions and prioritisation. The tool should give most important suggestions, and an action plan for the next six months.”*

Also, considering the usability of the tool and users’ motivating factor increase the impact of CYSEC. SME6: *“You can improve the gamification elements.”* SME8: *“Improve the usability of the tool. The examples and questionnaires should be more concrete and more motivating.”*

Finally, CYSEC needs to support local languages to maximise its impact on security adoption and awareness improvement. We observed that the subject of SME4 had a problem with the English language understanding. He used Google translator several times to understand the questions and training content. SME7: *“translate coaches in different languages, because most SMEs have difficulty in using English and learn in English. It is necessary to have it in different languages, to spread the tool and improve awareness.”*

Table 31 shows the OpenCall SMEs’ opinions about the missing knowledge and capabilities in CYSEC.

Table 31: Missing knowledge and capabilities

SME	Missing Capabilities
SME 2	Protection of computer screens Password mechanism for cloud systems in a network level (cloud-based SMEs security), employees phone usage for emails and the email encryption on mobile devices
SME 5	Coaches about physical security for servers, laptops, infrastructure, malicious insider, stealing, destroying, Physical vulnerability, physical security controls, security event management, XL-SIEM, automated vulnerability assessment, for cloud infrastructure and other things relevant to web
SME 7	Physical security, both personal computer and server, network, mobile phone, and laptops, customers do not think about screen saver password, mobile password. They forget to protect physically the office (damage, stolen, network protection)
SME 8	Navigating through browsers bad behaviour to fight and report bad behaviour

Network segmentation, it is important for vulnerability management,

4.5.5 Overview of the impact

In summary, CYSEC depends on the SMEs' expertise, increased cybersecurity awareness (about some controls or threats), has been used for review and reassessment of the SMEs policy, implemented controls (through providing a holistic view), and training plans for the company members or the new employees.

Table 32. Impact after using CYSEC

SME	Impact after using CYSEC
SME 1	<p>[Training] In some degree, I can say training [implemented after using CYSEC], because it is almost in the plan, but using CYSEC boost us (Motivate) to implement these training.</p> <p>[New employees awareness improvement] CYSEC is most useful for the new members of the company, it gives quick training and view of all threats, we let them know, do the CYSEC assessment we see their results, and we update them.</p>
SME 2	<p>[Awareness] Social engineering</p> <p>[Intention and plan for security adoption] We were aware of most of them, but not actively thinking of them; however, after it [CYSEC] we decided and have planned to improve the process of password recycling and the process of backups</p>
SME 3	CYSEC gives a good overview of cyber threats
SME 4	<p>[Review and assessment] It is good to reach from a framework and ensures awareness of the controls, even we did not implement willingly</p>
SME 5	<p>[Awareness] software automated patching</p> <p>[Control] Semi-automatic update and training. Because of SMESEC in general, but I cannot say only because of CYSEC. It gives you comprehensive information in a holistic way</p>
SME 6	The complete manner that it [CYSEC] addresses individual security risks and relative solutions
SME 7	<p>[Review and assessment] CYSEC is useful to review and check if everything is OK or not, a complete review of cybersecurity issues. We used your tool to review our policy. We used the tool as a list to review cybersecurity topics.</p> <p>[The SME customers' point of view Awareness improvement] Almost not aware of all</p>
SME 8	<p>[Awareness] Questions that must be answered make the SME to be aware of its own status CYSEC increased employees' awareness</p> <p>[Impact on adoption] CYSEC clarifies and reinforces the improvement in processes, technical issues, and people</p>

4.6 Lesson Learnt

In this section, we summarize all the general conclusions based on the lessons learned section presented in all reports¹ received from the participants of Categories 2a and 2b.

¹ Full reports received from the Open Call participants can be found in the Annex of D7.4.

4.6.1 Summary and Conclusions for Category 2a

Challenges and technical issues faced(Pains):

- Fully understanding the functionality for each tool and its general role in the SMESEC framework. The Physical meeting in Heraklion as well as the bi-weekly meetings helped overcoming this challenge
- The installation difficulty for some of the tools, requiring specialized Linux administrative knowledge and significant communication and help with the tool owners, that was promptly given.
- Some discrepancies due to the on-going integration of the SMESEC tools in the platform whilst the initial period of the testing phase begun.
- Some minor downtime in individual tools of the SMESEC dashboard.
- Some of tools requirements were restrictive for the SME (e.g. the requirement for 2 IPs for CITRIX ADC, bridged-mode for FORTH's Cloud-IDS, large memory consumption of XL-SIEM)
- Some discrepancies were found between the training material and the actual installation process. Solved with the means of communication between the SMEs and the consortium, fixing the issue and providing newer versions of the training material.
- Beyond average IT skills is required to install some of the tools, needed direct assistance of the tool owners.
- Need to provide access to SME's servers in order to finalize the installation testing
- Not all cloud Environments were supported, needed to do the installation to the local machines/servers.

Positive aspects of SMESEC (Gains):

- Promoting SME's Cybersecurity growth
- The platform was great extend straightforward, and delivered what was promised.
- Study of the training material, installation guide provides info on more advanced tools and cybersecurity techniques
- Overall, the SMESEC project is an interesting proposition for SME companies and definitively worth to be consider as a full commercial product.
- The project proposal responded to our initial requirement and it might be worth to consider to be purchased as a universal cyber-protection solution in future.
- It informed SMEs about security in a very structured way
- It exposed the involved SMES to the state of the art of various tools, including new categories of tools which they were not aware of
- It helped Open Call SMEs improve our understanding of our own infrastructure and its security weaknesses.
- The CySec assessment and awareness tool as well as the training courses are just as interesting and helpful as the actual security tools.
- The "training courses and the awareness platform "is a very interesting offer of SMESEC project and at this point seems to be a promising prototype.
- The overall impact has been very positive for the SME. The engagement in the project increased significantly our security awareness.

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	79 of 115	
Reference:	D5.5	Dissemination:	PU	
	Version:	1.0	Status:	FINAL

Recommendations / Future improvements:

- Installation process should be improved, too complex at the moment for the “lambda” SMEs. it should not be necessary to hold a meeting
- Documentation should be more clear including common issues and troubleshooting(FAQ)
- A seamlessly integration process of the different components is needed, limiting the manual interventions from the users to the minimum.
- More and more adapted content in the trainings aligned with the proposed solutions and requirements
- The tools should be made available as “Software as a Service” or a similar mode, so that more SMEs can test and use them in a simpler and more efficient manner.
- Merge all tools’ dashboards to a single one

4.6.2 Summary and Conclusions for Category 2b

Challenges Identified in the process of integrated API:

- Understanding SMESEC API architectures and underline technologies
- Understanding of the API functionality and deciding on the proper module to integrate with our tool
- Design of the changes needed to each tool in order to include the necessary SMESEC functionality without interfering with existing operation of the tool
- Implementation of the required changes, testing and validation of the results
- Implementation of the security prerequisites of the SMESEC API and the following the testing procedure
- Integration seemed taking a bit more time than expected due to internal consortium time constraints
- Having experience in Java
- Certificate management
- Configuration of application.yml file
- More detailed description needed in the installation guides

These challenges were overcome by the following means:

- Participation to the physical meetings
- The provided training and communication tools by the SMESEC team.
- Reading the online documentation links provided e.g. <https://docs-adapter-tools.smesec.eu/architecture.html>.
- Participation in the online channels provided by SMESEC, namely the biweekly telcos, organized by the SMESEC technical team, including all Open Call participants
- Participating and using the project’s open call slack channel.
- Careful execution of the provided instructions and guides.
- Assistance provided in bilateral or group communications with the SMESEC team.
- New information/versions of the installation files were provided

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	80 of 115	
Reference:	D5.5	Dissemination:	PU	
	Version:	1.0	Status:	FINAL

- Improving JAVA-related skills and detailed guidance from the SMESEC team, concerning the REST API.
- Helpful and responsive support team for the external API

Recommendations for future improvements:

- Better testing of API's successful integration
 - Providing an online sandbox version of the tool to test proper communication and information exchange would help developers of external tools to quickly debug the integration procedure
 - Existing support methods provided by SMESEC provided the necessary information of successfully integrating and testing the API, but were more time-consuming than having an automated online sandbox version
- Recommendations on the technical aspects of the API
 - Adding more descriptive response codes in the API functions
 - Be more closed-source, not having to implement transform functions in java
 - Support integration with .NET-based applications
- Configuration management file to have more comments/documentations
 - Better certificate management (provision, issuance, management of certs and passwords).
 - Would be helpful to have a service portal for the external SMEs to drive all the management and issuance of certificates

4.7 Additional Input

During the open call phase all participants fulfilled a survey with an wide range of questions. Among these questions a specific group was financially related and tried to identify the real-life impacts of the project developments in an existing organization.

Three of the most relevant questions addressed the following topics:

- Which is the organization financial effort (budget related) to cybersecurity (i.e. What budget is allocated to cybersecurity?)
- Which is the average price for the functionalities they consider key to enhance their cyber-resilience (i.e. Which is the price, you as an SME, consider affordable?)
- Which are the daily activities where SMSEC could contribute to their organizations (i.e. Describe how do you think the SMESEC framework can contribute to your day-to-day business.)

The answers to these questions provided a tangible feedback from real SMEs' needs and how SMESEC framework could improve their daily activities.

A detailed description has been included as part of D6.4 [2] , but it can be summarized as follows:

- In terms of budget allocation, almost a 70% of the companies have no budget allocated or they do not know.

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	81 of 115
Reference:	D5.5	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

- The range of prices these companies consider affordable for their organizations ranges from 25€ head/month (in the lower part of the price range) to 85€
- On regards to how SMESEC could contribute to their organizations the main result of the surveys are linked to the awareness creation or acquiring knowledge

All these answers helped the consortium to benchmark the pricing structure against real organizations but also showed some of the main interest of the SMEs is related to the awareness creation into their organizations and also the knowledge acquisition, both ideas related to the enhancement of their cybersecurity capabilities.

Finally, in D5.4 [3] we have qualitatively and quantitatively assessed the performance gains of the SMESEC framework. Functionally, in both aspects we saw that the SMESEC framework garnered high marks. Survey results show there is a lack of understanding as to why it is important to follow standards and what they require. Combined with the general feeling that adhering to these standards is quite costly, one can assume that standards might not be fully followed by the companies. At the same time, companies are quite worried about cyber threats and believe they are the target of hackers. On the other hand when it comes to budgetary prioritization and allocation of resources, few are willing to adequately allocate resources to cybersecurity. Due to their size and cybersecurity resource allocation, SMEs often lack skilled personnel that are able to effectively handle some of the challenges of building and maintaining an effective Cyber-Security defence. This is evident throughout the survey responses. Hence, beyond its effectiveness and functional requirements, the requirement of Usability holds an especially significant role. Without it, no matter what the success rate in mitigating threats is, the tool will never be used. Usability is measured at different points in the software lifecycle. From installation, through configuration to actual operational use and finally removal. For usability, once installed and configured users tend to be able to handle the operation well and with ease. However, the installation and configuration process is still a pain point that is yet to be solved.

Document name:	D5.5 Open Call Design, Implementation and Results Report			Page:	82 of 115		
Reference:	D5.5	Dissemination:	PU	Version:	1.0	Status:	FINAL

5 Conclusions

In SMESEC we followed a two stages evaluation process. The initial evaluation was performed inside the consortium, by means of the four pilots participating in the project namely the Industrial IoT, Smart City, Power Grid and E-Voting pilots. Additionally, an Open Call was carried out, where It-enabled SME companies from various sectors within EU were invited to use and evaluate SMESEC, in their daily activities gaining all the benefits of the SMESEC security platform and providing an evaluation report to the Consortium. In this deliverable we described the process followed by the SMESEC consortium in order to execute the Open Call which was part of Task5.5. The whole procedure was successfully executed, and the results received depicted the efficacy of SMESEC in being integrated and protect SMEs of various flavours.

The Open Call offered two additional major benefits to the project: Firstly, we were able to test and evaluate the SMESEC external API, that allows companies and solutions outside the consortium to be added to security framework and to be provided to each user in an intuitive manner. Secondly, a Red team was recruited that evaluated both the framework as a whole as well as the security gains of a specific pilot while using SMESEC framework.

The analysis of the open call reporting denoted the actual security gains and protection derived from the use of the platform, the raise of cyber security awareness, which was measured by the CySEC tool of SMESEC, the knowledge gain through our training platform and finally the business opportunities accompanying the use of the platform. The business opportunities arise either directly, by integrating their security-related solution and offering it through SMESEC, or indirectly by providing more confidence to their clientele from the use of a state-of-the-art security platform that comprises of numerous components. Also, based on the feedback and the recommendations we were able to refine the final version of the SMESEC.

Some of the gains as reported by the Open Call participants:

- *"The overall impact has been very positive for the SME. The engagement in the project increased significantly our security awareness. "*
- *"The platform was great extend straightforward and delivered what was promised."*
- *"The "training courses and the awareness platform "is a very interesting offer of SMESEC project and at this point seems to be a promising prototype."*
- *"Overall, the SMESEC project is an interesting proposition for SME companies and definitively worth to be consider as a full commercial product."*
- *"It informs SMEs about security in a very structured way"*
- *"It exposed the involved SMES to the state of the art of various tools, including new categories of tools which they were not aware of"*
- *"It helped Open Call SMEs improve our understanding of our own infrastructure and its security weaknesses."*
- *"The CySec assessment and awareness tool as well as the training courses are just as interesting and helpful as the actual security tools."*

Document name:	D5.5 Open Call Design, Implementation and Results Report			Page:	83 of 115
Reference:	D5.5	Dissemination:	PU	Version:	1.0
				Status:	FINAL

6 References

- [1] Open Call web page: <https://www.smesec.eu/opencall.html>
- [2] D6.4: SMESEC annual report on exploitation, dissemination and standardization (Year 3)
- [3] D5.4: SMESEC Security Framework Assessment report
- [4] D7.4: SMESEC annual report on project management (Year 3)
- [5] D3.9: SMESEC Framework Public Report Final Version
- [6] SMESEC Adapter Tools documentation <https://docs-adapter-tools.smesec.eu/>
- [7] Albrechtsen, E. (2007) "A qualitative study of users' view on information security", *Computers & Security*, 26(4), 276-289.
- [8] Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010) "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness" *MIS Quarterly*, 34(3), 523-548.
- [9] Davis F. (1989), "Perceived usefulness, perceived ease of use, and user acceptance of information technology", *MIS Q.*, 13(3):319-339.

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	84 of 115				
Reference:	D5.5	Dissemination:	PU	Version:	1.0	Status:	FINAL

ANNEX I – Category 1 Contractual technical tasks

OBLIGATION TO PROPERLY IMPLEMENT THE EVALUATION TASKS

The Beneficiary must fulfil the technical specifications for the execution of the service of Assessment of the SMESEC platform, as described in this contract in compliance with all legal obligations under applicable EU, international and national law, and explicitly commits to perform the following tasks:

TASK 1. The evaluation stage shall take place from July through December 2019, both inclusive. Before January 31st 2020, all participants shall deliver to FORTH-ICS, who will act as representative of the SMESEC Consortium, the final evaluation report.

TASK 2. The beneficiary who was selected under **Category 1** will participate in two meetings with the SMESEC consortium. The first one will be held at the beginning of the Evaluation period, September 2019, when the technical details of the integration will be discussed and any integration issues will be addressed and a final one in January 2020, when the SMEs will presents the results of the evaluation to the SMESEC Consortium. The Beneficiary must attend all mandatory teleconferences for the execution of the evaluation process.

TASK 3. The beneficiary acts as a Red Team, and is expected to provide insight into the cybersecurity status of the elements that comprise the SMESEC framework, assessing how the detected weaknesses might affect the confidentiality, integrity and availability of the system and the data processed on them. Specifically, the Red Team will:

- Execute an initial reconnaissance and scanning exercise against listed assets (information to be provided by SMESEC consortium), whose preliminary results will be the starting point for further analysis and discussions. Any initial findings should be outlined during the KoM in September 2019 and more detailed planning of the evaluation process should be presented.
- Design, in collaboration with selected SMESEC consortium members, and perform a test campaign to assess in deep the SMESEC framework and some selected use case assets from a cybersecurity point of view. The final scope will be agreed between the Parties.
- Prepare a final report with the findings and the main recommended improvement actions of the SMESEC solution.

TASK 4. The evaluation of the framework will be divided in five categories which are based on the five pillars of features provided by the SMESEC framework, namely: **(i) “Detection and Response”, (ii) “Protection and Response”, (iii)“Capability and Awareness”, (iv)“Training Courses & Material”, (v)“Lessons Learned” and (vi) “Business model and the market acceptance”.**

TASK 5. The Beneficiary agrees to provide feedback in written form (report) based on the overall experience of assessing the SMESEC platform and the lessons learned from the assessment process. Respective evaluation category **(v)**

TASK 6. The Beneficiary will fill out any assessment questionnaires, on the final functionalities of the SMESEC framework and the expected impact in its particular area of business. Provide feedback in written form to the Coaching Team when required. Respective evaluation category **(vi)**

Document name:	D5.5 Open Call Design, Implementation and Results Report			Page:	85 of 115
Reference:	D5.5	Dissemination:	PU	Version:	1.0
				Status:	FINAL

ANNEX II - Category 2a Contractual technical tasks

OBLIGATION TO PROPERLY IMPLEMENT THE EVALUATION TASKS

The Beneficiary must fulfil the technical specifications for the execution of the service of Assessment of the SMESEC platform, as described in this contract in compliance with all legal obligations under applicable EU, international and national law, and explicitly commits to perform the following tasks:

TASK 1. The evaluation stage shall take place from July through December 2019, both inclusive. Before January 31st 2020, all participants shall deliver to FORTH-ICS, who will act as representative of the SMESEC Consortium, the final evaluation report.

TASK 2. All SMEs under **Category 2a** will participate in two meetings with the SMESEC consortium. The first one will be held at the beginning of the Evaluation period, September 2019, when the technical details of the integration will be discussed and any integration issues will be addressed and a final one in January 2020, when the SMEs will presents the results of the evaluation to the SMESEC Consortium. The Beneficiary must attend all mandatory teleconferences for the execution of the evaluation process.

TASK 3. The evaluation of the framework will be divided in five categories which are based on the five pillars of features provided by the SMESEC framework, namely: **(i) “Detection and Response”, (ii) “Protection and Response”, (iii)“Capability and Awareness”, (iv)“Training Courses & Material”, (v)“Lessons Learned” and (vi) “Business model and the market acceptance”.** The subcontractor is obligated to perform the actions for each of the evaluation categories, as detailed in the following tasks.

TASK 4. Perform all the validation tests indicated by the Coaching Team to substantiate that the SMESEC Framework is up and running. The minimal success criterion is the proper and reliable operation of the XL-SIEM and its coordinated work with a second security tool. The Beneficiary will submit a technical deliverable describing the technical activity performed during the Open Call period. Respective evaluation categories **(i)** and **(ii)**

TASK 5. The beneficiary will use the CYSEC tool for iteratively self-assessing cybersecurity capabilities, planning capability improvements, and monitoring improvement progress. Online and physical meetings will be used to help the SME get started and collect feedback about the usability, user experience, and impact generated with the CYSEC-based improvement method. The data collected will be anonymised logs of capability improvements, and notes or recordings taken from the discussions in the online and physical meetings with experts, all while the SME remains under control of how the data is used in the research. Respective evaluation categories **(iii)** and **(v)**

TASK 6. The beneficiary will measure the end user experience, as the SMESEC training platform is made to reach a diverse audience of users (from a non-tech person to a security analyst). The main concern of the user experience is ‘how it works’. To measure this level, a combination of metrics can be used, such as (Visual Hierarchy, Forms, First-Time User). Additionally, the beneficiary will evaluate the content of the training platform: This level measure the knowledge and skills gained by learners as a result of the training. It will be evaluated by a set of metrics/questions in a specific evaluation form. Respective evaluation category **(iv)**

TASK 7. The Beneficiary agrees to provide feedback in written form (report) based on the overall experience of using the SMESEC platform and the lessons learned from the usage of the framework to its day to day activities. Respective evaluation category **(v)**

TASK 8. The Beneficiary will fill out an assessment questionnaire on the final functionalities of the SMESEC framework and the expected impact in its particular area of business. Provide feedback in written form to the Coaching Team when required. Respective evaluation category **(vi)**

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	86 of 115	
Reference:	D5.5	Dissemination:	PU	
	Version:	1.0	Status:	FINAL

ANNEX III - Category 2b Contractual technical tasks

OBLIGATION TO PROPERLY IMPLEMENT THE EVALUATION TASKS

The Beneficiary must fulfill the technical specifications for the execution of the service of Assessment of the SMESEC platform, as described in this contract in compliance with all legal obligations under applicable EU, international and national law, and explicitly commits to perform the following tasks:

TASK 1. The evaluation stage shall take place from July through December 2019, both inclusive. Before January 31st 2020, all participants shall deliver to FORTH-ICS, who will act as representative of the SMESEC Consortium, the final evaluation report.

TASK 2. All SMEs under **Category 2b** will participate in two meetings with the SMESEC consortium. The first one will be held at the beginning of the Evaluation period, September 2019, when the technical details of the integration will be discussed and any integration issues will be addressed and a final one in January 2020, when the SMEs will presents the results of the evaluation to the SMESEC Consortium. The Beneficiary must attend all mandatory teleconferences for the execution of the evaluation process.

TASK 3. The evaluation of the framework will be divided in five categories which are based on the five pillars of features provided by the SMESEC framework, namely: (i) **“Detection and Response”**, (ii) **“Protection and Response”**, (iii) **“Capability and Awareness”**, (iv) **“Training Courses & Material”**, (v) **“Lessons Learned”** and (vi) **“Business model and the market acceptance”**. The beneficiary of will need to complete a sub-set of these tasks as described in tasks 5-8 and task 4 which is specifically designed for **Category 2b** of the Open Call.

TASK 4. The beneficiary will use the External API that is provided by the SMESEC Consortium to integrate the information generated from its security tool to the SMESEC framework. We will seek integration both in data as well as presentation layer. The minimum requirement is to be able to demonstrate the integration in the data layer with data generated by the beneficiary’s systems are correctly received and processed within the SMESEC Framework.

TASK 5. The beneficiary will use the CYSEC tool for iteratively self-assessing cybersecurity capabilities, planning capability improvements, and monitoring improvement progress. Online and physical meetings will be used to help the SME get started and collect feedback about the usability, user experience, and impact generated with the CYSEC-based improvement method. The data collected will be anonymized logs of capability improvements, and notes or recordings taken from the discussions in the online and physical meetings with experts, all while the SME remains under control of how the data is used in the research. Respective evaluation categories (iii) and (v)

TASK 6. The beneficiary will measure the end user experience, as the SMESEC training platform is made to reach a diverse audience of users (from a non-tech person to a security analyst). The main concern of the user experience is ‘how it works’. To measure this level, a combination of metrics can be used, such as (Visual Hierarchy, Forms, First-Time User). Additionally, the beneficiary will evaluate the content of the training platform: This level measure the knowledge and skills gained by learners as a result of the training. It will be evaluated by a set of metrics/questions in a specific evaluation form. Respective evaluation category (iv)

TASK 7. The Beneficiary agrees to provide feedback in written form (report) based on the overall experience of using the SMESEC platform and the lessons learned from the usage of the framework to its day to day activities. Respective evaluation category (v)

TASK 8. The Beneficiary will fill out an assessment questionnaire on the final functionalities of the SMESEC framework and the expected impact in its particular area of business. Provide feedback in written form to the Coaching Team when required. Respective evaluation category (vi)

Document name:	D5.5 Open Call Design, Implementation and Results Report			Page:	87 of 115
Reference:	D5.5	Dissemination:	PU	Version:	1.0
				Status:	FINAL

ANNEX IV- Category 3 Contractual technical tasks

OBLIGATION TO PROPERLY IMPLEMENT THE EVALUATION TASKS

The Beneficiary must fulfil the technical specifications for the execution of the service of Assessment of the SMESEC platform, as described in this contract in compliance with all legal obligations under applicable EU, international and national law, and explicitly commits to perform the following tasks:

TASK 1. The evaluation stage shall take place from July through December 2019, both inclusive. Before January 31st 2020, all participants shall deliver to FORTH-ICS, who will act as representative of the SMESEC Consortium, the final evaluation report.

TASK 2. All SMEs under **Category 3** will participate in at least one physical meetings with the SMESEC consortium. Two physical meetings are currently planned: the first one will be held at the beginning of the evaluation period, September 2019, when the technical details of the integration will be discussed and any integration issues will be addressed and a final one in January 2020, when the SMEs will presents the results of the evaluation to the SMESEC Consortium. The beneficiary must attend all mandatory teleconferences for the execution of the evaluation process.

TASK 3. The evaluation of the framework will be divided in five categories which are based on the five pillars of features provided by the SMESEC framework, namely: **(i) “Detection and Response”, (ii) “Protection and Response”, (iii)“Capability and Awareness”, (iv)“Training Courses & Material”, (v)“Lessons Learned” and (vi) “Business model and the market acceptance”.**

TASK 4. The SME association will be joining expert focus group meetings to discuss the experiences with the participating SMEs and offer advice from the association's perspective of managing an SME community. The SME association will further join discussion for refining the dissemination method of bringing SMESEC to SMEs and the business model offering opportunities for SME associations to become active participants in the SMESEC ecosystem.


TASK 5. The beneficiary will help disseminate the SMESEC training platform promoting cybersecurity awareness to its SME association. Additionally, the beneficiary will measure the end user experience, as the SMESEC training platform is made to reach a diverse audience of users (from a non-tech person to a security analyst). The main concern of the user experience is ‘how it works’. Specific guidelines will be provided by the Consortium. Respective evaluation category **(iv)**

TASK 6. The Beneficiary will fill out any assessment questionnaires on the expected impact in its particular area of business. Provide feedback in written form to the Coaching Team when required. Respective evaluation category **(vi)**

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	88 of 115
Reference:	D5.5	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

ANNEX V- Application Evaluation Templates

An excel file with the required input fields and formulas were made available to the evaluators. The following images show the information regarding the evaluation template.

 SMESEC OPEN CALL EVALUATION FORM						
EVALUATOR and APPLICANT		Please fill in with the data from the application below:				
Name of the Evaluator:						
Name of the Applicant Company/Association:						
Application Category:						
ELIGIBILITY CRITERIA		Please fill in with the data from the application below: Remarks				
Eligibility Criteria for All Categories						
SME is eligible for participation in the EC Framework Programme H2020						
SME conforms with the SME definition used by the EC						
Single parties (no consortia are allowed)						
Declaration by the applicant is in conformity with the supporting documents requested.						
Being GDPR compliant						
Eligibility Criteria for Category 2a						
Having the required technical infrastructure in place to deploy the SMESEC framework						
Eligibility Criteria for Category 2b						
Do you have a cybersecurity solution that fits in at least one the categories: detection, alerting, protection and response for network or host-based security incidents?						
EVALUATION CRITERIA		Please fill in with the data from the application below:				
Evaluation Criteria Applicable to All Categories	Evaluation Mark (0-10)	Weight Factor (1-5)	Score (Evaluation Mark*Weight Factor)	Remarks	Marking Guideline	
Express your number of years of experience in IT security	0	5.00	0.00			
Ability to deploy SMESEC Framework in the live environment with the help of SMESEC partners (preferable)	0	5.00	0.00		0 The SME cannot be judged due to missing or incomplete information	
Ability to deploy SMESEC Framework in test environment with the help of SMESEC partners	0	4.00	0.00		1- 2 Very poor, Criterion is addressed in an unsatisfactory way	
The SME is part of a SME association that can provide feedback and participate in other SMESEC activities. (A letter of support from the SME association is preferable)	0	4.00	0.00		3- 4 Poor, There are serious weaknesses related to the criterion in question	
Total number of employees	0	3.00	0.00		5- 6 Fair, The criterion is addresses broadly, but there are important weaknesses that need to be corrected	
Having a person appointed as cybersecurity manager	0	2.00	0.00		7- 8 Good, The criterion is addressed well although several improvements are possible	
Number of IT technical stuff and software developers	0	4.00	0.00		9- 10 Excellent, All significant aspects of the criterion in question are addressed successfully. Any possible defect found is minor.	
Evolution of the SME in the last five years (prices, funding, rate of growth, etc.)	0	2.00	0.00			
The number of years that the SME has been legally constituted for.	0	2.00	0.00			
Describe how your participation in the Open Call will benefit SMESEC in terms of experience, technology.	0	5.00	0.00			
Final Score General			0.00			
Evaluation Criteria Applicable to Category 1						
Experience in assessing systems for cyber threats	0	5.00	0.00			
Final Score Category 1			0.00			
Evaluation Criteria Applicable to Category 2a						
Express your number of years of experience in external software deployment and validation on premises servers.	0	5.00	0.00			
# of SMESEC features planned to be exploited with the SME.	0	5.00	0.00			
Having the required technical infrastructure in place to deploy the SMESEC framework	0	4.00	0.00			
Typical types of assets used by the SME (e.g. Cloud Services, Databases, IoT sensors)	0	5.00	0.00			
Final Score Category 2a			0.00			
Evaluation Criteria Applicable to Category 2b						
Being experienced in with IT cybersecurity (Express your number of years of experience in IT security)	0	5.00	0.00			
Having a cybersecurity solution that fits in at least one the categories: detection, alerting, protection and response for network or host-based security incidents.	0	5.00	0.00			
The SME's product is able to provide security information (raw data, incident logs, events description) via an API.	0	5.00	0.00			
Having the required technical infrastructure in place to deploy the SMESEC framework	0	2.00	0.00			
Final Score Category 2b			0.00			
Evaluation Criteria Applicable to Category 3						
# of SMEs associated with the SME association	0	5.00	0			
# of events with member SMEs per year	0	5.00	0			
Potential impact of SMESEC to increase SMEs' cybersecurity protection	0	5.00	0			
Final Score Category 3			0.00			
Overall Score Category 1			0.00			
Overall Score Category 2a			0.00			
Overall Score Category 2b			0.00			
Overall Score Category 3			0.00			

In the excel file provided for evaluation, a sheet for facilitating the profiling of Category 2a applicants was also provided as follows:

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	89 of 115
Reference:	D5.5	Dissemination:	PU
	Version:	1.0	Status:
			FINAL

Criteria for Profiling for Category 2a	Remark	High	Medium	Low	<i>Please Enter Value:</i>	<i>Please Choose:</i>
Express your number of years of experience in IT security	General Criterion	>5	2-5	0-1		
Number of IT technical staff and software developers.	General Criterion	>5	2-5	0-1		
Total number of employees.	General Criterion	101-250	26-100	0-25		
The number of years that the SME has been legally constituted for.	General Criterion	>8	3-7	0-2		
Express your number of years of experience in external software deployment and validation on premises servers.	2a Criterion	>5	2-5	0-1		
# of SMESEC features planned to be exploited with the SME.	2a Criterion	5	3-4	1-2		
	Number of High					0
	Number of Medium					0
	Number of Low					0
	Final Profile for the Applicant					Not defined

The document (including 3 pages) describing the evaluation process for the applicants is given below:

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	90 of 115	
Reference:	D5.5	Dissemination:	PU	
	Version:	1.0	Status:	FINAL



SMESEC Open Call for system validation: Evaluation process

Verification of eligibility will be carried out using the following criteria in Table 1:

<p>Eligibility Criteria for All Categories</p> <p>SME is eligible for participation in the EC Framework Programme H2020. SME conforms with the SME definition used by the EC. Single parties (no consortia are allowed).</p> <p>Declaration by the applicant is in conformity with the supporting documents requested. Being GDPR compliant.</p> <p>Eligibility Criteria for Category 2a</p> <p>Having the required technical infrastructure in place to deploy the SMESEC framework.</p> <p>Eligibility Criteria for Category 2b</p> <p>Do you have a cybersecurity solution that fits in at least one the categories: detection, alerting, protection and response for network or host-based security incidents?</p>
--

Table 1 Eligibility Criteria

EVALUATION AND SELECTION OF APPLICATIONS

If the examination of the application reveals that the applicant does not meet the eligibility criteria stated in paragraph 1.1, the application will be rejected on this sole basis.

Applications will be examined and evaluated by the Contracting Authority with the possible assistance of external assessors. All actions submitted by applicants will be assessed according to the following steps and criteria in Table 2.

Evaluation Criteria Applicable to All Categories	Weight Factor (1-5)
Express your number of years of experience in IT security	5.00
Ability to deploy SMESEC Framework in the live environment with the help of SMESEC partners (preferable)	5.00
Ability to deploy SMESEC Framework in test environment with the help of SMESEC partners	4.00



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101017707 (SMESEC). This work is supported by the Dutch State Secretariat for Education, Research and Innovation (OSIRIS) under contract number 02-20007. The opinions expressed and arguments employed herein do not necessarily reflect the official views of these funding bodies.



Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	91 of 115
Reference:	D5.5	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

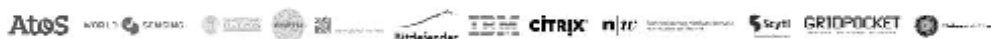
The SME is part of a SME association that can provide feedback and participate in other SMESEC activities. (A letter of support from the SME association is preferable)	4.00
Total number of employees	3.00
Having a person appointed as cybersecurity manager	2.00
Number of IT technical stuff and software developers	4.00
Evolution of the SME in the last five years (prices, funding, rate of growth, etc.)	2.00
The number of years that the SME has been legally constituted for.	2.00
Describe how your participation in the Open Call will benefit SMESEC in terms of experience, technology.	5.00
Evaluation Criteria Applicable to Category 1	
Experience in assessing systems for cyber threats	5.00
Evaluation Criteria Applicable to Category 2a	
Express your number of years of experience in external software deployment and validation on premises servers.	5.00
# of SMESEC features planned to be exploited with the SME.	5.00
Having the required technical infrastructure in place to deploy the SMESEC framework	4.00
Typical types of assets used by the SME (e.g. Cloud Services, Databases, IoT)	5.00
Evaluation Criteria Applicable to Category 2b	
Being experienced in with IT cybersecurity	5.00
Having a cybersecurity solution that fits in at least one the categories: detection, alerting, protection and response for network or host-based security incidents.	5.00
The SME's product is able to provide security information (raw data, incident logs, events description) via an API.	5.00
Having the required technical infrastructure in place to deploy the SMESEC framework	2.00
Evaluation Criteria Applicable to Category 3	
# of SMEs associated with the SME association	5.00
# of events with member SMEs per year	5.00
Potential impact of SMESEC to increase SMEs' cybersecurity protection	5.00

Table 2 The Evaluation Criteria and the Weight of the Criteria

Each evaluation criterion will be marked between 0-10 using the following guidelines in Table 3 :

Evaluation Criteria Marking Guidelines
0 The SME cannot be judged due to missing or incomplete information





1 - 2 Very poor	Criterion is addressed in an unsatisfactory way
3 - 4 Poor	There are serious weaknesses related to the criterion in question
5 - 6 Fair	The criterion is addressed broadly, but there are important weaknesses that need to be corrected
7 - 8 Good	The criterion is addressed well although several improvements are possible
9 - 10 Excellent	All significant aspects of the criterion in question are addressed successfully. Any possible defect found is minor.

Table 3 Evaluation Criteria Marking Guidelines

Final score for each criterion will be calculated by multiplying the mark and the weight factor of the criterion.

Total score for an application is the sum of all scores for all the applicable criteria.

Once all criteria have been assessed, a list will be drawn up with the applications ranked according to their total score.

There will be a profiling process for the applications for Category 2a according to Table 4.

Criteria for Profiling for Category 2a	High	Medium	Low
Express your number of years of experience in IT security	>5	2-5	0-1
Express your number of years of experience in external software deployment and validation on premises servers.	>5	2-5	0-1
# of SMESEC features planned to be exploited with the SME.	5	3-4	1-2
Number of IT technical staff and software developers.	>5	2-5	0-1
Total number of employees.	101-250	26-100	0-25
The number of years that the SME has been legally constituted for.	>8	3-7	0-2

Table 4 Criteria for Profiling for Category 2a

As we are seeking for a diverse set of SMEs for this category, all applicants will be placed into one of the three categories (High, Medium, Low) based on the expertise on IT and the adoption level of ICT to their day-to-day operations. Then two applicants will be selected from the High and Medium category and 1 from the Low.

The following guideline in Table 5 will be applied according to the answers given to the profiling criteria.

Guideline	Final Profile
Number of High ≥ 3 and Medium < 3 and Low < 3	High
Number of Medium ≥ 3 and High < 3 and Low < 3	Medium
Number of Low ≥ 3 and High < 3 and Medium < 3	Low
Number of High = 3 and Medium = 3 and Low = 0	High
Number of Medium = 3 and Low = 3 and High = 0	Medium
Number of High = 3 and Low = 3 and Medium = 0	Medium
Number of High = Medium = Low = 2	Medium

Table 5 Guideline for Profiling Category 2a Applicants



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 741207 (SMESEC). This work is supported by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 17.00007. The opinions expressed and arguments employed herein do not necessarily reflect the official views of these funding bodies.



Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	93 of 115
Reference:	D5.5	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

ANNEX VI- Questionnaires

The public questionnaire that was disseminated through various public channels is given below:

3/30/2020

SMESEC - SMEs' Cybersecurity Watch 2

SMESEC - SMEs' Cybersecurity Watch 2

General survey

*Required



The survey intends to identify, in less than 10 minutes, the cyber threats you are exposed to and the status of your organisation concerning cybersecurity. Your contribution will help in bringing together the facts from small and medium-sized enterprises. We will use the information to inform about the state of cyber threats across industries and guide the development of lightweight answers for thorough protection.

We simplified the questionnaire as much as possible. Even if you are not a cybersecurity specialist, you can easily answer them. An optional, more technical part of the survey is also available for the person responsible for cybersecurity in your organisation. Fill it out to get ideas of what cybersecurity is about!

All data will be treated anonymously and analysed in a continuous report available on the project website. www.smesec.eu

SMESEC is a European research project funded by the European Commission under the Grant Agreement 740787 and the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 17.00067. The project aims at supporting SMEs in the area of cybersecurity offering two different tools: on the one hand a cybersecurity framework offering state-of-the-art tools and on the other hand cybersecurity training and awareness courses.



About You

1. What is the job title stated on your business card?

<https://docs.google.com/forms/d/1zJXADKwVoSesekZaMfLUndHnwy21q7gWwGWMvxtkaEg/edit>

1/22

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	94 of 115
Reference:	D5.5	Dissemination:	PU
	Version:	1.0	Status: FINAL

3/30/2020

SMESEC - SMEs' Cybersecurity Watch 2

2. Are you responsible for the cybersecurity of your company?

Mark only one oval.

- Yes
 Yes, partly
 No

3. Did you receive any training in the field?

Applies to you as a person and not to your company.

Mark only one oval.

- Yes
 No

4. Your pseudonymous identifier

Create here a unique anonymous identifier that you remember and reuse in future questionnaires as long as you stay with the same company. E.g. compose the identifier with the month and day of your birthday and the place on earth with your best memories (example: 1105rapperswil). The identifier will allow us to study trends over time.

Company Profile

Your Company's Profile

We anonymise and summarise the responses. No conclusions can be made about an individual company.

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	95 of 115				
Reference:	D5.5	Dissemination:	PU	Version:	1.0	Status:	FINAL

5. Company Size

Choose the smallest size for which all criteria apply.

Mark only one oval.

- Micro: <10 employees and turnover ≤ 2 Million €
- Small: <50 employees and turnover ≤ 10 Million €
- Medium-sized: <250 employees and turnover ≤ 50 Million €
- Government or public organization
- Other: _____

6. Type of Business

Please indicate the business models that contribute with >20% of the turnover of your company. You may select multiple entries. Examples and more information:

https://www.smesec.eu/SMESEC_Questions_Answers.html

Tick all that apply.

	Financial	Physical, devices	Software, SaaS	Data, digitally encoded knowledge	Humans, experts, person-hours
Developer, inventor	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Producer, manufacturer	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Reseller, distributor	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Service-provider, lessor	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Broker	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

7. Domain of Business

Please indicate the main business domain of your company.

Mark only one oval.

- Agriculture, forestry and fishing
- Mining and quarrying
- Manufacturing
- Electricity, gas, steam and air conditioning supply
- Water supply; sewerage, waste management and remediation activities
- Construction
- Wholesale and retail trade; repair of motor vehicles and motorcycles
- Transportation and storage
- Accommodation and food service activities
- Information and communication
- Financial and insurance activities
- Real estate activities
- Professional, scientific and technical activities
- Administrative and support service activities
- Public administration and defence; compulsory social security
- Education
- Human health and social work activities
- Arts, entertainment and recreation
- Other service activities
- Activities of households as employers; undifferentiated goods- and services-producing activities of households for own use
- Activities of extraterritorial organisations and bodies

Degree of outsourcing

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	97 of 115
Reference:	D5.5	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

3/30/2020

SMESEC - SMEs' Cybersecurity Watch 2

8. To what degree is software development outsourced in your SME?

Mark only one oval.

- 0-25%
- 25-50%
- 50-75%
- 75-100%
- I don't know.

9. To what degree are software and services hosted externally?

Mark only one oval.

- 0-25%
- 25-50%
- 50-75%
- 75-100%
- I don't know.

Reliance on IT for running the business operations

10. The organization can do business without IT support for how many minutes/hours

Mark only one oval.

- 0 -10 minutes
- 10 min to 1 hour
- 1 to 24 hours
- 24 or more hours
- I don't know.

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	98 of 115				
Reference:	D5.5	Dissemination:	PU	Version:	1.0	Status:	FINAL

11. The importance of Availability of the organization's critical information. (Availability means your critical information can be used by any authorized parties whenever needed, i.e. your customers' data is available to your sales personnel when they need.)

Mark only one oval.

- High
 Medium
 Low
 I don't know.

12. The importance of Confidentiality of the organization's critical information. (Confidentiality means your critical information can be viewed only by authorized parties, i.e. an attacker cannot view your customers' data on your website.)

Mark only one oval.

- High
 Medium
 Low
 I don't know.

13. The importance of Integrity of the organization's critical information. (Integrity means your critical information can be modified only by authorized parties, i.e. an attacker cannot update your customers' data on your website.)

Mark only one oval.

- High
 Medium
 Low
 I don't know.

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	99 of 115				
Reference:	D5.5	Dissemination:	PU	Version:	1.0	Status:	FINAL

Complexity of the IT environment

14. The number of employees supporting the IT environment.

Mark only one oval.

- < 1 employees
- 1 - 2.5 employees
- 2.5 - 5 employees
- 5 - 10 employees
- > 10 employees
- I don't know.

15. The organization's annual spend on IT

Mark only one oval.

- 0-1% turnover
- 1%-3% turnover
- 3-5% turnover
- 5-10% turnover
- >10% turnover
- I don't know.

Budget Allocation to Cybersecurity

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	100 of 115				
Reference:	D5.5	Dissemination:	PU	Version:	1.0	Status:	FINAL

3/30/2020

SMESEC - SMEs' Cybersecurity Watch 2

16. What budget is allocated to cybersecurity?

Select the closest fitting number.

Mark only one oval.

- No budget
- 2% of turnover
- 5% of turnover
- 10% of turnover
- 20% of turnover
- I do not know and cannot estimate

17. In case of budget restrictions, is there any component you will consider a MUST and pay for it individually? (without paying for the whole framework)

18. Which is the price, you as an SME, consider affordable?

Expected Value and Acquisition of SMESEC**19. Describe how do you think the SMESEC framework can contribute to your day-to-day business.**

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	101 of 115				
Reference:	D5.5	Dissemination:	PU	Version:	1.0	Status:	FINAL

3/30/2020

SMESEC - SMEs' Cybersecurity Watch 2

20. Is there a preferred distribution channel to obtain the framework?

User Experience

21. Do you think the SMESEC Framework is conservative or innovative?

Mark only one oval.

Conservative

Innovative

22. Are you missing any functional capabilities that are not present in the SMESEC Framework and are crucial in your opinion? If yes, please explain.

Cybersecurity Standardisation

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	102 of 115				
Reference:	D5.5	Dissemination:	PU	Version:	1.0	Status:	FINAL

3/30/2020

SMESEC - SMEs' Cybersecurity Watch 2

23. Do you believe that information security standards or cybersecurity standards may improve the quality of your services or products?

Mark only one oval.

- Yes
 No
 Maybe

24. Do you use any information security standards or cybersecurity standards in your business? If yes, which ones?

Mark only one oval.

- Yes
 No

25. If yes, which ones?

To what degree do you agree with the following statements as barriers for using information security or cybersecurity standards.

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	103 of 115				
Reference:	D5.5	Dissemination:	PU	Version:	1.0	Status:	FINAL

3/30/2020

SMESEC - SMEs' Cybersecurity Watch 2

26. There are too many standards. It is difficult to decide which ones to use.

Mark only one oval.

1	2	3	4	5	
Strongly disagree	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Strongly agree

27. Standards are technically complex, not easy to understand or implement.

Mark only one oval.

1	2	3	4	5	
Strongly disagree	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Strongly agree

28. Cost of acquiring standards is high.

Mark only one oval.

1	2	3	4	5	
Strongly disagree	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Strongly agree

29. Cost of implementing standards is high.

Mark only one oval.

1	2	3	4	5	
Strongly disagree	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Strongly agree

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	104 of 115
Reference:	D5.5	Dissemination:	PU
	Version:	1.0	Status:
			FINAL

3/30/2020

SMESEC - SMEs' Cybersecurity Watch 2

30. Benefits from implementing standards are unknown.

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Strongly agree

Cybersecurity

Cyber Threats

Please judge the following statements.

31. Your company considers itself to be a target for hackers.

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Strongly agree

32. What cyber attacks or data breaches did your company experience in the past 12 months?

One answer per row.

Mark only one oval per row.

	Frequent	Occasional	Almost never	Never	I do not know
Severe attacks (threat to your operations)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Moderate attacks (requiring dedicated attention)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mild attacks (without significant impact)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

3/30/2020

SMESEC - SMEs' Cybersecurity Watch 2

33. What were the consequences of the attacks on your company?

Multiple answers possible; some are exclusive.

Tick all that apply.

- Closure of the company or business
- Temporary disruption of the company's business
- Reputational damage: loss of customers, sales, profits
- Extra costs for incident recovery and prevention
- Regulatory or contractual sanctions or fines
- No consequences
- I do not know

Other: _____

34. Your company is worried about cyber threats.

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Strongly agree

35. In comparison to 12 months ago, your company's worries about cyber threats changed as follows.

Mark only one oval.

	1	2	3	4	5	
Much less concerned	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Much more concerned

Your Company's Protection and Practices

Please consider the opinion of your company as of today.

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	106 of 115
Reference:	D5.5	Dissemination:	PU
	Version:	1.0	Status:
			FINAL

3/30/2020

SMESEC - SMEs' Cybersecurity Watch 2

36. Your company can well mitigate cyber risks, vulnerabilities, and attacks.

Please judge the statement.

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Strongly agree

37. Your company can easily recover from a cyber attack.

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Strongly agree

38. Your company has a systematic approach to ensuring cybersecurity.

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Strongly agree

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	107 of 115
Reference:	D5.5	Dissemination:	PU
	Version:	1.0	Status: FINAL

39. Sources of knowledge about cybersecurity

Please judge the attractiveness of the following sources for your company.

Mark only one oval per row.

	Unattractive (1)	2	3	4	Attractive (5)
Own research	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
External experts	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Web pages and forums	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Online courses, webinars, and videos	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Classroom courses, workshops	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Newspapers, radio, and television	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

40. Who does cybersecurity for your company?

Multiple answers possible; some are exclusive.

Tick all that apply.

- Everybody a bit
- A dedicated person or team
- External consultants or service providers
- Nobody
- I do not know

Other: _____

Improving Cybersecurity

3/30/2020

SMESEC - SMEs' Cybersecurity Watch 2

41. Your company may consider slowing or pausing operations for some days and improve cybersecurity.

Mark only one oval.

1	2	3	4	5	
Strongly disagree	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Strongly agree

42. How could your company improve cybersecurity?

Multiple answers possible; some are exclusive.

Tick all that apply.

- Train employees in cybersecurity awareness and practices
- Employ or contract cybersecurity specialists
- Systematize the search for vulnerabilities
- Respond to prioritised threats
- Exchange lessons-learned with other SMEs
- Acquire a more advanced set of security solutions
- Allocate extra budget for cybersecurity
- Improve the cybersecurity tooling
- I do not know

Other: _____

43. Are you the cybersecurity responsible in your company and want to help us with answers to technical questions? *

If there is no cybersecurity responsible in your company, you are also kindly invited to do the technical part (please select "Yes" below). "I do not know" will be allowed, and all questions will be optional.

Mark only one oval.

- Yes, I would like to offer technical feedback *Skip to question 44*
- No, I am unable to or should not provide technical feedback *Skip to question 53*

**Technical
Feedback**

Note, it will not be possible to trace your answers to your person or company. We do not collect any information about the identity of your organisation.

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	109 of 115
Reference:	D5.5	Dissemination:	PU
	Version:	1.0	Status: FINAL

44. What data do you store or process?

More information about the GDPR-based classification:

https://www.smesec.eu/SMESEC_Questions_Answers.html. Multiple answers possible; some are exclusive.

Tick all that apply.

- I do not know (please do not combine with other answers)
- Personal data
- Profiling data
- Genetic data
- Biometric data
- Health data
- Sensitive data
- Intellectual property
- Trade or business secrets
- Information about your business strategy
- Data about your markets or customers

Other: _____

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	110 of 115				
Reference:	D5.5	Dissemination:	PU	Version:	1.0	Status:	FINAL

3/30/2020

SMESEC - SMEs' Cybersecurity Watch 2

45. How critical are these concerns for your company?

Please judge the following common threats. You may select "I do not know."

Mark only one oval per row.

	I do not know	Uncritical (1)	2	3	4	Critical (5)
System Availability	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
System Intrusion or Tampering	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
System Destruction or Deletion	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
System Theft	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Viruses	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Transaction Integrity	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fraud	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ransom or Blackmail	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Regulatory Compliance	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Privacy	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
User Errors	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Malicious Insiders	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Malicious Outsiders	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Deception of Manipulation of Users	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Sensitive Data Exposure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Data Integrity or Availability	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Unwanted Data Loss or Theft	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Garbage Data (Spam)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

<https://docs.google.com/forms/d/1zJXADKwVoSesekZaMfUcHnWY21q7gWwGWMvxtkaEg/edit>

18/22

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	111 of 115
Reference:	D5.5	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

3/30/2020

SMESEC - SMEs' Cybersecurity Watch 2

Natural Disasters	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Power Failure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

46. If applicable: what other threats does your company consider critical?

Your Opinion as Cybersecurity Responsible in your Company

47. Attacks on your company are successful.

With "successful," we mean that the attacker's objective was achieved. For example, an attacker may have successfully compromised a system, or an attacker may have successfully stolen a password.

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Strongly agree

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	112 of 115
Reference:	D5.5	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

48. Does your company use the following?

Multiple answers possible; some are exclusive.

Tick all that apply.

- Cybersecurity policy or baseline
- Computer use and misuse policy
- Proprietary data use and misuse policy
- Communication use and misuse policy
- Business continuity plan
- Information security procedures
- Data or media destruction procedures
- Information sensitivity levels or coding
- Incident response plan
- Incident response team
- Data backup or recovery procedures
- Password management policy
- I do not know (please do not combine with other answers)

49. How does your company do cybersecurity?

Multiple answers possible; some are exclusive.

Tick all that apply.

- Facility or physical access control
- System or data access control
- Team training and awareness measures
- Systematic and regular updates
- Systematic and regular review of the cybersecurity practices
- Cybersecurity plan supported by the top-management and with allocated budget and resources
- Data segregation
- Redundant systems or data storage
- Power surge protection
- Insurances
- I do not know (please do not combine with other answers)

 Other: _____

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	113 of 115
Reference:	D5.5	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

50. What cybersecurity tools does your company use?

Multiple answers possible; some are exclusive.

Tick all that apply.

- Security Information and Event Management (SIEM) tools
- Virus, rootkit, malware, phishing, or data loss protection tools
- Secure gateways or firewalls
- Baselines for cybersecurity (guidelines)
- Intrusion detection (IDS) or prevention systems (IPD)
- Vulnerability assessment tools (VAS) or security evaluation systems
- Physical or virtual network protection tools, e.g. a Virtual Private Networks (VPN)
- Encryption
- System activity monitors or loggers
- Shredders
- Data backup systems
- I do not know (please do not combine with other answers)

Other: _____

51. For your IT security solutions, where do you think specific improvements are needed?

Multiple answers possible; some are exclusive.

Tick all that apply.

- User-friendly
- Easy deployment
- Common attack defence
- Endpoint protection
- Cloud/Hypervisor security
- Flexible alerting
- Affordability
- Strong privacy and authentication
- Security event processing
- Scalability

Other: _____

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	114 of 115
Reference:	D5.5	Dissemination:	PU
		Version:	1.0
		Status:	FINAL

3/30/2020

SMESEC - SMEs' Cybersecurity Watch 2

52. How could an initiative like www.smesec.eu contribute best to making your company safe and secure?

Skip to question 53

Closure

By clicking on the submit button, you duly confirm that you have read and accept the Informed consent procedures and recruitment criteria available on <https://www.smesec.eu/informedconsent.pdf>

53. My Answers are accurate and correct *

Mark only one oval.

Yes

No

Thank you!

To get the survey results, please leave us your e-mail in the separate form accessible after submission.

This content is neither created nor endorsed by Google.

Google Forms

<https://docs.google.com/forms/d/1zJXADKwVoSeseKZaMfUnclHNwy21q7gWwGWMvxkkaEg/edit>

22/22

Document name:	D5.5 Open Call Design, Implementation and Results Report	Page:	115 of 115				
Reference:	D5.5	Dissemination:	PU	Version:	1.0	Status:	FINAL