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

D3.6 Final SMESEC Security Awareness and Training Report

Document Identification			
Status	Final	**Due Date**	30/05/2020
Version	1.0	**Submission Date**	05/06/2020

Related WP	WP3	**Document Reference**	D3.6
Related Deliverable(s)	-----	**Dissemination Level (*)**	PU
Lead Organisation	EGM	**Lead Author**	Philippe Cousin
Contributors	EGM, FHNW, FORT	**Reviewers**	

Keywords: Awareness Goals, SME Challenges, Good Cybersecurity Practice, Awareness Roadmap, Validation Plan

Document Information

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.

(*) 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.

List of Contributors	
Name	Partner
Samuel Fricker, Alireza Shojaifar, Martin Gwerder	FHNW
Philippe Cousin,	EGM
Kostas Lampropoulos	UoP

Document History			
Version	Date	Change editors	Changes
0.1	18/04/2020	Philippe Cousin	ToC for discussion and contribution
0.3	20/05/2020	Kostas Lampropoulos	Contribution UoP on training
0.5	29/05/2020	Samuel Fricker	Contribution FNHW on
0.6	3/06/2020	Alberto Miranda	Contribution ATOS
0.7	3/06/2020	Manos Athanatos	Contribution Forth
1.0	4/06/2020	P.Cousin	Pre-final for review

Quality Control		
Role	**Who (Partner short name)**	**Approval Date**
Deliverable leader	Philippe Cousin (EGM)	
Technical manager	Christos Tselios (Citrix)	
Quality manager	Rosana Valle Soriano (Atos)	
Project Manager	Jose Fran. Ruíz (Atos)	

Table of Contents

List of Tables

List of Figures

List of Acronyms

Abbreviation / acronym	Description
ACL	Network Access Control List
APT	Advanced Package Tool (Linux)
BSI	British Standards Institution
BYOD	Bring Your Own Device
CIRT	Cyber Incident Response Team
CSRF	Cross-site Request Forgery
CYSFAM	Cyber Security Focus Area Maturity Model
Dx.y	Deliverable number y belonging to WP x
EC	European Commission
FAQ	Frequently Asked Question(s)
HIPAA	American Health Insurance Portability and Accountability Act
ISFAM	Information Security Focus Area Maturity Model
ISMS	Information Security Management System
ISO	International Organisation for Standardisation
Mx	Month x
NERC CIP	North American Electric Reliability Corporation: Critical Infrastructure Protection
OSSEC	Open Source Host-based Intrusion Detection System
OWASP	Open Web Application Security Project
PCI DSS	American Payment Card Industry: Data Security Standard
PDCA	Plan-Do-Check-Act
SIEM	Security Information and Event Management
SME	Small and Medium Enterprises
WP	Work Package
XSS	Cross-site Scripting
YUM	Yellowdog Updater Modified (Linux flavor)

Executive Summary

This report provides an overview of the activities carried out within the task T3.5 "Implementation of SMESEC SME end user training and security awareness plan "(M7-M36). It implements the security awareness plan that was road mapped in task T2.4 and described in Deliverable 2.3.

The task collected feedback from SME end-users and following the D2.3 roadmap structure implements appropriate actions that include the recording of SME and public authorities' end-user personnel views on security issues and the development of training sessions, workshops and appropriate certification actions.

This report overviews the work to develop tools to interact with the SMEs such as the dedicated questionnaires and the Cyber Security Coaching tool (e.g. CYSEC tool) which was up and running and demonstrated in this third period

The SMESEC consortium has interacted with many SMEs at various events and initiated many contacts with European and National SMEs associations. Many associations are still interested to see the exploitation of the SMESEC tools with a specific interest on CYSEC in this context of awareness raising. In this period, we got also useful feedbacks on personnel from Public authority. We increase cooperation with other cybersecurity related European projects or organisations and SMESEC offers are now promoted and will continue to be along many existing and continuing channels (e.g. Cyberwatching.eu)

The training platform was operational and populated by many courses which were followed and individual certification per training was put in place.

Finally, in cooperation with 3 other projects, SMESEC promote a self-assessment best practices quiz leading to give certificate to check people skill. This and many other results will continue to live after the end of the SMESEC project.

1 Introduction of the T3.3 task activity

This report provides an overview of the status of task T3.3 "*Implementation of SMESEC SME end user training and security awareness plan*" (M7-M36). It implements the security awareness plan that was road mapped in task T2.4 and described in D2.3.

The task considers the collected feedback from SME end-users and following the **D2.3 roadmap** structure implements appropriate actions that include the recording of SME and public authority's end-user personnel views on security issues and the development of training sessions, workshops and appropriate certification actions. The training and awareness phase that is consolidated in this task will be realized in various stages within the project lifecycle, aiming to collect appropriate feedback from the define/protect/monitor actions. For this reason, two reports will be provided: one preliminary report (this one) and a final one where after collecting data from the validation phase (in WP4 and WP5) a new recommendation phase will be triggered with the implementation of more accurate training and security awareness actions.

Cybersecurity has become a problem for many small and medium-sized companies (SMEs). Despite a continued rise in cyber threats and digital connectivity that allows threats to propagate, SMEs continue to protect themselves insufficiently. For that reason, SMESEC aims at improving the awareness of the cybersecurity problem, knowledge of good practices, and the institutionalisation of tailored, effective capabilities in SMEs. This aim applies to the whole company as well as to the individual employees who are the users of cybersecurity tools.

In the context of cybersecurity for an SME, a "security awareness plan" can have multiple interpretations, both for the entity developing the awareness and the scope of the plan. Security awareness may be the awareness of the SME about cyber threats matched with capabilities for addressing these threats. Security awareness may also be the awareness of the SME's employees about cybersecurity threats and how the employees should behave to avoid or mitigate problems. The plan may be enacted from the perspective of the entity benefitting from the cybersecurity actions. For example, the plan may be a step-wise process of discovering cyber threats and building the capabilities of addressing the threats. The plan may also be enacted from the perspective of the SMESEC project. The plan may involve dissemination actions raising awareness in the targeted industries and the release, validation, evolution, and exploitation of the SMESEC framework that helps European SMEs to build up cybersecurity capabilities.

1.1 The overall approach

According to the task description and duties to increase awareness to SMEs and provide the related training, we carried out the following tasks:

a) **Using tools for interacting with SMEs**: the main tool is the Cyber Coaching (CYSEC) tool (see 2.2) but other tools were also used such a self –assessment questionnaire and feedback questionnaires (see 3.3.1).

b) **Organise the SMEs feedbacks**. This is done through:
   - On-line interactions through questionnaires and webinars;
   - F2F meetings at key-events (eg. IoT world Congress 2018, ICT 2018 Vienna, Crete Workshop, FIC 2020 …

- Direct interviews by phone or F2F with selected SME people also as part of the open call process; Interaction with Public authorities as part of the feedback process

c) **training materials and the organisation of training sessions**: we have put in place a training platform and have populated it with specific material;

d) **a certification programme**: we put in place individual certification per training and we developed an overall certification programme for cybersecurity for SMEs like a self-assessment quiz with 3 other EU cybersecurity related projects (see xxx)

The overall activities over the project implementation period can be described as follow:

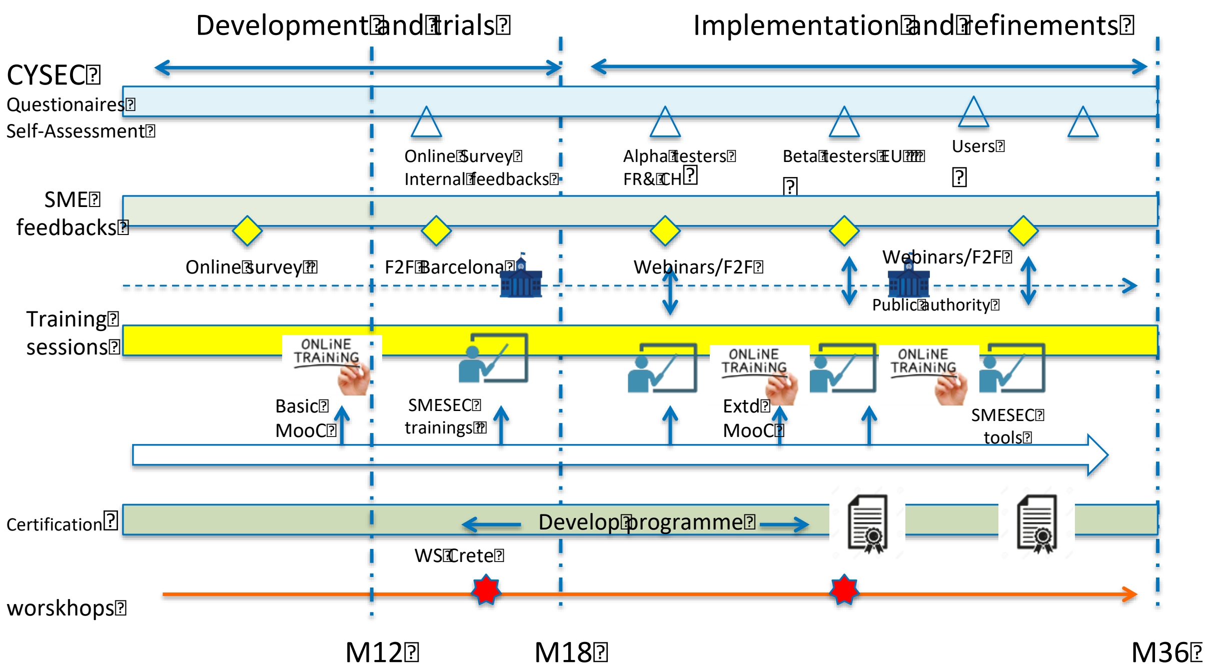


Figure 1: simplified overview of T3.3 activities

The awareness programme activity is aligned with actions organised in the dissemination plan. To reach the SMEs, we have combined 3 forces of SMEs contacts over 3 axes, as described in the D6.2:

a) Overall SMEs reached through F2F meetings and the European and National Associations. Individual SMEs were contacted through such associations;

b) SMEs using technologies known by SMESEC partners and where partners experience can be useful. For instance, IoT is already a major technology field impacting SMEs in a broad range of domains. We approached IoT-related SMEs at major IoT events (e.g. IoT World Congress or Smart Cities (eg http://www.smartcityexpo.com/));

c) SMEs already involved in the cybersecurity domain and acting as multipliers. SMEs selling cybersecurity services are already in contact with their “customers”. For instance, in the first period we have been present at ETSI security week. In the 3rd we have been at the International Cybersecurity Forum FIC 2020 where we had a booth and a workshop was organised all together with 3 other EU project; More actions are described in Deliverable 6.4.

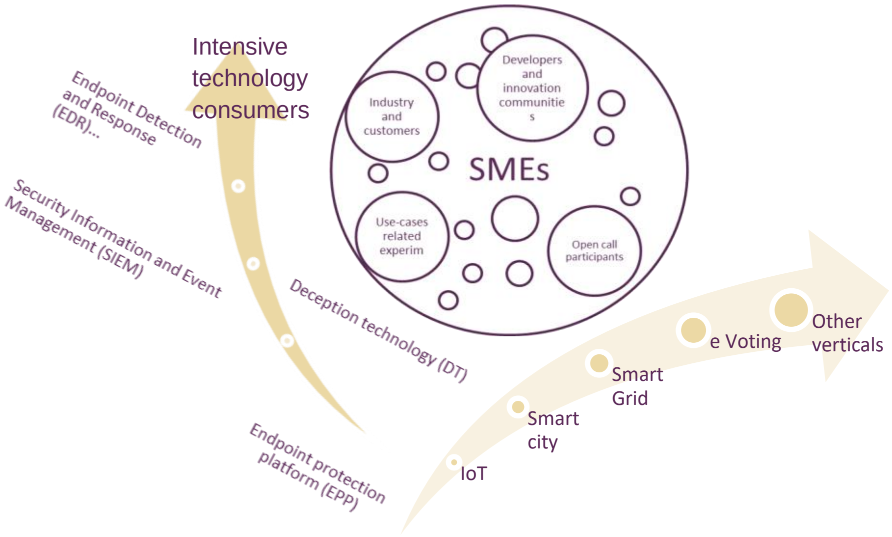

Intensive technology consumers
Endpoint Detection and Response (EDR)...
Security Information and Event Management (SIEM)
Deception technology (DT)
Endpoint protection platform (EPP)
SMEs
Developers and innovation communitie s
Industry and customers
Use-cases related experim
Open call participants
IoT
Smart city
Smart Grid
e Voting
Other verticals

Figure 2: 3 axis SMEs contact forces described in dissemination plan (D6.2)

1.2 Relation to other project works

The task implements the security awareness plan that was road mapped in WP2- task T2.4.

A final report prepared after collecting data from the validation phase (in WP4 and 5) will close the work.

The task is synchronised with WP6; in particular on dissemination and standardisation actions as they foresee steps to reach SMEs directly or indirectly (e.g. through SDOs).

1.3 Structure of the document

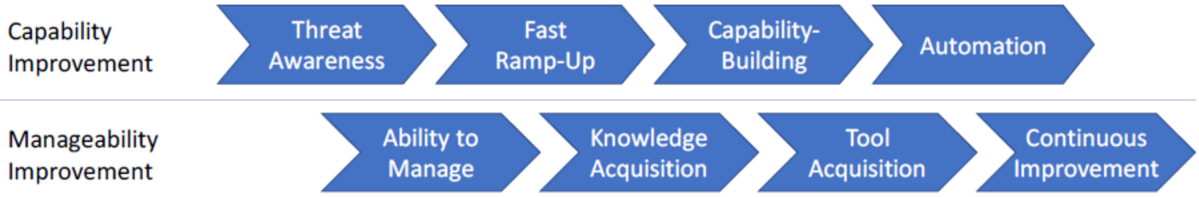
In Chapter 2, we present the overall approach to the task of raising the cyber security awareness in SMEs and the linked training actions. First, we present some tools to interact with the SMEs, such as the Cyber security coach described in Chapter 2. In Chapter 3 we report on how we reach the SMEs and how we have already met some of them through meetings and national associations. In Chapter 4 we present the SMESEC training platforms, which are ready to welcome more training courses in the coming weeks and which will be used later on to help SMEs during the second period. Finally, in section 5 we provide the initial feedback from some SMEs about their cybersecurity understanding taken from the analysis of the initial responses to the SMESEC questionnaires.

2 Implementing the roadmap (D2.3)

2.1 Reminding of the D2.3 roadmap: awareness and training plan

D2.3 has proposed the following process to be followed by an SME for awareness and capability building. We proposed the CYSEC tool to automate cybersecurity communication, allowing each SME to become aware and improve their ability to prevent incidents or mitigating their impact. The following figure, extracted from D2.3, illustrates.

Table 1: Capability improvement process for raising awareness and enable capability-building (D2.3)



On the side of capability improvement, the goal of CYSEC was to raise awareness of threats, guide the SME in the adoption of cybersecurity practices that are easy to adopt and have all-over-the-board security improvement impact for the SME, guide the development of specialist capabilities, and enable cybersecurity automation with recommendations for proper controls. On the side of manageability improvement, the focus of CYSEC is on first setting up the organisation allowing the SME to manage security, offer knowledge about controls and practices for the CISO and employees, recommend tools to be adopted, and encourage continuous improvement with reminders that brings the SME back to reassessing and continuing to improve their cybersecurity.

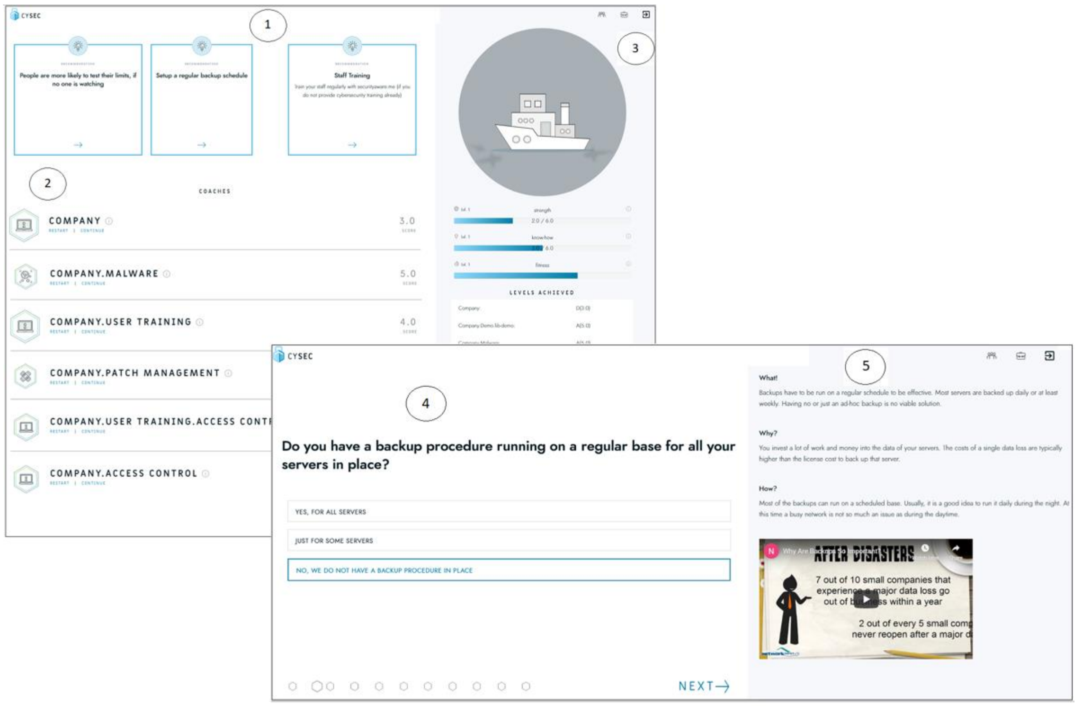
In this section, we report the results of evaluating the CYSEC tool's impact on the four SMESEC use case SMEs.

2.2 CYSEC tool used by the SMESEC use case SMEs

In this section, we describe the CYSEC features offered to the SMEs and explain how these features were proposed 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.

2.2.1 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 Fig. 3, the work area at the bottom right.



People are more likely to test their limits, if no one is watching

Setup a regular backup schedule

Staff Training

Train your staff regularly with securityaware.me (if you do not provide cybersecurity training already)

Do you have a backup procedure running on a regular base for all your servers in place?

YES, FOR ALL SERVERS

JUST FOR SOME SERVERS

NO, WE DO NOT HAVE A BACKUP PROCEDURE IN PLACE

What!

Backups have to be run on a regular schedule to be effective. Most servers are backed up daily or at least weekly. Having no or just an ad-hoc backup is no viable solution.

Why?

You invest a lot of work and money into the data of your servers. The costs of a single data loss are typically higher than the license cost to back up that server.

How?

Most of the backups can run on a scheduled base. Usually, it is a good idea to run it daily during the night. At this time a busy network is not so much an issue as during the daytime.

Figure 3: 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 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.

Tables 4 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 2: A detailed list of threat, vulnerabilities, and security controls for refreshing interviewees' minds

Threats
Disaster, malicious insider, Downloading App from not-trusted store, Ransomware, using 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 a 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

2.2.2 Proposed impact of CYSEC on SME awareness

Albrechtsen [5] 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. [6], 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*. In addition, 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*** [7].
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 securityware.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 and 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.

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 SMESEC use case SMEs' awareness improvement and cybersecurity adoption. The presented results were gathered using structured interviews with the four use case SMEs. The names of the companies have been kept anonymous to ensure confidentiality.

2.3.1 Method of the evaluation

To evaluate if CYSEC enhanced use case partners' awareness, four structured interviews were conducted after the SMEs' extended use of the CYSEC tool in the SME's operational environment. The study sought answers to the following research questions. RQ1 reflects the impact of actual usage of the CYSEC on cybersecurity awareness improvement. RQ2 evaluates the users' needs and missing features in the context of security awareness improvement after experiencing the tool's actual usage. RQ3 aims at understanding the users' attitudes about tool acceptance and usefulness.

RQ1: How do the SMEs build cybersecurity awareness improvement when assisted with the CYSEC cybersecurity coach? 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? 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? This question wants to know users' attitudes and evaluation of the tool acceptance and usefulness. Usefulness is a significant factor for us to study security adoption.

For answering the research questions, we allowed the SMEs to use the CYSEC tool over a prolonged time. The installation and short training session for using the final version of the CYSEC tool for operational use were at the end of February 2020. Thereafter, we offered repeated support to check whether the tool is still in use and to inform about updates. The final interview used for data collection about CYSEC impact was in May 2020. Before conducting the final interview, all subjects confirmed that they had applied the tool.

A request for the final online interview has been sent to all use cases. All interviewees had the possibility to 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 had the possibility to 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 the 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 D3.6 and obtained the subjects' consent.

Table 3 presents the questionnaire for the interviews.

Table 3: the questionnaire template for the structured interview with the SMEs

Impact of CYSEC	
Threats and Vulnerabilities	
1	What threats or vulnerabilities have not you been aware before using CYSEC?
2	What threats or vulnerabilities have you been aware before 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?
Controls and Practices	
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 to you agree with the following? CYSEC had 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?

2.3.2 Results

Table 2 gives an overview of the SMEs' demographics. The SME identifiers are consistently used throughout the rest of the results' description.

Table 4: Use case partners demographics

ID	Size	Offices	Maturity	Subject cybersecurity experience	Structure
1	Small	1	Some controls implemented (Randomly patching and backup)	Some years (non-expert)	Professors, manager, Security team, users (university-hosted start-up)
2	Med	3	everything (introduced by CYSEC) implemented before,	CISO	CEO, security team, employees
3	Med	3	everything (introduced by CYSEC) implemented before, instead of app stores	CISO	CEO, security team, employees
4	Small	2	Some controls implemented	Some years (non-expert)	CEO, security team, employees

2.3.2.1 Interview results for the SME 1

Table 5 gives an overview of the SME 1 opinions about the CYSEC impacts on cybersecurity awareness-raising in the company. The SME worked primarily with the company and malware coaches offered by CYSEC. The interview lasted one hour and 27 minutes.

Table 5: SME 1 interview results

Impact of CYSEC		
Threats and Vulnerabilities		
#	Questions	Subject Statement
1	Not aware before?	We did not have a policy for a strong password and changing the passwords regularly (password management) and a person in charge. We did not do patch management and backups correctly and regularly (awareness of the importance of regular and organised patching and backup). We were not aware of vulnerability about downloading from not trusted sources We were not aware of checking and monitoring software policies (e.g., antimalware policies) We learned new concepts (e.g., CISO) and their security importance.
2	Aware before?	antimalware, limiting access control permission right for virtual machines, blocking malicious website endpoints (a manual process)
3	Missing in CYSEC?	For me, it is difficult to identify since I did not go through all coaches (only checked company and malware coaches) due to a connection problem in the framework and availability of the tool.
4	Irrelevant but still suggested?	The questions are not arranged properly. Why do we need to answer questions about scanning all servers while we do not have windows servers
Controls and Practices		
5	Implemented now and not before?	After CYSEC, we realized that all controls are important, and there is no control that we can ignore. Implemented: (Access control and password policies) After CYSEC, we organised small meetings discussing the problems, and there is a person in charge of managing it and monitoring the plans and goals.
6	Already implemented before?	Randomly patching and backup (no plan for regular patching or backup)
7	Missing in CYSEC?	I do not know exactly; I am learning.
8	Irrelevant but still suggested?	All relevant.
Impact Creation		
9	CYSEC most useful?	We have a lot of online features, when you start a company, you should be aware of all security threats and controls, and we must have CYSEC at the beginning of a start-up.
10	How would you measure the impact?	It [CYSEC] has a high impact, and we have realized about security threats and controls. Now we know the risk of ignoring the implementation of security controls. I understand the threats and efforts to deal with the threats.
11	CYSEC impact rate.	(**5 - fully agree**) for awareness-raising, but (**2.5**) for improving security in our organisation. We were at zero. We thought we were secure, and now we know we are still not in a secure situation.
12	Why? What should be done?	We need to know how to solve the problems (not only presenting the problems). There should be a list of products that you can use. For instance, if you do not have a CISO, CYSEC offers training classes and certification. We need delivery of services and not only telling the solution. Access to patches, training courses, and personalizing security products are some of them.

The subject stated the following comments, suggestions, and opinions about their security issues during the interview. *We do not know how to improve compliance or monitor changes in individuals'* *behaviours. Inside the network, we cannot check if all mobile equipment and personal devices are secure or not, also if the users download applications from trusted stores. Besides, we still have no plan for limiting access control for those people who leave the organisation.*

The subject suggested that instead of asking several questions about different servers (iOS, Mac, Linux, Windows), we should have one question about all servers. *We have antimalware in all servers, why there is a distinction between servers*. Moreover, the subject explained that CYSEC should use simple terminology. *I just want to answer the questions; I did not click on the video to understand what is a CISO. We need to have the relevant information immediately in the questions*.

The subject indicated that *we do not have a CSIRT and security team department. Also, organising processes is difficult for us*.

2.3.2.2 Interview results for the SME 2

Table 6 gives an overview of the SME 2 opinions about the CYSEC impacts on cybersecurity awareness-raising in the company. The SME used and reviewed all offered coaches two times. The interview lasted half an hour.

Table 6: SME 2 interview results

Impact of CYSEC		
Threats and Vulnerabilities		
#	Question	Subject Statement
1	Not aware before?	-
2	Aware before?	everything aware before
3	Missing in CYSEC?	The strategic level of cybersecurity (alignment with business, how you collaborate with c-level), control over third-parties
4	Irrelevant but still suggested?	-
Controls and Practices		
5	Implemented now and not before?	-
6	Already implemented before?	everything implemented before, basic enough
7	Missing in CYSEC?	asset management (e.g., documentation for backups such as for HR systems), architecture (e.g., documentation for access control), monitoring of assets (e.g., XLSIEM), network protection
8	Irrelevant but still suggested?	-
Impact Creation		
9	CYSEC most useful?	the questions would have been so valuable at the beginning of CISO career the added value of making people aware, not necessarily what to do next (offering a choice) a structured way of assessing and planning
10	How would you measure the impact?	The impact is hard to measure point out what has been done by the CISO (e.g., in the first year), considering coach by coach and checking how many of the controls have been implemented (the matter of understanding impact for each company) types of impact: Compliance? Strong sales argument?
11	CYSEC impact rate.	**(4.5, between fully agree and agree)**
12	Why? What should be done?	depends on the questions (are going to be there) depends on budget and person who use the tool Provides quick wins that can be shown to upper management

The subject stated that he has experience in the cybersecurity area; however, he indicated that a tool like CYSEC could help him at the beginning of his job as a person responsible for cybersecurity. He could check the implemented controls, and the tool would provide him with quick wins for presenting to the management.

2.3.2.3 Interview results for the SME 3

Table 7 gives an overview of the SME 3 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.

Table 7: SME 3 interview results

Impact of CYSEC		
Threats and Vulnerabilities		
#	Question	Subject Statement
1	Not aware before?	-
2	Aware before?	All
3	Missing in CYSEC?	Physical access to the hardware (stealing hard drives, copy and obtain the information)
4	Irrelevant but still suggested?	They are basic awareness for our company; however, for our customers, they are very reasonable (e.g., password length, password policy).
Controls and Practices		
5	Implemented now and not before?	-
6	Already implemented before?	All implemented instead of app stores; we are not using android devices in the company,
7	Missing in CYSEC?	More advanced security controls about trusted Boot, and hardware encryption,
8	Irrelevant but still suggested?	All of them are relevant to our customers; however, some are not achievable (for private companies which are not in the IT industry or security context), for instance, response team incidents. Our customers cannot implement some of the controls 100%. Our small customers do not have CISO.
Impact Creation		
9	CYSEC most useful?	Providing follow up checklist for all the security controls we can apply. (Checklist to be sure you do not forget)
10	How would you measure the impact?	We used CYSEC at a pilot level, We know all controls, and we have developed awareness. We worked a long time on security. We are a security company. We have high-level security skills.
11	CYSEC impact rate.	**(3 - neither agree nor disagree)**
12	Why? What should be done?	A checklist is interesting, but we know all, CYSEC is more useful for us if you add more advanced security controls such as trusted boot, and hardware encryption,

The subjects stated that they are a security company and are familiar with all security control in CYSEC. They emphasised that although the tool is very useful for their customers, it should have included advanced security controls to be more useful for the company.

2.3.2.4 Interview results for the SME 4

Table 8 gives an overview of the SME 4 opinions about the CYSEC impacts on cybersecurity awareness-raising in the company. The SME confirmed that it worked with CYSEC and reported that they had used all coaches for introducing their new employees. The interview lasted half an hour.

Table 8: SME 4 interview results

Impact of CYSEC		
Threats and Vulnerabilities		
#	Question	Subject Statement
1	Not aware before?	We knew about them but not well protected, before CYSEC it was hard to get knowledge, now it is easier since there are a lot of links of knowledge in the coaches. We gained more knowledge in the CYSEC links.
2	Aware before?	All, we had some knowledge; the tool provided us with more knowledge
3	Missing in CYSEC?	-
4	Irrelevant but still suggested?	everything is relevant to us
Controls and Practices		
5	Implemented now and not before?	We use the coaches for the new employees; they are doing coaches and get knowledge (training) at the beginning, every employee does some courses
6	Already implemented before?	I do not know what was exactly, because I joined the company after the beginning of the SMESEC project.
7	Missing in CYSEC?	Coaches about data flow prevention, how employees should work remotely, usage of VPNs,
8	Irrelevant but still suggested?	everything is relevant
Impact Creation		
9	CYSEC most useful?	I think CYSEC has a company orientation and not employee orientation. It would be good if there are coaches and training content for new employees (employees who have no idea about security, about email, password, malicious link) to improve their level of knowledge. Having personalised coaches for each company
10	How would you measure the impact?	It is hard to measure that because, after doing some coaches, we found some points that could be more protected, we can always do more to be better protected.
11	CYSEC impact rate.	**(4 - agree)**
12	Why? What should be done?	It gives us knowledge and what is missing in our company, impact security in our company, There should be more coaches, it means more knowledge, having a mobile version of the coaches is very good, and some notification about new coaches can help. Some issues about stability, (I know you are developing the tool, and it is not very important)

The subject stated that they are also using CYSEC for new employees to measure their level of knowledge and awareness. Moreover, the subject indicated that since some companies' employees are working remotely after the corona pandemic, it would be nice to have some coaches about remote work cybersecurity.

2.3.3 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 interview results.

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

CYSEC provided knowledge and had a positive impact on security awareness for those SMEs that were not experts in cybersecurity. The immediate relevance of the training material and self-assessment questions provided by the CYSEC tool affected the subjects' overall understanding of the status of security in their companies and made changes in the companies' activities. *SME1: "It [CYSEC] has a high impact, and we have realized about security threats and controls. Now we know the risk of ignoring the implementation of security controls. I understand the threats and efforts to deal with the threats. After CYSEC, we realized that all controls are important, and there is no control that we can ignore. We did not do patch management and backups correctly and regularly. We were not aware of vulnerability about downloading from not trusted sources. We were not aware of checking and monitoring software policies (e.g., antimalware policies)." SME4: "Before CYSEC, it was hard to get knowledge, now it is easier since there are a lot of links of knowledge in the coaches. We gained more knowledge in the CYSEC links. We had some knowledge [about all threats and vulnerabilities in the CYSEC], the tool provided us with more knowledge."* In addition, SME1 and SME4 explained new activities in their companies after using CYSEC. *SME1: "After CYSEC, we organised small meetings discussing the problems, and there is a person in charge of managing it and monitoring the plans and goals." SME4: "We use the coaches for the new employees; they are doing coaches and get knowledge (training) at the beginning."*

For the companies that were experts in cybersecurity and the subjects have expertise in security already, CYSEC had no impact on the SME's security awareness improvement. *SME2:* "*We were aware of everything before using CYSEC and implemented all basic enough."* SME3 explained that although CYSEC had no impact on security awareness, it can be useful for their customers. *SME3:" We were aware of all. they are basic awareness for our company; however, for our customers, they are very reasonable (e.g., password length, password policy)."*

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

The answer to RQ3 is based on a Likert question at the end of each study to gain the SME end-users' attitudes about the impact of CYSEC. 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) and justified their evaluation. Table 11 shows the users' scores.

Table 9: Perceived CYSEC usefulness
(5 - fully agree, 4 - agree, 3 - neither agree nor disagree, 2 - disagree, 1 - fully disagree)

	SME1	SME2	SME3	SME4
Usefulness	5 (for awareness-raising) 2.5 (for improving security)	4.5	3	4

SME1 provided two scores to differentiate between the awareness-raising and security improvement impact. *SME1: "We thought we were secure, and now we know we are still not in a secure situation. We need delivery of services and not only telling the solution."* SME2 explained that *"It [CYSEC] provides quick wins that can be shown to upper management." SME3: "We know all controls, and we have developed awareness. We worked a long time on security. We are a security company. We have high-level security skills. CYSEC is more useful for us if you add more advanced security controls."*

SME4: "It gives us knowledge and what is missing in our company and impact security in our company. There should be more coaches; it means more knowledge." SME4 pointed to the stability issues in CYSEC. *SME4: "There were some issues about stability; I know you are developing the tool, and it is not very important."*

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

If CYSEC wants to maximise its impact, it needs to support the diversity of the users and SMEs by providing relevant and personalised knowledge and capabilities. The provided knowledge should cover basic and also advanced levels of security awareness. Moreover, the tool should offer even more practical solutions. *SME1: "We need to know how to solve the problems (not only presenting the problems). We do not know how to improve compliance or monitor changes in individuals' behaviours. There should be a list of products that you can use. For instance, if you do not have a CISO, CYSEC offers training classes and certification. Access to patches, training courses, and personalizing security products are some of them." SME4: "I think CYSEC has a company orientation and not employee orientation. It would be good if there are coaches and training content for new employees (employees who have no idea about security, about email, password, malicious link) to improve their level of knowledge. Also, we need to have personalised coaches for each company."* SME2 and SME3 wanted to have more advanced level coaches. *Comapny3: "They are basic, more advanced security controls are missing."*

Table 10 shows the SMEs' opinions about the missing knowledge and capabilities in CYSEC.

Table 10: Missing knowledge and capabilities

Use case	Missing Capabilities
SME1	-
SME2	The strategic level of cybersecurity (alignment with business, how you collaborate with c-level), control over third-parties asset management (e.g., documentation for backups such as for HR systems), architecture (e.g., documentation for access control), monitoring of assets (e.g., XLSIEM), network protection
SME3	physical access to hardware advanced security controls about trusted Boot, and hardware encryption
SME4	data flow prevention, how employees should work remotely, and usage of VPNs

3 Meeting SMEs to increase awareness in security

SMESEC has carried out many actions at several events in particular in the second year and documented in the D6.3 This gave already opportunity to meet SMEs. The information below focus on the 3rd and outstanding events in the period 2019-2020 showing SMESEC framework available.

3.1 Meeting SMEs at large event – the FIC 2020

As decided in the dissemination strategy (See D6.4) we found a big Cybersecurity related event in the 3rd period to show the SMESEC framework and get feedback from SMEs.

We decided to go to the International Cybersecurity Forum , a big event called FIC 2020 held in Lille from 28 to 30 visitors (see https://www.forum-fic.com/en/home.htm

FIC 2020
International Cybersecurity Forum
28th,29th & 30th January 2020
LILLE GRAND PALAIS

The International Cybersecurity Forum (FIC) is the leading European event on Cybersecurity. The event relies on: a TRADE SHOW for buyers and suppliers of cybersecurity solutions to meet and network and a FORUM to foster reflection and exchanges among the European cybersecurity ecosystem. The International Cybersecurity Forum, place for open discussions and debate, welcomed in 2020 more than 450 speakers, through 4 plenary sessions, 33 round tables, 24 conferences, 35 technical demonstrations and 15 masterclass.!

This was a big opportunity for SMESEC to be present in an event which attracted +12500 visitors and 488 million of internet views

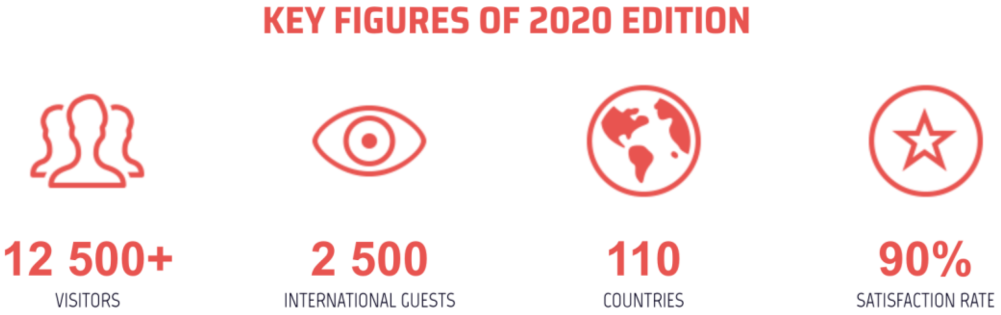
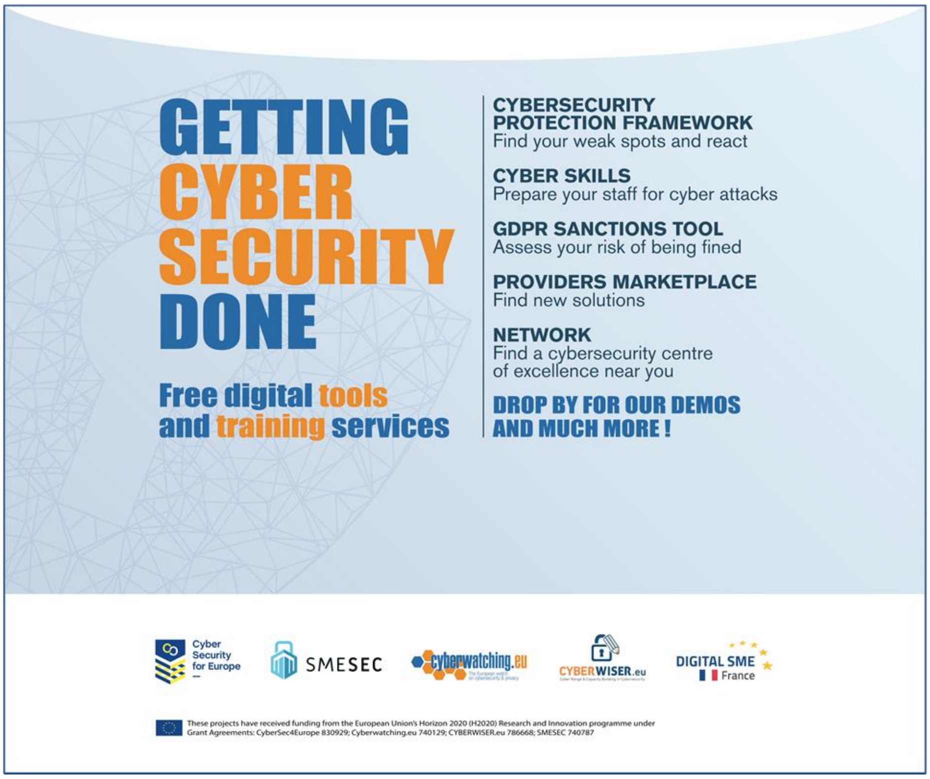


Figure 4: photos on showing massive attendance at FIC2020

SMESEC drove its presence and decided to contact 4 other EU partners to join forces to promote their offers to SMEs with the following messages:



GETTING CYBER SECURITY DONE

Free digital tools and training services

CYBERSECURITY PROTECTION FRAMEWORK
Find your weak spots and react

CYBER SKILLS
Prepare your staff for cyber attacks

GDPR SANCTIONS TOOL
Assess your risk of being fined

PROVIDERS MARKETPLACE
Find new solutions

NETWORK
Find a cybersecurity centre of excellence near you

DROP BY FOR OUR DEMOS AND MUCH MORE !

Cyber Security for Europe
SMESEC
cyberwatching.eu
The European watch on cybersecurity & privacy
CYBERWISER.eu
DIGITAL SME France

These projects have received funding from the European Union's Horizon 2020 (H2020) Research and Innovation programme under Grant Agreements: CyberSec4Europe 830929; Cyberwatching.eu 740129; CYBERWISER.eu 786668; SMESEC 740787

Figure 5: design of the "wall" on the common EU Cybersecurity projects

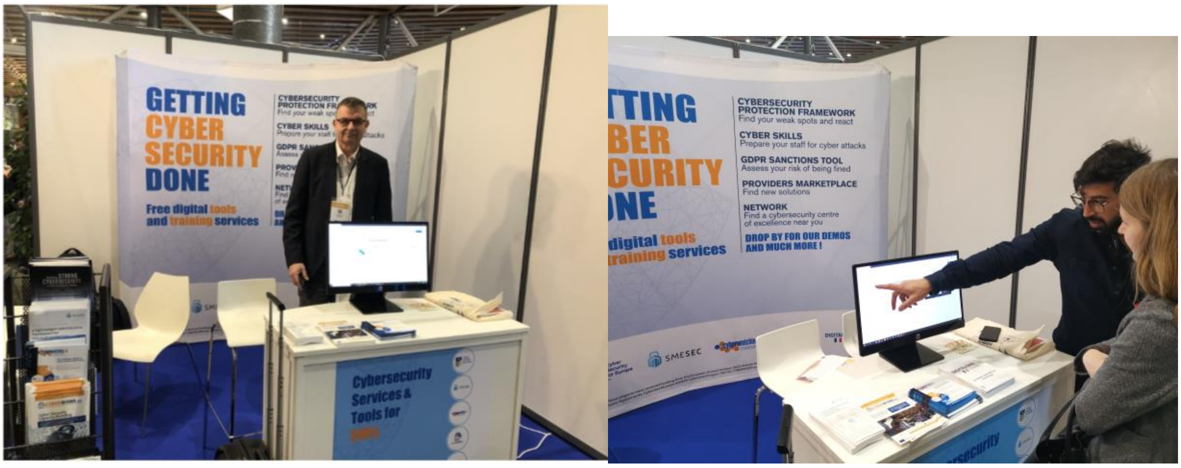


Figure 6: P.Cousin and H. Baqua from EGM at SMEESEC booth, FI2020

`

We had a lot of interest and contacts. The organizer set also a “SMEs pathway” which bring SMEs to specific booth like ours. The big companies including SMEs MEDEF (see 3.3) was also active to promote our offers.

3.2 The cooperation at EU level with other projects

At FIC we cooperate with 3 other EU projects as well as with Digital SME alliance

All three initiatives are tackling cybersecurity and privacy from complementary perspectives, providing European SMEs with key resources to boost their online security:

- CyberSec4Europe is one of the four recently funded competence pilot projects aiming at setting up a European network of centres of cybersecurity expertise.
  The project activities range from combining formal, professional and non-traditional cybersecurity skills sand capacity building to open-source tools development to support cybersecurity education, software testing, and certification of hardware and software products.
- CYBERWISER.eu delivers a flexible, risk-centred, capacity-building platform, combining a theoretical and practical approach to cybersecurity with innovative features (including a cutting edge cyber range). CYBERWISER.eu implements customisable training pathways in cybersecurity to fit a broad range of needs and capacity building targets.
- Cyberwatching joined key initiatives aiming at raising awareness on cybersecurity and bringing into the spotlight key services,
- SMESEC proposes a cost-effective framework composed of specific cyber-security tool-kits to support SMEs in managing network information security risks and threats including: detection and alerting tools, threat protection and response as well as awareness and trainingtutorials.

The joint info booth was supported by Digital SME Alliance France which promotes a European oriented approach towards the development of French SMEs active in Information and Communication Technologies.

See below the design of the welcome desk at FIC2020 :

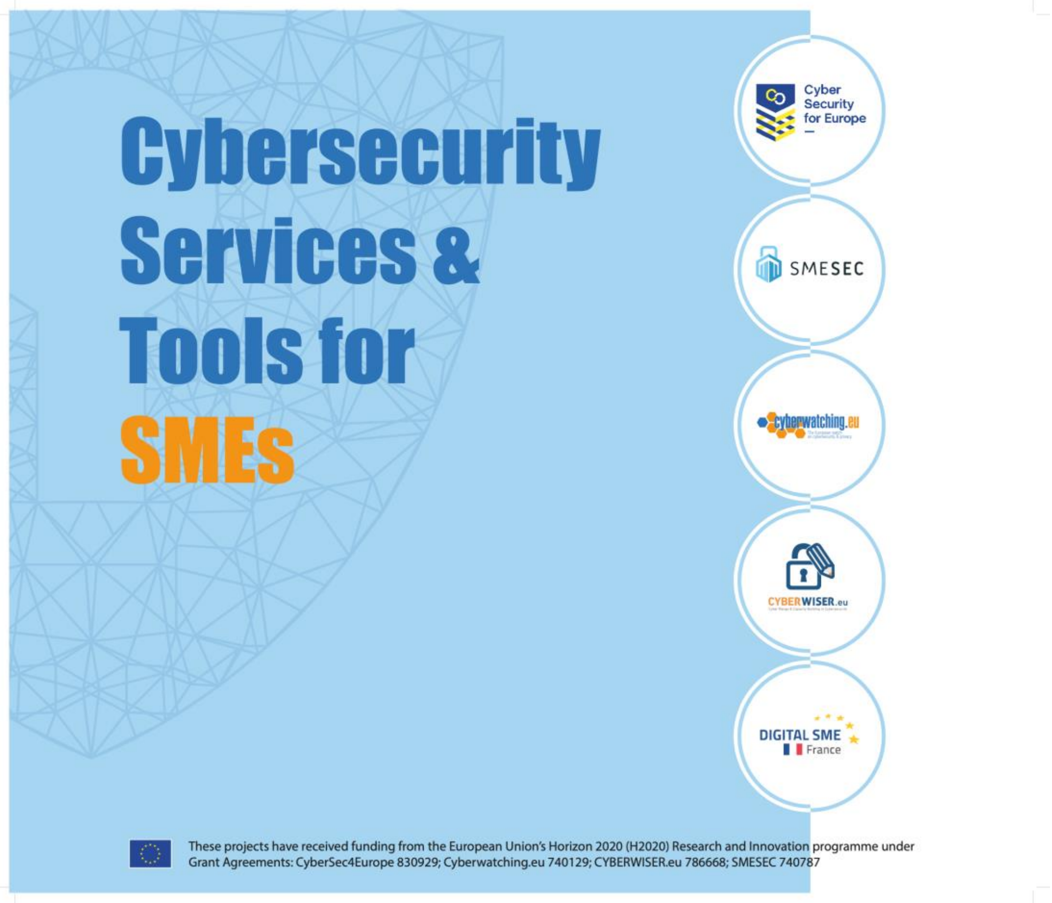

Cybersecurity
Services &
Tools for
SMEs
Cyber Security for Europe
SMESEC
cyberwatching.eu
CYBERWISER.eu
DIGITAL SME France
These projects have received funding from the European Union's Horizon 2020 (H2020) Research and Innovation programme under Grant Agreements: CyberSec4Europe 830929; Cyberwatching.eu 740129; CYBERWISER.eu 786668; SMESEC 740787

Figure 7: design of the welcome desk at FIC2020

While SMESEC has already several talks and cooperation with other cubersecurity related EU projects such as with Cyberwatching.eu, the cooperation leading to the common booth in FIC2020 lead to improve overall cooperation. In particular Cyberwiser organized a workshop at FIC 2020 where SMESEC participated as shown below:

CYBERWISER.eu
Cyber Range & Capacity Building in Cybersecurity
2nd CYBERWISER.eu
Open Pilots Workshop
Your chance to train your staff, to face cybersecurity threats and attacks, for free.
Lille Grand Palais, Lille, France
31st January 2020
Only few more seats available
Register now!
Conveniently located in the same premises of the FIC event
FIC 2020
Forum International de la Cybersécurité
28, 29 & 30 janvier 2020
LILLE GRAND PALAIS
Date: Friday, 31 January, 2020

The key message and information of the workshop were the following:

Your chance to train your staff, for free

Prepare your company to face cybersecurity threats and attacks

Lille, 31st January 2020 – Lille Grand Palais, 1 Boulevard des Cités Unies, 59777 - Salle: Rotterdam 1 and 2

Despite rising concerns about information security risks, companies and organisations around Europe are desperate for cybersecurity talent. This is especially true for SMEs, as as they often lack both the time and resources to attract, hire, train, retain, and equip such talent.

This workshop will give the opportunity to SMEs to define a customised learning path based on their specific needs and train their staff for free by joining the Open Pilot programme of the CYBERWISER.eu project. The Open Pilot programme allow SMEs to freely use the risk-centred, capacity building platform, combining a theoretical and practical approach to cybersecurity with innovative features including a cutting edge cyber range.

Content of the workshop

The workshop is a mix of motivational, panel and training sessions in which attendees will get the chance to know the key elements of the CYBERWISER.eu online platform through a live demo, define with the CYBERWISER.eu experts their own customisable training pathway to specifically fit their needs and actually test the platform through an interactive session involving a simple exercise in a simulated environment.

The workshop will also introduce attendees to complementary tools and services to support the cybersecurity needs of SMEs coming from other European R&I initatives.

Who should attend?

The workshop is for organisations, **especially** but not limited to **SMEs**, seeking a qualified entry point to cybersecurity training and advisory services.

Given that cybersecurity is not just an IT issue, the workshop will cater for both IT specialists and a wider audience including employees from all departments and at all levels of seniority.

What's in it for me?

If you're looking for guidance or a complete cybersecurity solution for your organisation, seize the opportunity to get in front of Europe's leading cybersecurity experts!

By participating you can:

- Present your organisation to the workshop attendees in a dedicated session
- Discuss the specific needs of your cybersecurity training pilot with the CYBERWISER.eu team
- Test the platform in a live session
- Meet cybersecurity experts from all over Europe and build your network

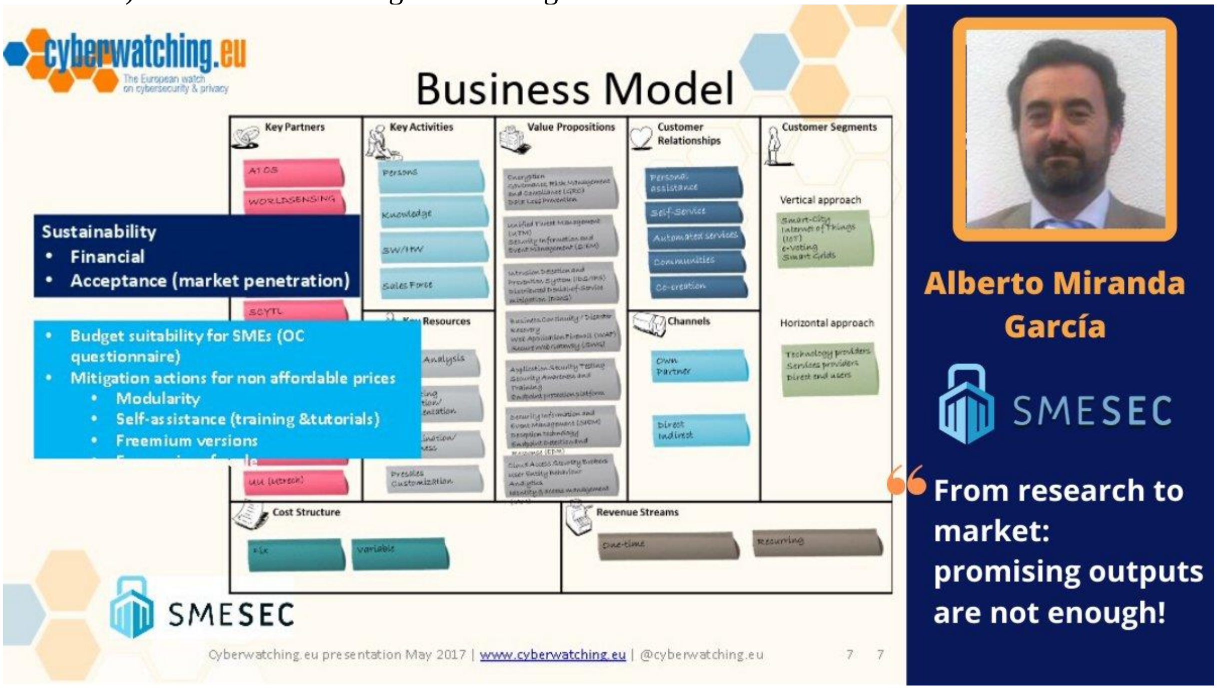
The bottom line

- Jumpstart your own Pilot with CYBERWISER.eu: Gain hands-on experience on the platform and outline the specs of your pilot with our team of experts.
- Get to know complementary cybersecurity tools and services: Practical tools and services as well as opportunities to synergies with initiatives such as CyberSec4Europe, ECHO, Cyberwatching.eu and SMESEC

SMESEC
Cybersecurity for SMEs
increase your awareness
be ready, protected and aware
General presentation
CYBERWISER.eu
Pitch the needs of your own pilot & we'll train you!
SMESESC Training Platform
A wide selection of cybersecurity courses (Beginners to experts)
Public and private courses.
Flexible courses management.
User-friendly interface.

Figure 8: P.Cousin, SMESEC representative presenting SMESEC

Also SMESEC representative participated to several discussions and webinars such as the webinar "From Research to Market: Promising Outputs are not Enough!" on March 11Th organized by Cuberwatching.eu This webinar focused on improving project market readiness topics to identify the timing for project exploitation. In the webinar, three H2020 projects (PROTECTIVE, GHOST, and SMESEC) shared their knowledge and findings.


cyberwatching.eu
The European watch on cybersecurity & privacy
Key Partners
Key Activities
Value Propositions
Customer Relationships
Customer Segments
Key Resources
Channels
Cost Structure
Revenue Streams
ATOS
WORLDSENSING
SCYTL
UU (Utrecht)
Persons
Knowledge
SW/HW
Sales Force
Analysis
Presales Customization
Personal assistance
Self-Service
Automated services
Communities
Co-creation
Own Partner
Direct Indirect
Vertical approach
Smart-City
Internet of Things (IoT)
e-Voting
Smart Grids
Horizontal approach
Technology providers
Services providers
Direct end users
Fix
Variable
One-time
Recurring

Business Model

Sustainability
- Financial
- Acceptance (market penetration)

- Budget suitability for SMEs (OC questionnaire)
- Mitigation actions for non affordable prices
  - Modularity
  - Self-assistance (training &tutorials)
  - Freemium versions

SMESEC

Cyberwatching.eu presentation May 2017 | www.cyberwatching.eu | @cyberwatching.eu 7 7

Alberto Miranda García

SMESEC

From research to market: promising outputs are not enough!

Alberto Miranda Garcia (Senior Business Consultant at Atos) presented the SMESEC framework, project partners, open call partners, the generation of the business model, and the findings of the project from the exploitation perspective. Knowledge-sharing and interaction with H2020 projects can provide SMESEC with opportunities for future improvement.

More information: https://www.cyberwatching.eu/research-market-promising-outputs-are-not-enough

We should also recall the successful "Cybersecurity Standards Workshop: impacts and gaps for SMEs" which was a one-day workshop hosted by CEN & CENELEC Management Center and intended to support SMEs in the relevant cybersecurity policies, rules, and standards. Also, Cenelec on cybersecurity, ETSI TC Cyber, Digital SME Alliance, and European Cybersecurity Organization (ECSO) are participating. The workshop took place in Brussels on May 24, 2019, from 10:00 to 16:00.

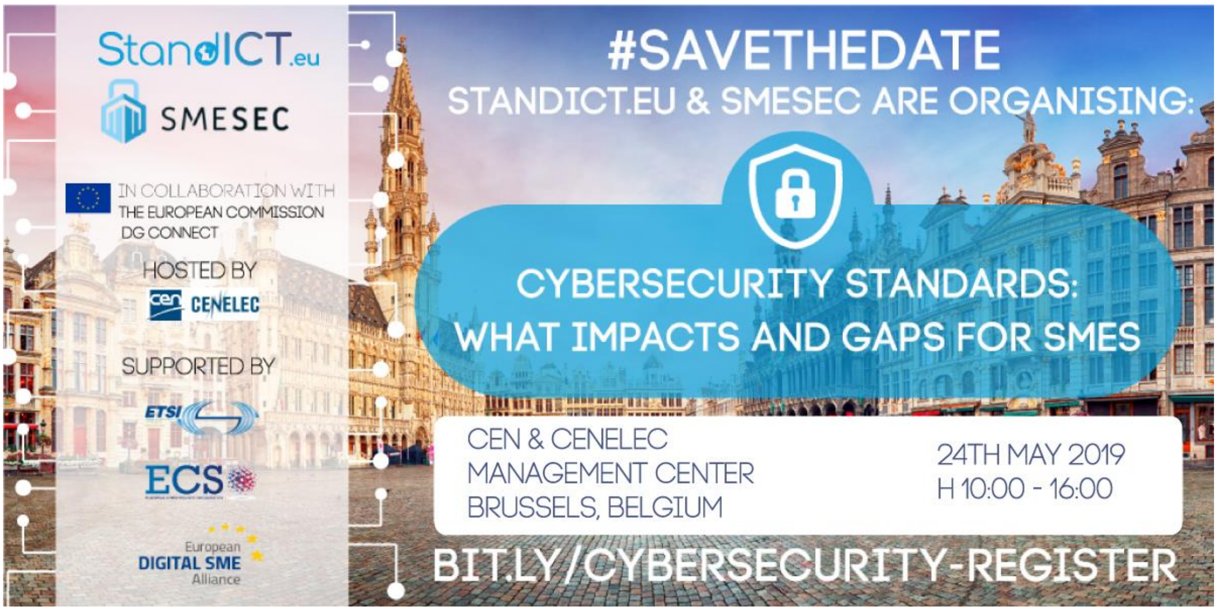


Figure 9: invitation to Cybersecurity standards for SMEs

SMESEC and StandICT come together and invited all innovators, ICT SMEs, SMEs associations, policy makers and funding agencies to come together to assess the future priorities and challenges in cybersecurity standardisation. In this workshop, not only will SMEs acquire practical knowledge about SME related cybersecurity standards, they may join a big cybersecurity community and apply for an open call.

The workshop helped to set the scene to develop a guideline for SMEs and engaged key supporter such as CEN and ETSI TC CYBER representative leading to the acceptance of SMESEC contributions . see more detailed in the deliverable D6.4

3.3 The SME associations

3.3.1 The IT Forum - Denmark

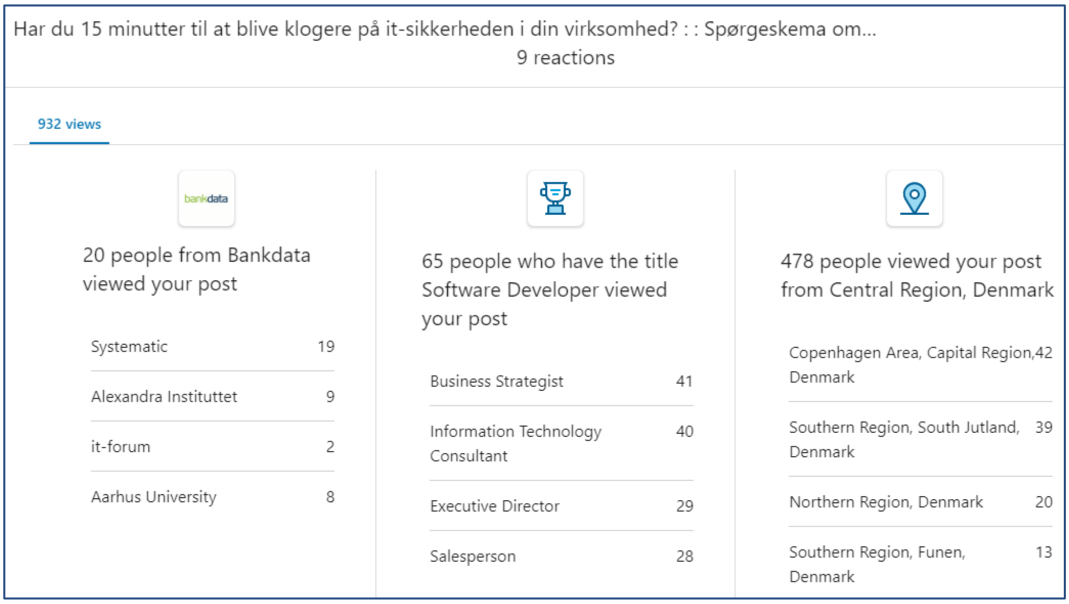
From the open call, an SME association was selected to help promoting SMESEC at larger scale and give feedback on SMESEC framework from multiple users perspective.

The selected association was the IT Forum in Denmark.I t-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.

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 2.5 and 2.6 for LinkedIn statistics.



Har du 15 minutter til at blive klogere på it-sikkerheden i din virksomhed? : : Spørgeskema om...
9 reactions

932 views

20 people from Bankdata viewed your post

Systematic	19
Alexandra Instituttet	9
it-forum	2
Aarhus University	8

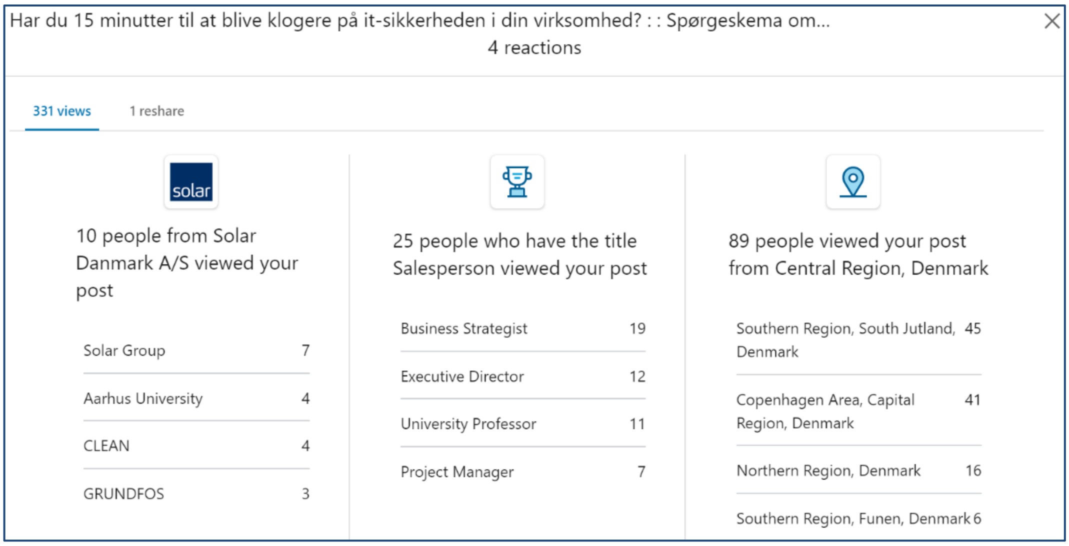
65 people who have the title Software Developer viewed your post

Business Strategist	41
Information Technology Consultant	40
Executive Director	29
Salesperson	28

478 people viewed your post from Central Region, Denmark

Copenhagen Area, Capital Region, Denmark	42
Southern Region, South Jutland, Denmark	39
Northern Region, Denmark	20
Southern Region, Funen, Denmark	13

Figure 2.5 – detailed numbers from CEO's share on LinkedIn.



Har du 15 minutter til at blive klogere på it-sikkerheden i din virksomhed? : : Spørgeskema om...
4 reactions

331 views 1 reshare

10 people from Solar Danmark A/S viewed your post

Solar Group	7
Aarhus University	4
CLEAN	4
GRUNDFOS	3

25 people who have the title Salesperson viewed your post

Business Strategist	19
Executive Director	12
University Professor	11
Project Manager	7

89 people viewed your post from Central Region, Denmark

Southern Region, South Jutland, Denmark	45
Copenhagen Area, Capital Region, Denmark	41
Northern Region, Denmark	16
Southern Region, Funen, Denmark	6

Figure 2.6 – detailed numbers from CCO's share on LinkedIn.

Total number of views for the two posts was 1.263

After have shared access to the online form and information about SMESEC several times in November and December 2019 the number of completed questionnaires was very disappointing.

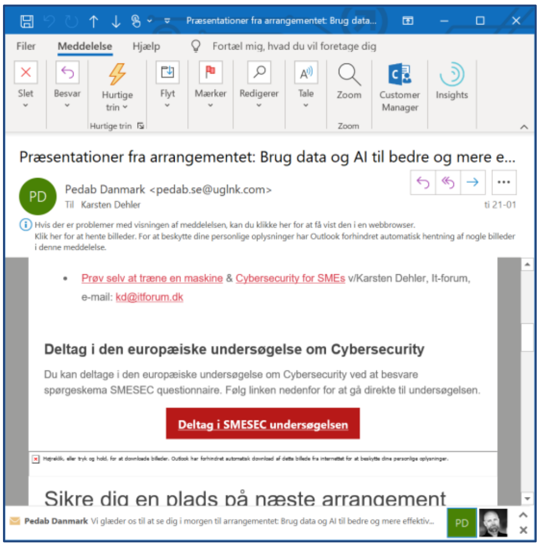
Final list of actions taken:

- Two newsletters/direct mails in November 2019

- Two dedicated LinkedIn post in December 2019
- Two psychical events in Vejle and Aarhus in January 2020

In January 2020 we had two physical events where CEOs, CTOs and other “strategic decisionmakers” where invited. The events where 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 bee found in Appendix 1].

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 v]. The deadline for completion was set to Friday the of January.



Præsentationer fra arrangementet: Brug data og AI til bedre og mere e...

PD Pedab Danmark <pedab.se@uglnk.com>
Til Karsten Dehler
ti 21-01

Hvis der er problemer med visningen af meddelelsen, kan du klikke her for at få vist den i en webbrowser.
Klik her for at hente billeder. For at beskytte dine personlige oplysninger har Outlook forhindret automatisk hentning af nogle billeder i denne meddelelse.

- Prøv selv at træne en maskine & Cybersecurity for SMEs v/Karsten Dehler, It-forum, e-mail: kd@itforum.dk

Deltag i den europæiske undersøgelse om Cybersecurity

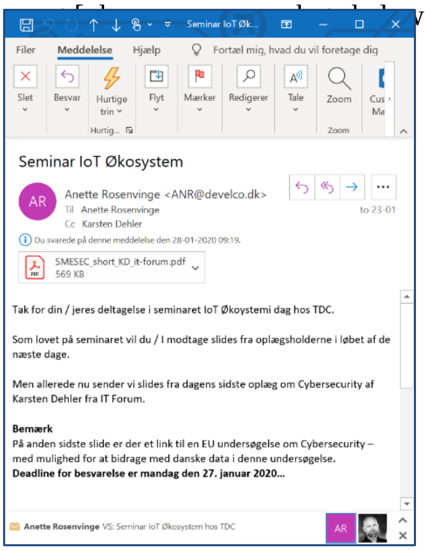
Du kan deltage i den europæiske undersøgelse om Cybersecurity ved at besvare spørgeskema SMESEC questionnaire. Følg linken nedenfor for at gå direkte til undersøgelsen.

Deltag i SMESEC undersøgelsen

Højreklik, eller tryk og hold, for at downloade billeder. Outlook har forhindret automatisk download af dette billede fra internettet for at beskytte dine personlige oplysninger.

Sikre dig en plads på næste arrangement

Pedab Danmark Vi glæder os til at se dig i morgen til arrangementet: Brug data og AI til bedre og mere effektiv...



Seminar IoT Økosystem

AR Anette Rosenvinge <ANR@develco.dk>
Til Anette Rosenvinge
Cc Karsten Dehler
to 23-01

Du svarede på denne meddelelse den 28-01-2020 09:19.

SMESEC_short_KD_it-forum.pdf
569 KB

Tak for din / jeres deltagelse i seminaret IoT Økoystemi dag hos TDC.

Som lovet på seminaret vil du / I modtage slides fra oplægsholderne i løbet af de næste dage.

Men allerede nu sender vi slides fra dagens sidste oplæg om Cybersecurity af Karsten Dehler fra IT Forum.

Bemærk
På anden sidste slide er der et link til en EU undersøgelse om Cybersecurity – med mulighed for at bidrage med danske data i denne undersøgelse.
Deadline for besvarelse er mandag den 27. januar 2020...

Anette Rosenvinge VS: Seminar IoT Økosystem hos TDC

Figure 3.1 – examples on follow up email.

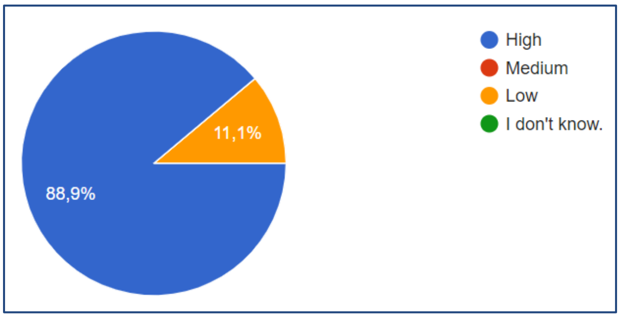
In both events other presenters where talking about the potential of Digital Transformation and my expectation was that adding the Cyber Security aspect here would create interest from the participants as they got the “all-around image” of the whole AI/IoT ecosystem. Addressing non-technical matters 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 have succeeded in this task and for me personal I have tried to create a user without any luck. Therefore, the personal interviews have not been carried out as planned.

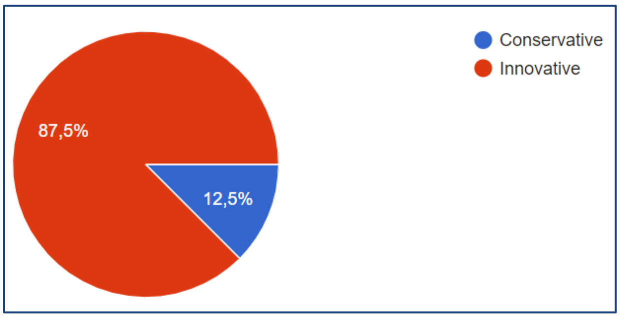
Access to online survey has been broadcasted as mentioned above. The introduction and background have been in Danish but info about SMESEC and the online questionnaire in English also asking the participants to please give their replies in English

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

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



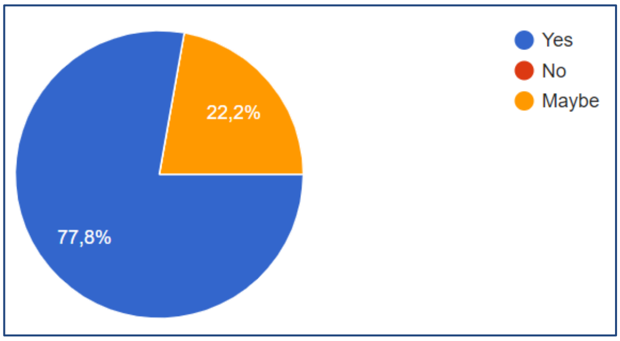
2) Do you think the SMESEC Framework is conservative or innovative ?



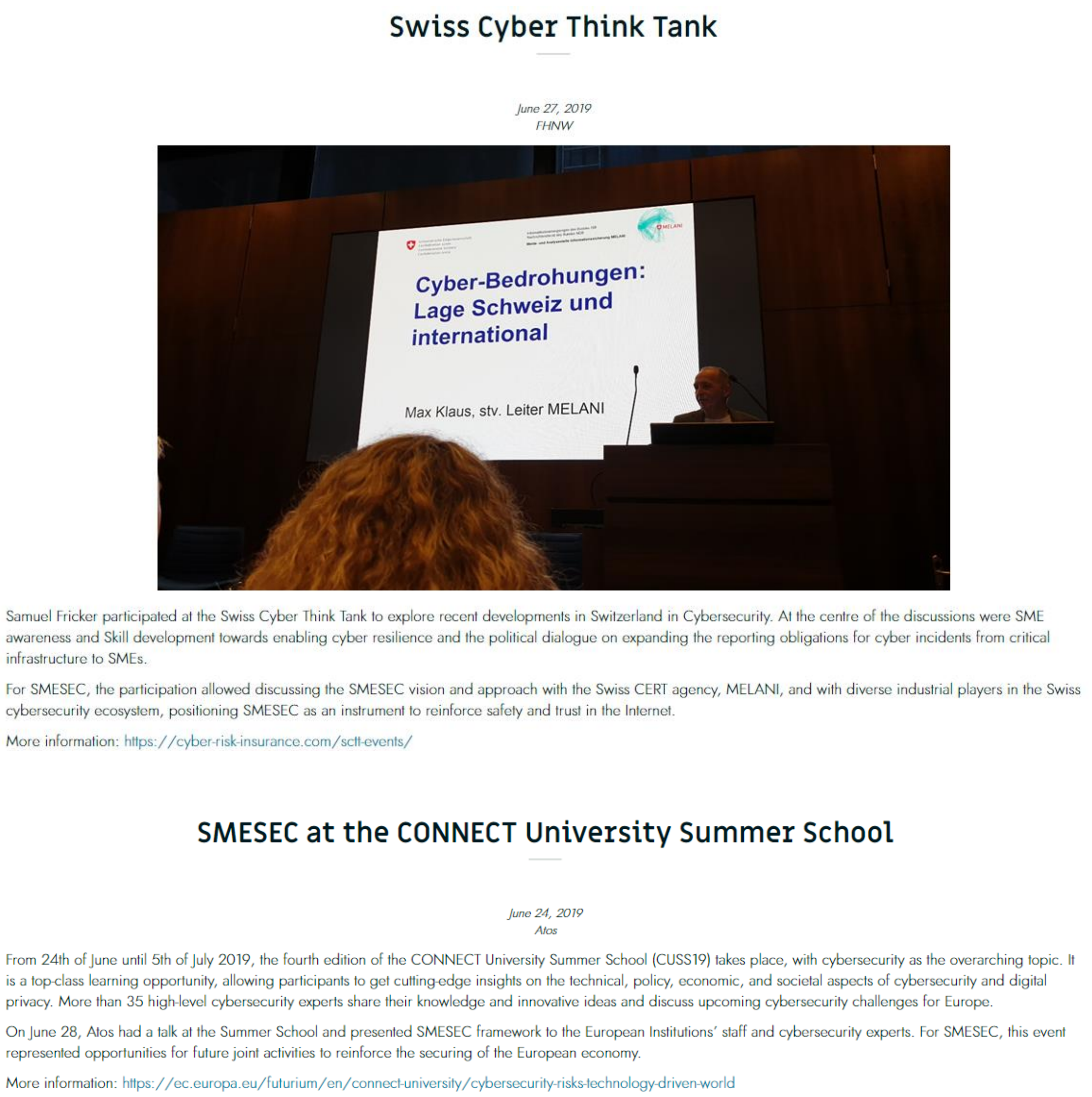
So, a vast majority of the participants are rates the Integrity of the organization's critical information as high (89,9%) and 87,5% of the participants finds SMESEC Innovative.

Even though we must be careful not to conclude to 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 you services or products?



3.3.2 The Swiss Cyber think thank



Swiss Cyber Think Tank

June 27, 2019
FHNW

Samuel Fricker participated at the Swiss Cyber Think Tank to explore recent developments in Switzerland in Cybersecurity. At the centre of the discussions were SME awareness and Skill development towards enabling cyber resilience and the political dialogue on expanding the reporting obligations for cyber incidents from critical infrastructure to SMEs.

For SMESEC, the participation allowed discussing the SMESEC vision and approach with the Swiss CERT agency, MELANI, and with diverse industrial players in the Swiss cybersecurity ecosystem, positioning SMESEC as an instrument to reinforce safety and trust in the Internet.

More information: https://cyber-risk-insurance.com/sctt-events/

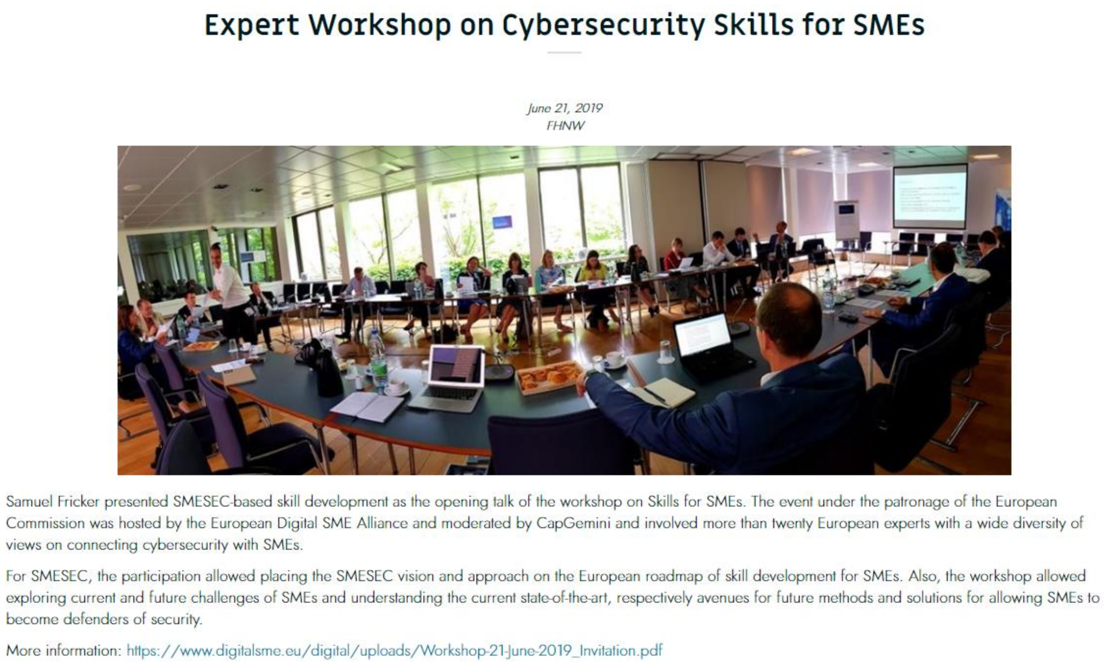
SMESEC at the CONNECT University Summer School

June 24, 2019
Atos

From 24th of June until 5th of July 2019, the fourth edition of the CONNECT University Summer School (CUSS19) takes place, with cybersecurity as the overarching topic. It is a top-class learning opportunity, allowing participants to get cutting-edge insights on the technical, policy, economic, and societal aspects of cybersecurity and digital privacy. More than 35 high-level cybersecurity experts share their knowledge and innovative ideas and discuss upcoming cybersecurity challenges for Europe.

On June 28, Atos had a talk at the Summer School and presented SMESEC framework to the European Institutions' staff and cybersecurity experts. For SMESEC, this event represented opportunities for future joint activities to reinforce the securing of the European economy.

More information: https://ec.europa.eu/futurium/en/connect-university/cybersecurity-risks-technology-driven-world



Expert Workshop on Cybersecurity Skills for SMEs

June 21, 2019
FHNW

Samuel Fricker presented SMESEC-based skill development as the opening talk of the workshop on Skills for SMEs. The event under the patronage of the European Commission was hosted by the European Digital SME Alliance and moderated by CapGemini and involved more than twenty European experts with a wide diversity of views on connecting cybersecurity with SMEs.

For SMESEC, the participation allowed placing the SMESEC vision and approach on the European roadmap of skill development for SMEs. Also, the workshop allowed exploring current and future challenges of SMEs and understanding the current state-of-the-art, respectively avenues for future methods and solutions for allowing SMEs to become defenders of security.

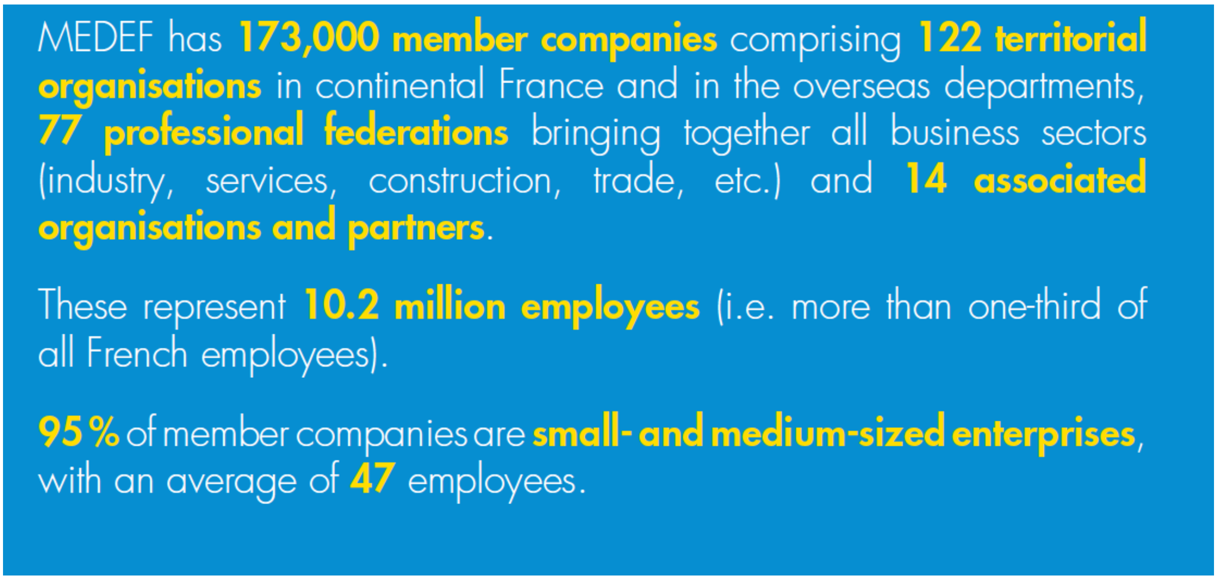
More information: https://www.digitalsme.eu/digital/uploads/Workshop-21-June-2019_Invitation.pdf

3.3.3 The French MEDEF

SMESEC has established an active liaison with French MEDEF which represent +160K SMEs !!

The MEDEF is the leading network of entrepreneurs in France. Over 95% of the businesses belonging to the MEDEF are SMEs. The MEDEF places job creation and sustainable growth at the heart of its action. It promotes entrepreneurship and defends free enterprise.

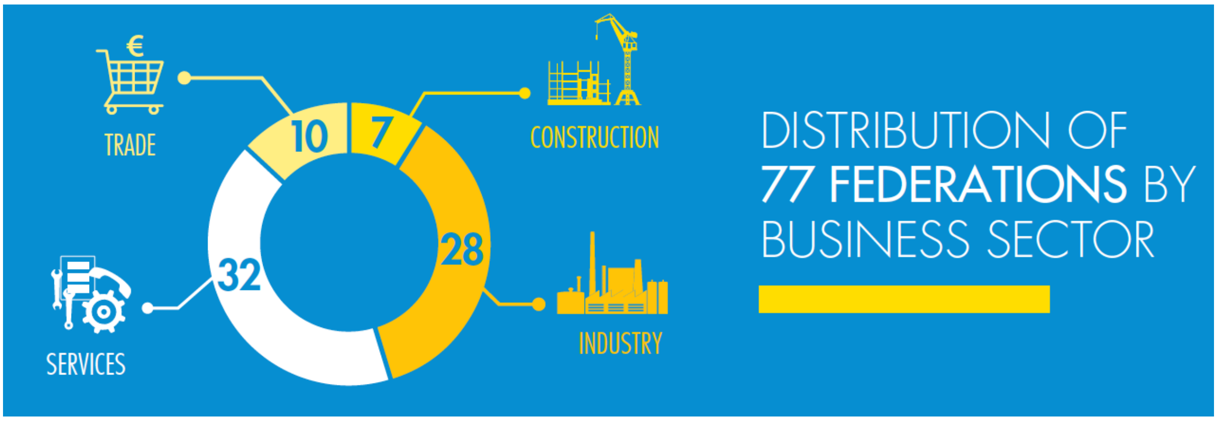
The MEDEF maintains a dialogue with all the actors of civil society and, with the various decision-makers, works towards achieving a better understanding of the constraints and the strengths of businesses. Some figures :



MEDEF has **173,000 member companies** comprising **122 territorial organisations** in continental France and in the overseas departments, **77 professional federations** bringing together all business sectors (industry, services, construction, trade, etc.) and **14 associated organisations and partners**.

These represent **10.2 million employees** (i.e. more than one-third of all French employees).

95 % of member companies are **small- and medium-sized enterprises**, with an average of **47** employees.



MEDEF has a specific Cybersecurity working group and we had several discussions at teleconference with MEDEF to present SMESEC framework . The discussions were intensified end of 2019 when SMESEC framework was available including CYSEC which got great attention to them.

We studied the CYSEC translation to French and this is still ongoing for future actions. End January 2020 MEDEF supported the SMESEC booth at FIC2020 and bring many SMEs to us. MEDEF confirmed interested for the SMESEC framework and more particularly the CYSEC. In French. As soon as this version will be available it could get great attention within the French network.

3.3.4 SMEs in Spain

Atos is an active member of different associations and platforms aiming at boosting the implementation of information technologies at different levels. Taking advantage of our membership, Atos contacted two of these initiatives, Planetic and Turistec, in order to engage a larger amount of SMEs from different industries as in the SMESEC survey to get their experience in cybersecurity mattes.

More specifically, Planetic (a national technological platform to boost the ICT adoption and promotion in Spain) where Atos is currently holding the Presidency and Secretary, included a link to the survey in its weekly bulletin. This bulletin reaches around 360 recipients and is available on the platform website.

Turistec is an international cluster, dedicated to Information and Communication Technologies applied to tourism; this cluster gathers tourism Industry leaders, SME's, entrepreneurs, University of the Balearic Islands (UIB), knowledge centers and entities dedicated to excellence and quality. Together we concentrate the knowledge equivalent to more than half a century experience in the development of a tourist destination. As part of its communication activities, Turistec contacted all its partners to inform about SMESEC objectives and the link to the survey.

3.3.5 SMEs in Greece

In 2020 FORTH promoted the final SMESEC quiz through PRAXIS network to many SMEs via email. (still waiting for the exact number of receivers) The same quiz was also promoted through FORTH's social media with more than 3k followers each and was republished by STEP-C science park. (i)https://twitter.com/ICS_FORTH/status/1255819660618092544

(ii)https://www.linkedin.com/posts/icsforth_a-lightweight-cybersecurity-framework-for-activity-6661585500140380160-LVrq

(iii)https://www.facebook.com/ICSFORTH/posts/1962345197224087

In 2019 FORTH promoted the SMESEC Open Call via PRAXIS network

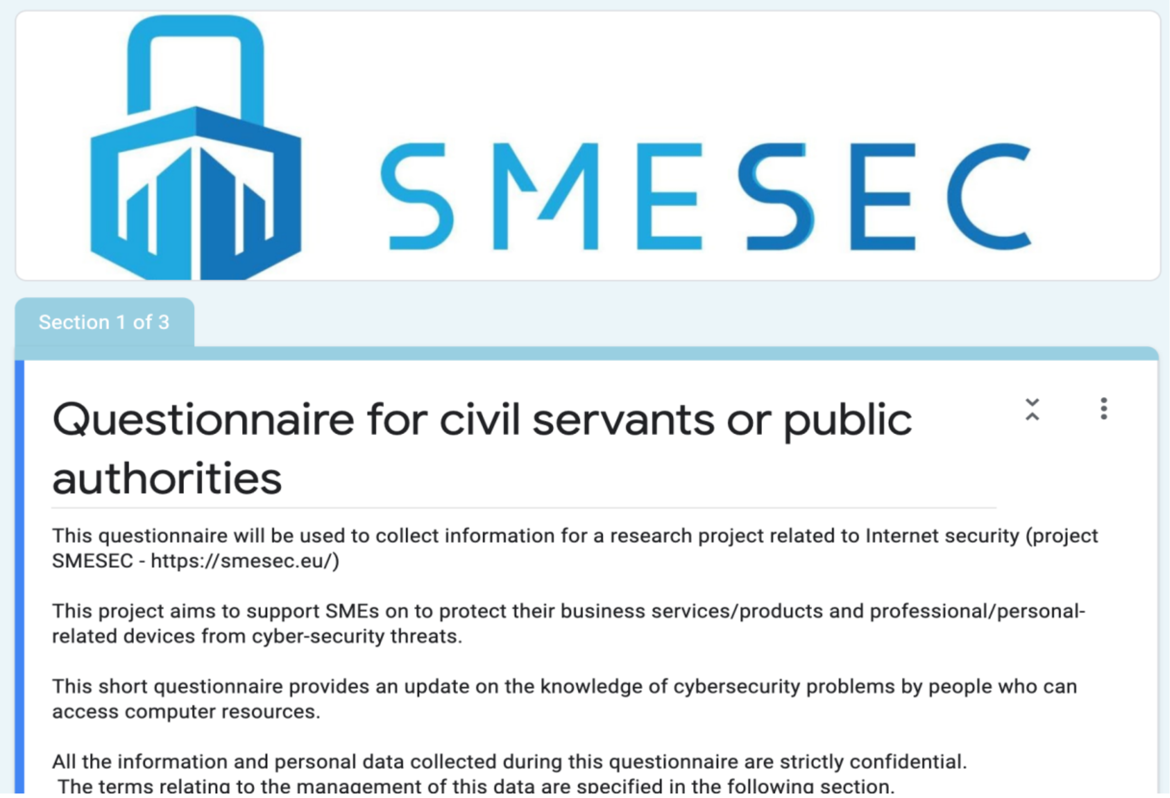
https://www.linkedin.com/feed/update/urn:li:activity:6513347368484765696

- https://twitter.com/PraxiNetwork/status/1107581992382726144
- https://www.facebook.com/PraxiNetwork/photos/a.437796929654253/1800364343397498

and also through FORTH's media channels, through the STEP-C science park and through H2B hub (https://www.facebook.com/htobhub/)

3.4 Feedback about Suitability of SMESEC Approach from Public Administration

We had several interactions with Public Authorities and we used a questionnaire to get their feedbacks. The questionnaire was initiated in Greece by UoP and the results can be found in annex. It was later on translated in French and English for contacting public authorities in other countries.



Questionnaire for civil servants or public authorities

This questionnaire will be used to collect information for a research project related to Internet security (project SMESEC - https://smesec.eu/)

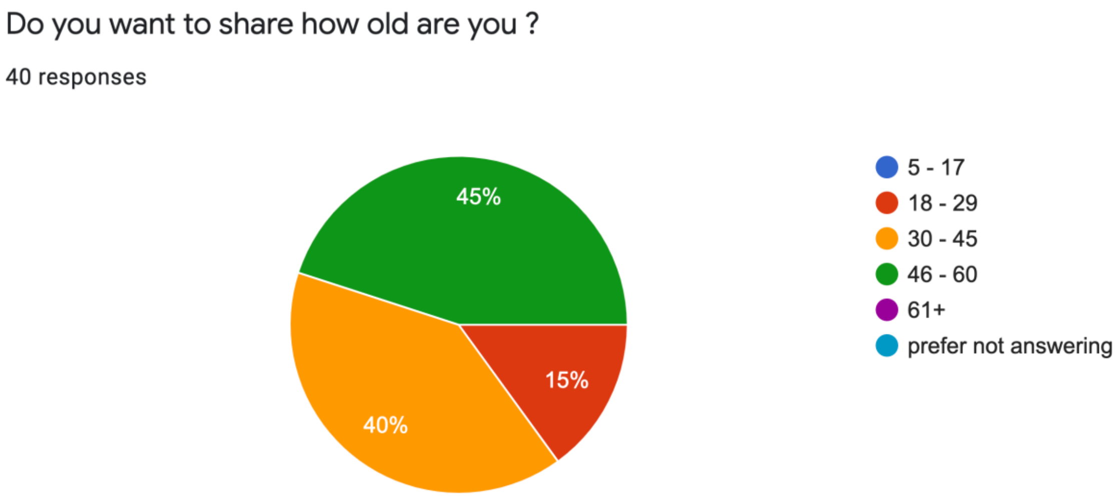
This project aims to support SMEs on to protect their business services/products and professional/personal-related devices from cyber-security threats.

This short questionnaire provides an update on the knowledge of cybersecurity problems by people who can access computer resources.

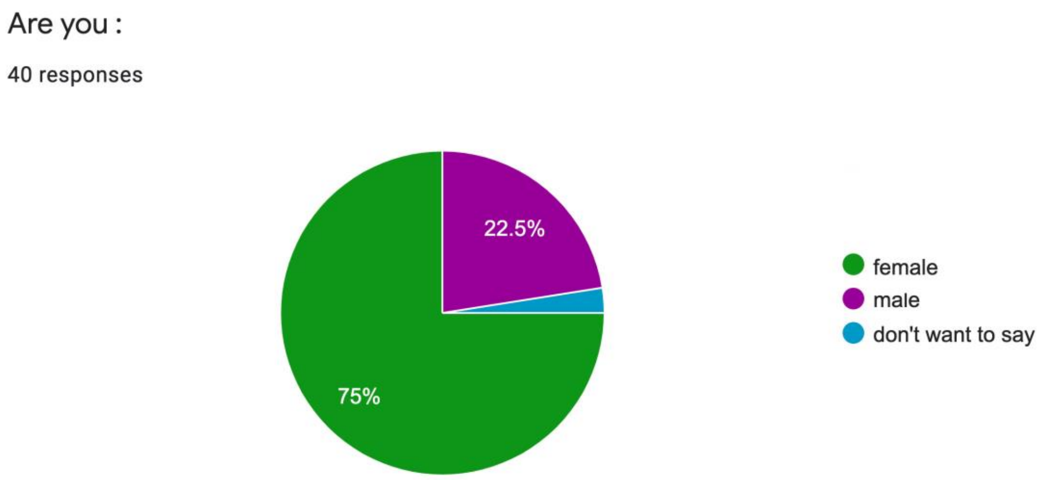
All the information and personal data collected during this questionnaire are strictly confidential.
The terms relating to the management of this data are specified in the following section.

We had a good feedback from France from a local territory grouping 23 municipalities called Communauté d'agglomeration Pays de Grasse (CAPG) representing +100K inhabitants (https://www.paysdegrasse.fr/)

40 employees filled in the questionnaire which give the following feedbacks


Do you want to share how old are you ?

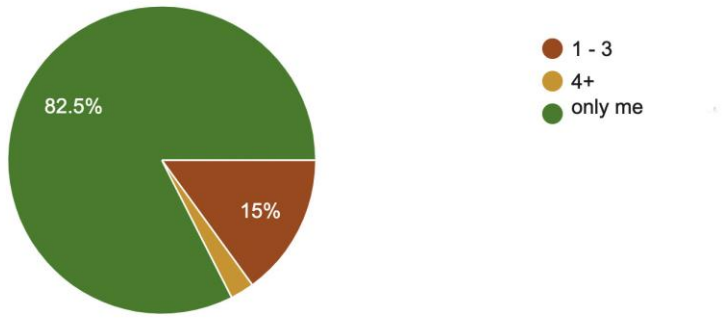
40 responses


Are you :

40 responses

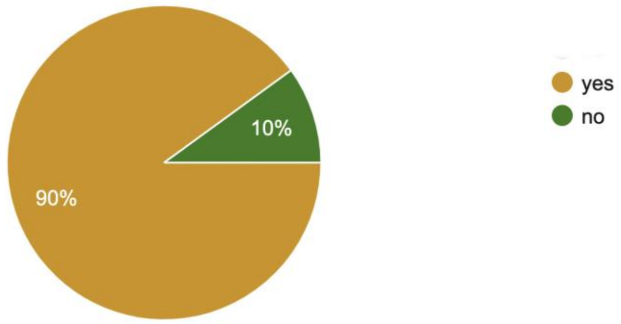
How many people have access to this device

40 responses



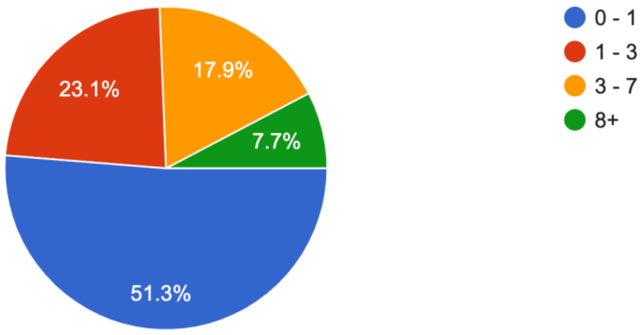
Does the device you use to connect to internet have a security code (password - fingerprint- security pattern)?

40 responses



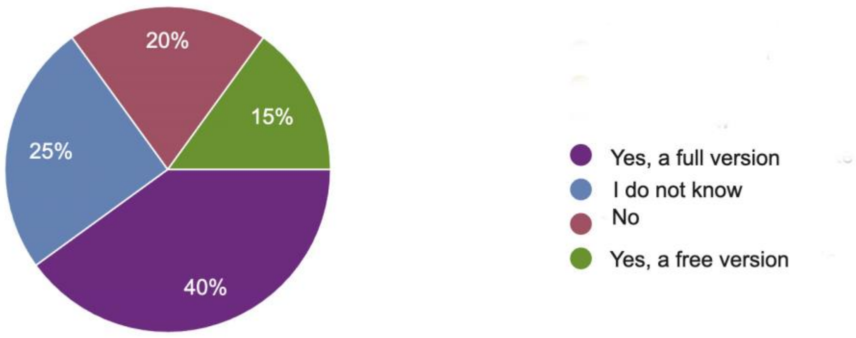
How many apps or programs do you or others install on your device in 1 month in average?

39 responses



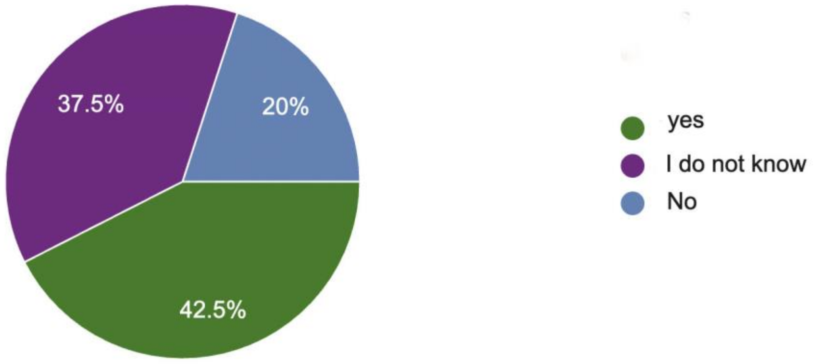
Does your device have an antivirus program installed?

40 responses



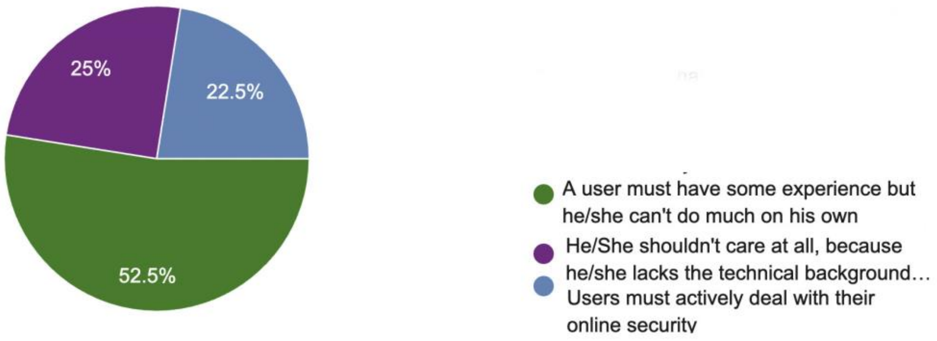
Is the antivirus program frequently updated?

40 responses



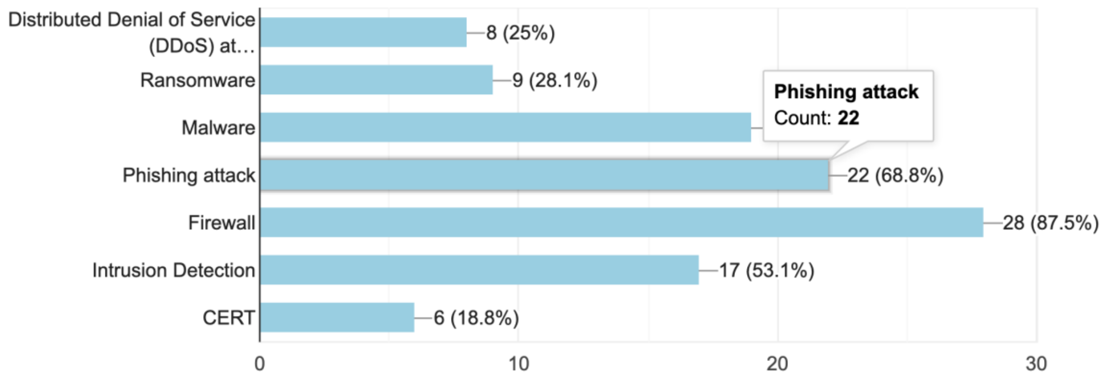
In your opinion, how much should an end-user care about his Internet security?

40 responses



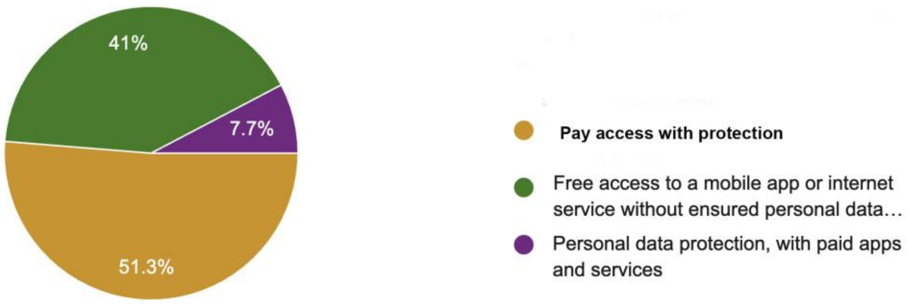
From the following list, check the terms you are familiar with.

32 responses



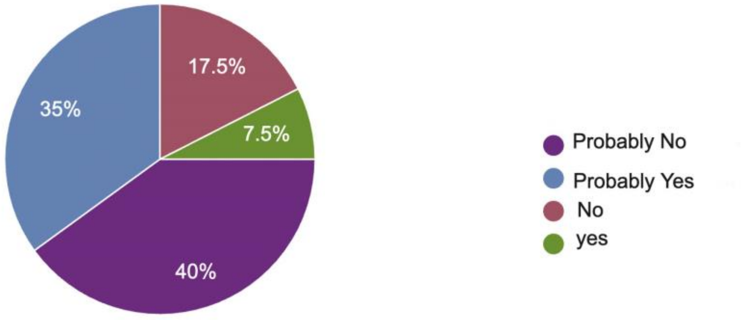
What would you choose?

39 responses



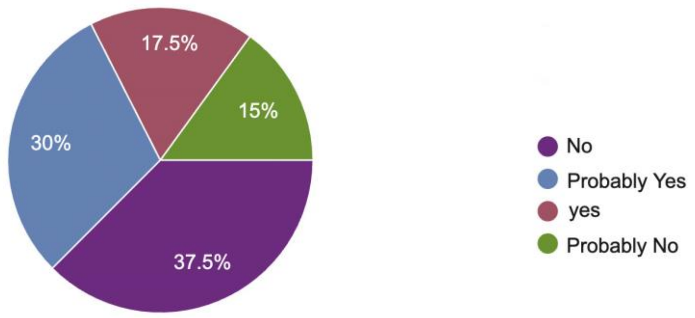
Free access to a mobile app or internet service without ensured personal data protection

40 responses



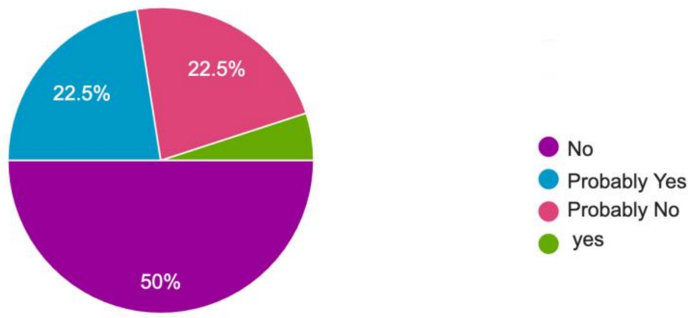
Would you pay for a security application in your device?

40 responses



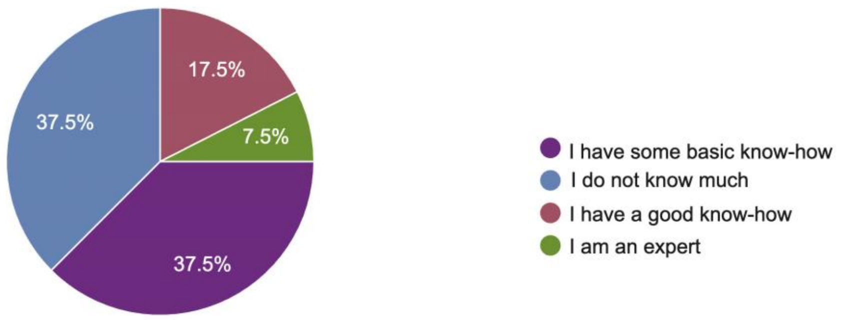
would you pay for a training events on internet security

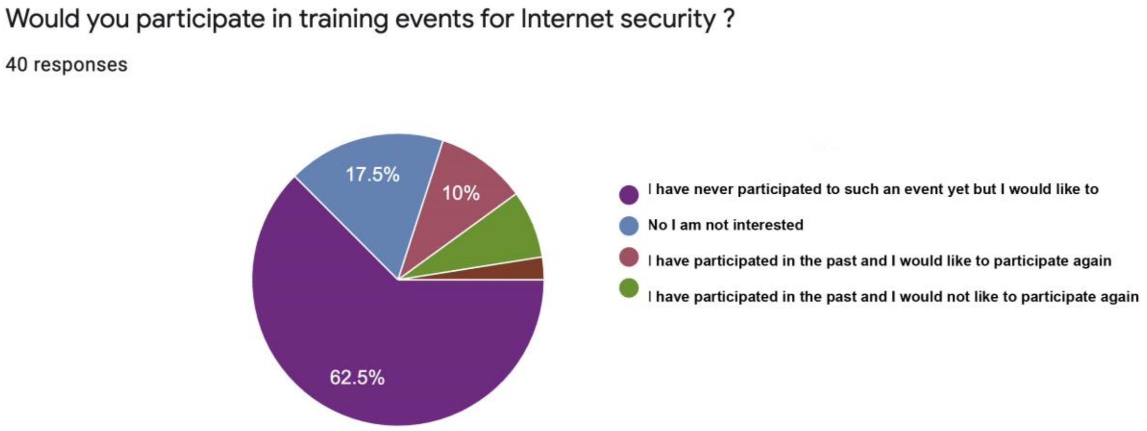
40 responses



How would you rate your background on Internet security and privacy?

40 responses





The conclusion is that the personnel is eager to know more and get trainings.

Another feedback has been done by FHNW in Western Europe The SMESEC approach has been evaluated by a representative of the **public administration of a political community with approximately 6500 inhabitants** located. The community has been chosen due to its size, which is twice the average size of the concerned country and the high level of technological maturity of the country. We expect that this critical choice sample represents an optimistic example of cybersecurity behavior of a political community. Smaller communities and communities in technologically less developed areas are likely to exhibit less awareness of cybersecurity and greater risk of incidents.

The feedback was received from a competent staff employee who was overseeing the community administration's ICT infrastructure, hence had relevant responsibility for the community's cybersecurity. The respondent did not have any specialized cybersecurity education.

Perception of Cybersecurity

The community did not see itself as a target for hackers; also, it did not aware of any cyberattacks on its ICT infrastructure in the past 12 months, not even minor ones.

The community is somewhat concerned of cyber threats; the concerns are unchanged in comparison to the previous year.

Exposure to Cyber Threats

The community manages personal data, sensible data, and intellectual property.

The following table shows the perceived criticality of cyber threats:

Level of Criticality	**Treats**
Critical	Virusses, compliance, privacy, user errors
Somewhat critical	-
Average criticality	System availability, malicious insiders, data integrity and availability, data loss or theft, spam
Little critical	Intrusion or manipulation of systems, system destruction or deletion, fraud, power outage

Not critical	Natural disasters

The community was not able to judge the following threats: system theft, integrity of transactions, ransomware and blackmailing, malicious outsiders, deception of users, and exposure of sensible data.

Management of Cybersecurity

The community believes that it can mitigate risks, vulnerabilities, and attacks to some extent but may have difficulties to recover from a cyberattack.

No systematic approach is institutionalized, however, to ensure the community's cybersecurity. For its defence, the community uses the following:

Category	Measures
Policy	Security baseline, guidelines for the use of computers, guidelines for the use of data
Physical	Physical access control, document shredder
Technical	Gateways and firewalls, VPN, regular updates, backup
Social	Employee training
Business	Insurances

The community considers online courses, webinars, and videos to be an attractive source for cybersecurity knowledge and expects external experts to deliver the that knowledge. Less attractive are physical courses or workshops, webpages and online for a, and newspaper, radio, or television. Out of scope is own research.

Cybersecurity is performed by a dedicated team, an external service provider. No dedicated budget has been allocated to cybersecurity.

Improvement of Cybersecurity

The community had no clear priorities for how cybersecurity should be improved. At the same time, it could not think of slowing and stopping its operations for improving its cybersecurity. If it would, it would train employees to strengthen the cybersecurity culture and contract cybersecurity specialists for improving the technical controls.

Potential for SMESEC

SMESEC has potential for increasing the community's awareness of cybersecurity needs and for closing gaps in the cybersecurity of the community. The clearest gaps that could be addressed with SMESEC are described in the following table.

Category	Potential SMESEC Contributions
Policy	Transparency of attacks and incidents achieved with the SMESEC Hub, XL-SIEM, and the FORTH Honeypot. These tools could allow the community to understand how secure it is and set priorities for improving cybersecurity.
Physical	-

Technical	SMESEC could reinforce the community's endpoint and network controls with the Bitdefender GravityZone and Citrix ADC, offering protection for system availability and against malicious insiders.
Social	SMESEC CYSEC could offer step-by-step guidance for capability improvement, allowing the community to set priorities for rapidly achieving all-over-the-board security, or for confirming that such protection has been achieved. Securityaware.me could fill gaps of online security training to the employees – the community's preferred way of training.
Business	-
Other	IBM Anti-ROP and EGM TaaS have little relevance for the community, which is an ICT user and not an ICT developer.

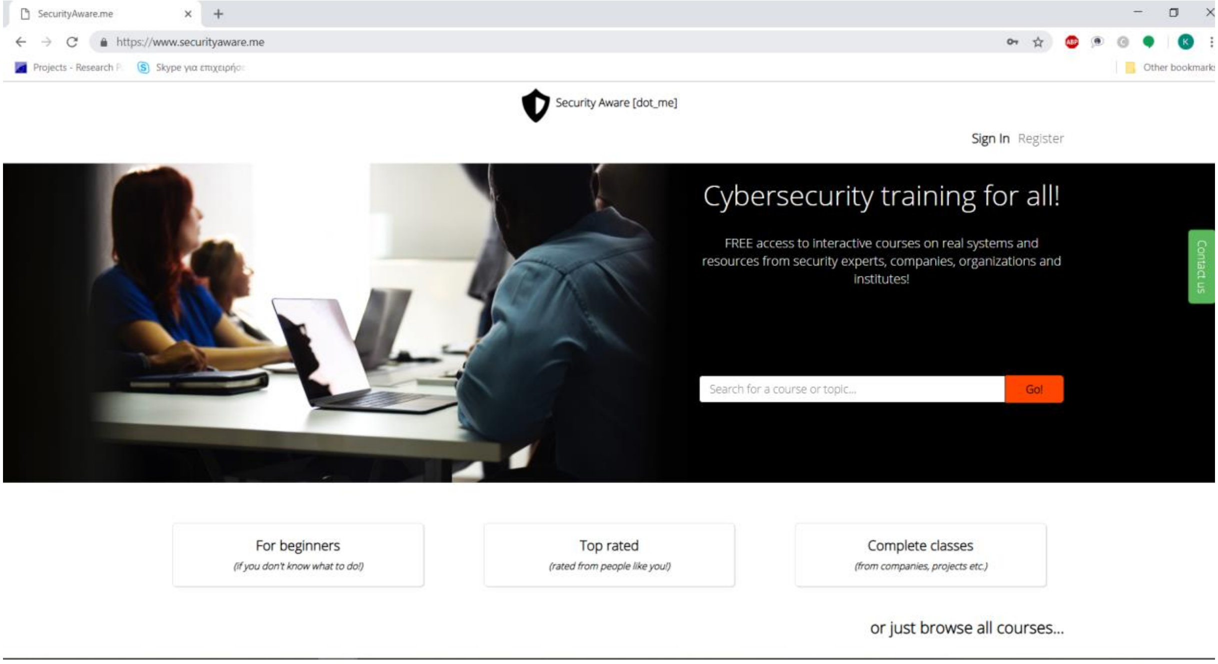
The SME associations

4 SMESEC training platform and trainings

4.1 The training platform

SMESEC project created and published a complete set of online courses to increase security awareness and also train its users on how to configure and operate the SMESEC framework. To provide these courses, the project adopted the free e-learning platform designed and operated by one of its partners (UoP). This platform is called SecurityAware.me and can be found at the https://www.securityaware.me website.

SecurityAware.me is a platform which allows users to create and manage "interactive" online courses using real infrastructures and testbeds (servers, computers, networks etc.) across Europe. Contrary to various e-learning platforms SecurityAware.me focuses solely on cybersecurity. Experts from security companies and institutes around Europe are invited to create courses and contribute training material for various security topics and levels of complexity.



Cybersecurity training for all!

FREE access to interactive courses on real systems and resources from security experts, companies, organizations and institutes!

SecurityAware.me
https://www.securityaware.me
Projects - Research P
Skype για επιχειρήσ
Other bookmarks
Security Aware [dot_me]
Sign In
Register
Contact us
Search for a course or topic...
Go!
For beginners
(if you don't know what to do!)
Top rated
(rated from people like you!)
Complete classes
(from companies, projects etc.)
or just browse all courses...

Figure 10 SecurityAware.me website

The platform is completely free and can host courses that are open to the public (no registration required) or only accessible by registered users. One of the platform’s features is the ability to allow companies, projects etc. create their own space (page in the website) and host their own private or public courses, presenting to their users a personalized training experience. In this space, the company/project can create their own security training courses or select among the free courses that are already created by other experts in the platform.

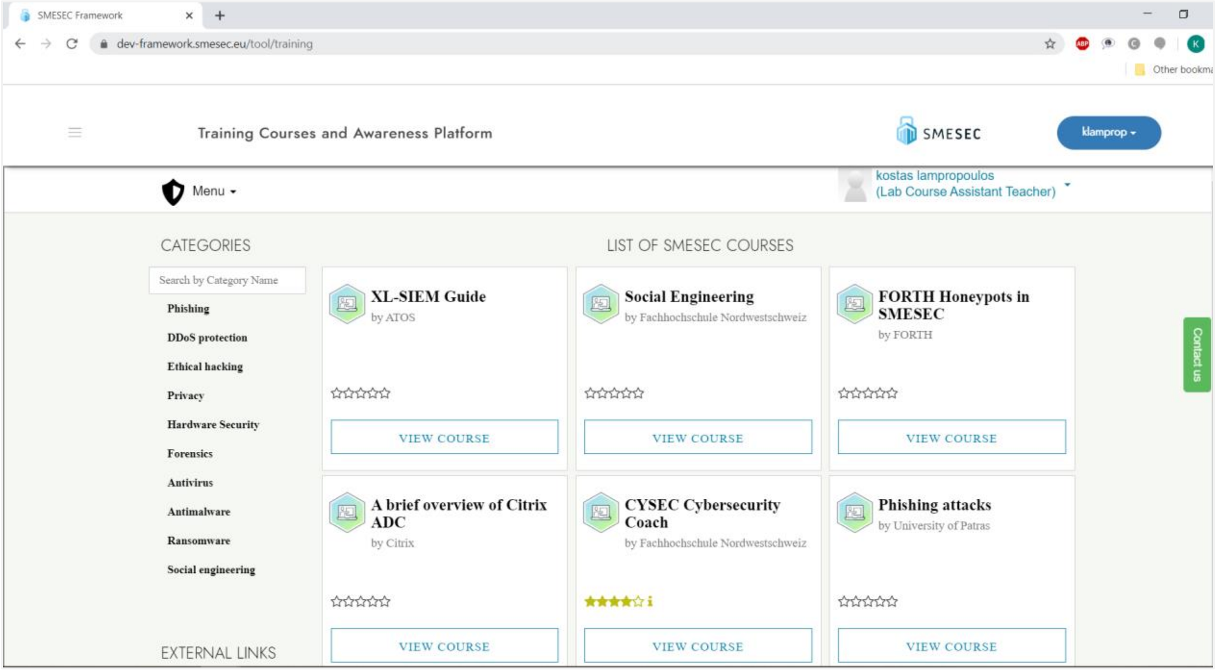
Hosted courses can be executed directly in this platform or exported in various formats to be inserted in other LMS (e.g. Moodle).

SMESEC and SecurityAware.me.

As mentioned above, one of the SecurityAware.me platform’s main features is its ability to allow companies, projects etc. create their own space (page in the website). However, inside the context of SMESEC, SecurityAware.me did not just created a new separate space but implemented a full set of new features and APIs to allow full integration with the SMESEC framework. These features are presented below:

Automatic authentication of SMESEC users: SecurityAware.me implemented all the necessary authentication components to connect with the SMESEC framework through keycloak. Now the platform (SecurityAware.me) creates new profiles and automatically signs in SMESEC users that connect to the training service through the unified dashboard.

Personalised webpage for SMESEC courses: Inside SecurityAware.me, a special webpage was created to present SMESEC courses. This page (landing page) follows all the design principles, colours, fonts etc. of the SMESEC unified dashboard and offers a unified experience to the end user. The figure below presents the SMESEC landing webpage inside the training platform.



Special project for SMESEC courses: A new project was created inside the training platform in order to distinguish courses that are offered only for the SMESEC training service.

List of SMESEC courses retrieval: A secure API (requires a token validated from keycloak) can provide a list of all available SMESEC courses, SMESEC users and their companies.

Personalization of SMESEC training service: The secure API (requires a token validated from keycloak) also provides a list of features to facilitate the personalization of SMESEC training inside the unified dashboard. With this feature a SMESEC user can see in its dashboard account the list of selected courses, the list of mandatory courses and percentage of completion for these courses.

Categories Menu: New categories that were identified inside SMESEC project were added in the user’s menu.

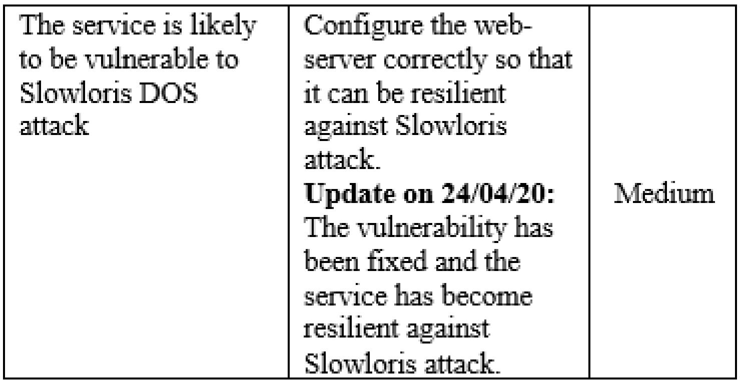
Security evaluation of SecurityAware.me platform.

Inside SMESEC project UOP requested from the open call’s Red Team participant (Montimage) to perform a penetration testing to its training platform (SecurityAware.me). Since the platform was created by a University it had not yet been tested against cyberattacks, and after it was eventually fully integrated to SMESEC dashboard, we needed to make sure that it did not pose any security threats to the framework and its potential customers.

Montimage performed two penetration testings. The first one (during the open call) revealed severe vulnerabilities to the training platform. Such vulnerabilities allowed the red team to launch various successful attacks. In total of 22 vulnerabilities were found with at least 4 of them been critical. After receiving the evaluation report, University of Patras communicated with Montimage and agreed on a second round of tests. University of Patras team would work on the identified vulnerabilities and specifically the critical ones and then it would informed Montimage to do the second penetration testing.

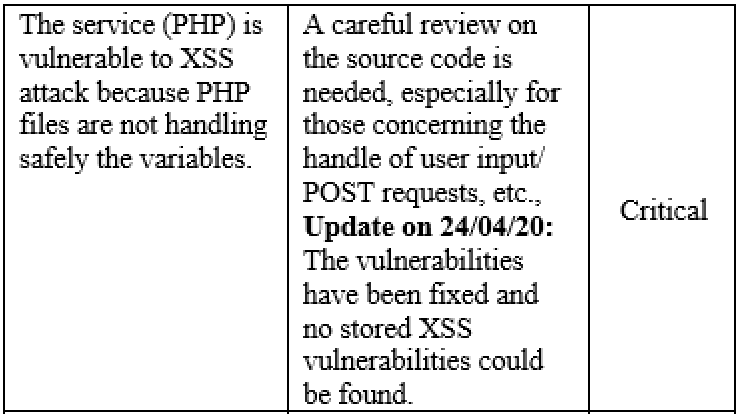
The second penetration testing was a success. The Red Team was not able to replicate any of the major attacks of the first round and also confirmed that all critical security fixes that were suggested after the first pen test were applied. The list of security issues that were addressed is presented below

1) Fixed issue which allowed our services and version of our server to be leaked.
2) We became resilient against Slowlors attack



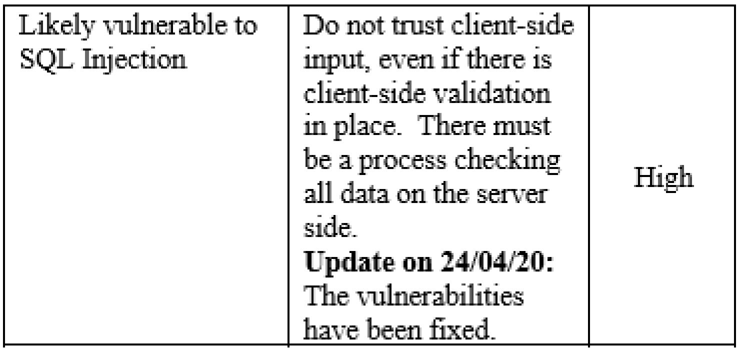
The service is likely to be vulnerable to Slowloris DOS attack	Configure the web-server correctly so that it can be resilient against Slowloris attack. **Update on 24/04/20:** The vulnerability has been fixed and the service has become resilient against Slowloris attack.	Medium

3) We addressed vulnerabilities to XSS attacks



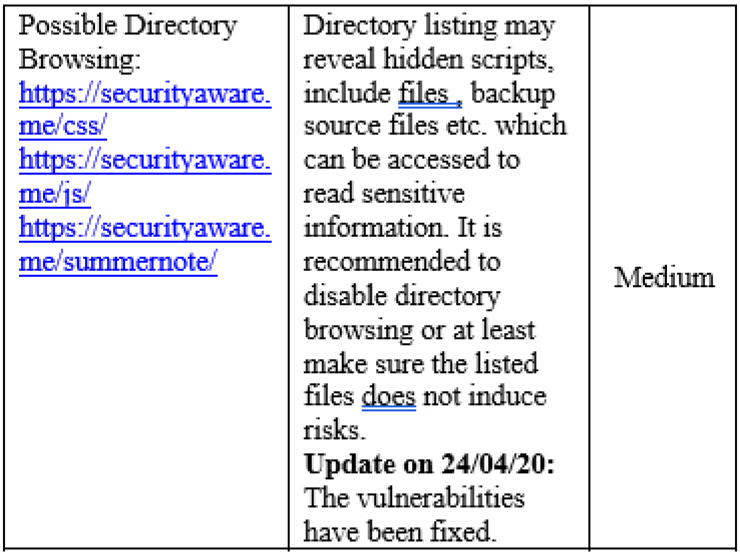
The service (PHP) is vulnerable to XSS attack because PHP files are not handling safely the variables.	A careful review on the source code is needed, especially for those concerning the handle of user input/ POST requests, etc., **Update on 24/04/20:** The vulnerabilities have been fixed and no stored XSS vulnerabilities could be found.	Critical

4) We addressed vulnerabilities to SQL injection attacks



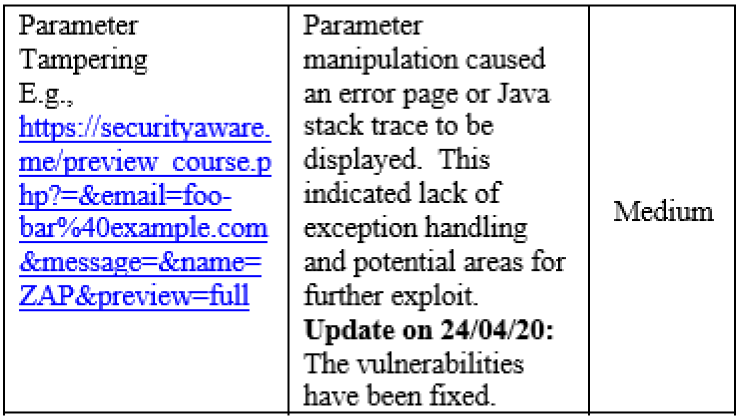
Likely vulnerable to SQL Injection	Do not trust client-side input, even if there is client-side validation in place. There must be a process checking all data on the server side. **Update on 24/04/20:** The vulnerabilities have been fixed.	High

5) We fixed directory listing.



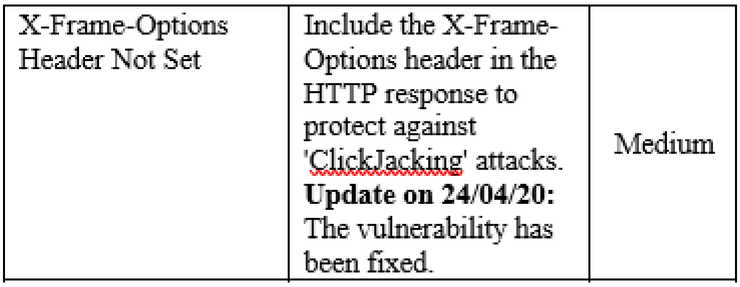
Possible Directory Browsing: https://securityaware.me/css/ https://securityaware.me/js/ https://securityaware.me/summernote/	Directory listing may reveal hidden scripts, include files , backup source files etc. which can be accessed to read sensitive information. It is recommended to disable directory browsing or at least make sure the listed files does not induce risks. **Update on 24/04/20:** The vulnerabilities have been fixed.	Medium

6) We addressed parameter manipulation in the webpage.



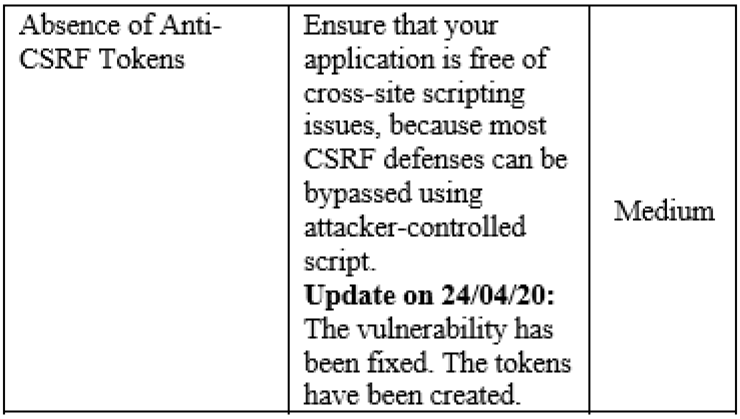
Parameter Tampering E.g., https://securityaware.me/preview_course.php?=&email=foo-bar%40example.com&message=&name=ZAP&preview=full	Parameter manipulation caused an error page or Java stack trace to be displayed. This indicated lack of exception handling and potential areas for further exploit. **Update on 24/04/20:** The vulnerabilities have been fixed.	Medium

7) Included X-Frame-Options Headers



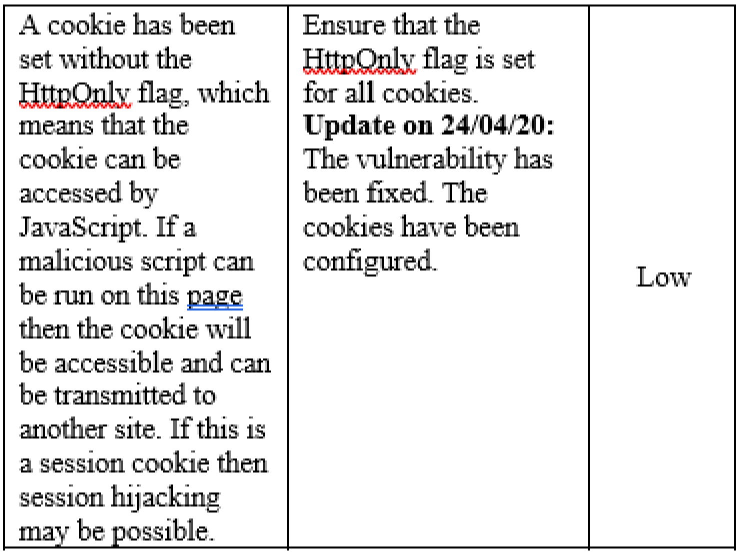
X-Frame-Options Header Not Set	Include the X-Frame-Options header in the HTTP response to protect against 'ClickJacking' attacks. **Update on 24/04/20:** The vulnerability has been fixed.	Medium

8) Created Anti-CSRF Tokens



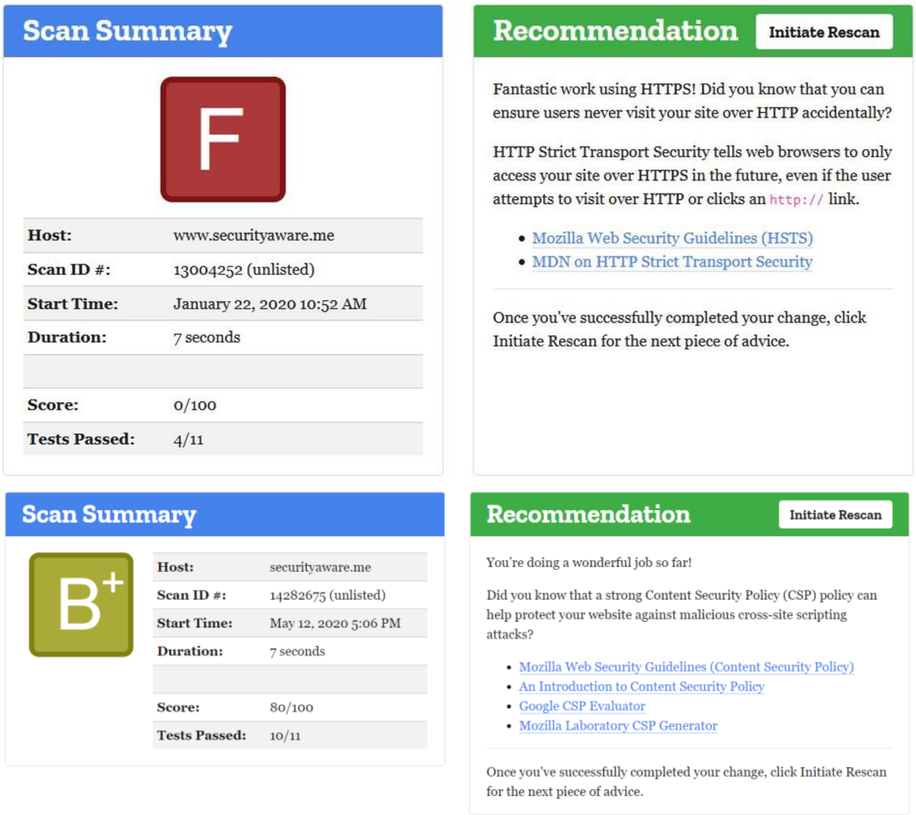
Absence of Anti-CSRF Tokens	Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script. **Update on 24/04/20:** The vulnerability has been fixed. The tokens have been created.	Medium

9) Set proper flags in cookies



A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.	Ensure that the HttpOnly flag is set for all cookies. **Update on 24/04/20:** The vulnerability has been fixed. The cookies have been configured.	Low

Eventually the security score of the training platform (tested using Mozilla Observatory tool) was updated from F to B+ Further improving the security score to A would affect its integration functionality with SMESEC dashboard.



Scan Summary

F

Host:	www.securityaware.me
Scan ID #:	13004252 (unlisted)
Start Time:	January 22, 2020 10:52 AM
Duration:	7 seconds
Score:	0/100
Tests Passed:	4/11

Recommendation Initiate Rescan

Fantastic work using HTTPS! Did you know that you can ensure users never visit your site over HTTP accidentally?

HTTP Strict Transport Security tells web browsers to only access your site over HTTPS in the future, even if the user attempts to visit over HTTP or clicks an `http://` link.

- Mozilla Web Security Guidelines (HSTS)
- MDN on HTTP Strict Transport Security

Once you've successfully completed your change, click Initiate Rescan for the next piece of advice.

Scan Summary

B+

Host:	securityaware.me
Scan ID #:	14282675 (unlisted)
Start Time:	May 12, 2020 5:06 PM
Duration:	7 seconds
Score:	80/100
Tests Passed:	10/11

Recommendation Initiate Rescan

You're doing a wonderful job so far!

Did you know that a strong Content Security Policy (CSP) policy can help protect your website against malicious cross-site scripting attacks?

- Mozilla Web Security Guidelines (Content Security Policy)
- An Introduction to Content Security Policy
- Google CSP Evaluator
- Mozilla Laboratory CSP Generator

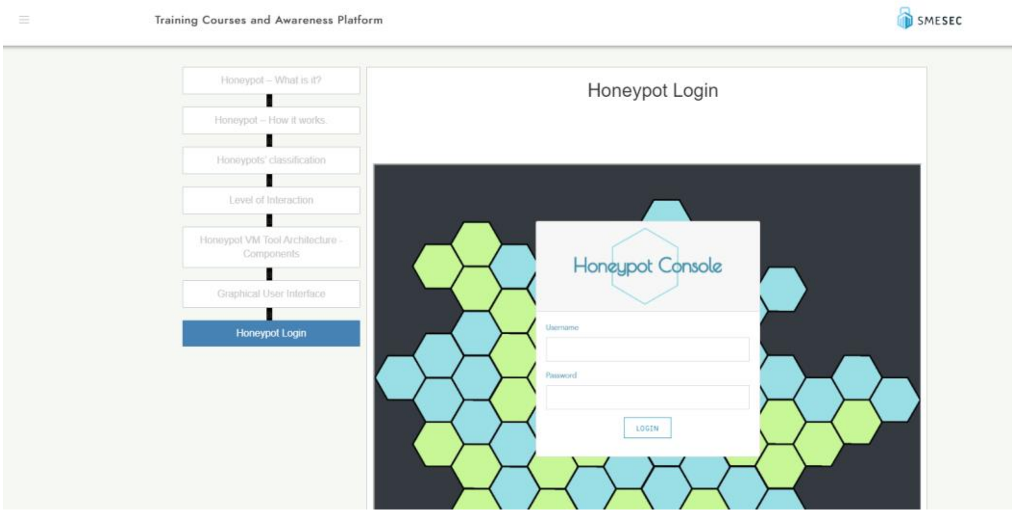
Once you've successfully completed your change, click Initiate Rescan for the next piece of advice.

4.2 The training modules

Inside SMESEC training we provide a list of training courses to cover various cybersecurity aspects. Such aspects include phishing attacks, DDoS, Privacy issues, Antivirus and Endpoint security, Ransomware, etc and are organized as categories in the main webpage. A user can select one of these categories and filter only the type of courses that he/she is interested in.

The platform includes two types of courses: a) general courses for protection against cyber-attacks (e.g. phishing attacks) and b) SMESEC specific courses provided by SMESEC tools' providers to describe procedures relevant to the tool usage e.g. installation, configuration details, user interfaces etc.

For all courses there is the ability to include an interactive part to allow a user to have a hands-on-experience with a real security product. An example of such a hands-on-experience can be found in FORTH's course: Introduction to Honeypots - section Honeypot Login (Figure X)



Training Courses and Awareness Platform

SMESEC

- Honeypot – What is it?
- Honeypot – How it works.
- Honeypots' classification
- Level of Interaction
- Honeypot VM Tool Architecture - Components
- Graphical User Interface
- Honeypot Login

Honeypot Login

Honeypot Console

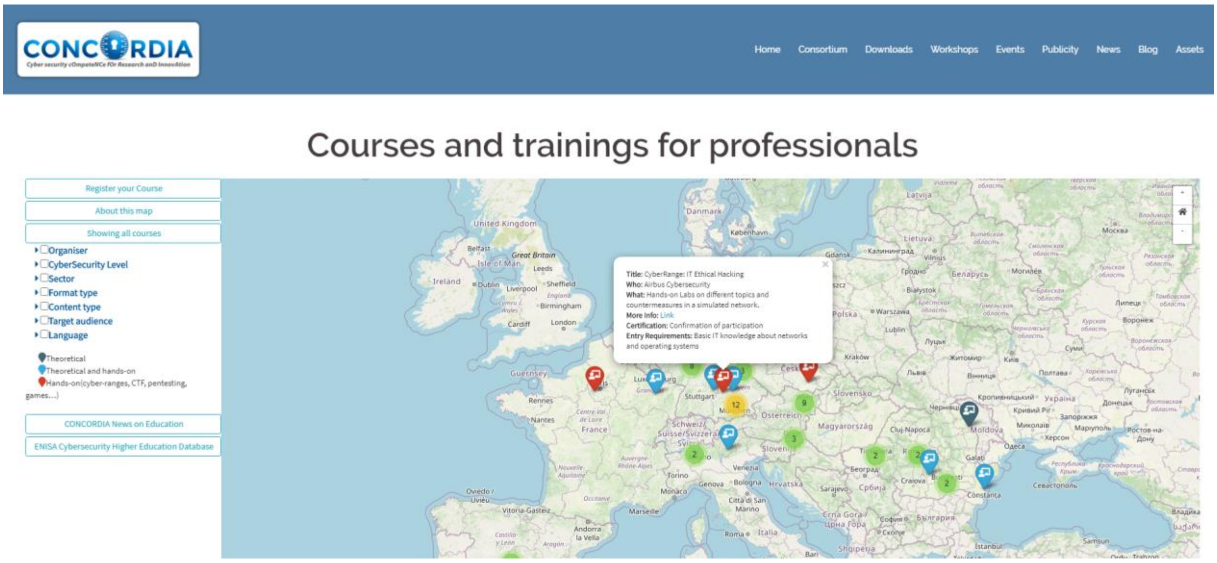
Username

Password

LOGIN

In SMESEC we did not only included courses created by the consortium, but we also included external courses from various sources and institutes. These courses are marked with a “flag” as external courses, and when they are clicked, they redirect the user to an external location.

Finally, we must note that the SMESEC training platform also included links of other projects and initiatives similar to SMESEC. For example, in our training webpage there are links like the CONCORDIA cybersecurity education ecosystem. This link will redirect the user to an interactive map of the EU where he/she can find information about cybersecurity courses from a large variety of institutes and companies around Europe (Figure).



CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

Home Consortium Downloads Workshops Events Publicity News Blog Assets

Courses and trainings for professionals

Register your Course

About this map

Showing all courses

- □Organiser
- □CyberSecurity Level
- □Sector
- □Format type
- □Content type
- □Target audience
- □Language

Theoretical
Theoretical and hands-on
Hands-on(cyber-ranges, CTF, pentesting, games…)

CONCORDIA News on Education

ENISA Cybersecurity Higher Education Database

Title: CyberRange: IT Ethical Hacking
Who: Airbus Cybersecurity
What: Hands-on Labs on different topics and countermeasures in a simulated network.
More Info: Link
Certification: Confirmation of participation
Entry Requirements: Basic IT knowledge about networks and operating systems

4.3 Feedbacks from users

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 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 X) 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.

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%

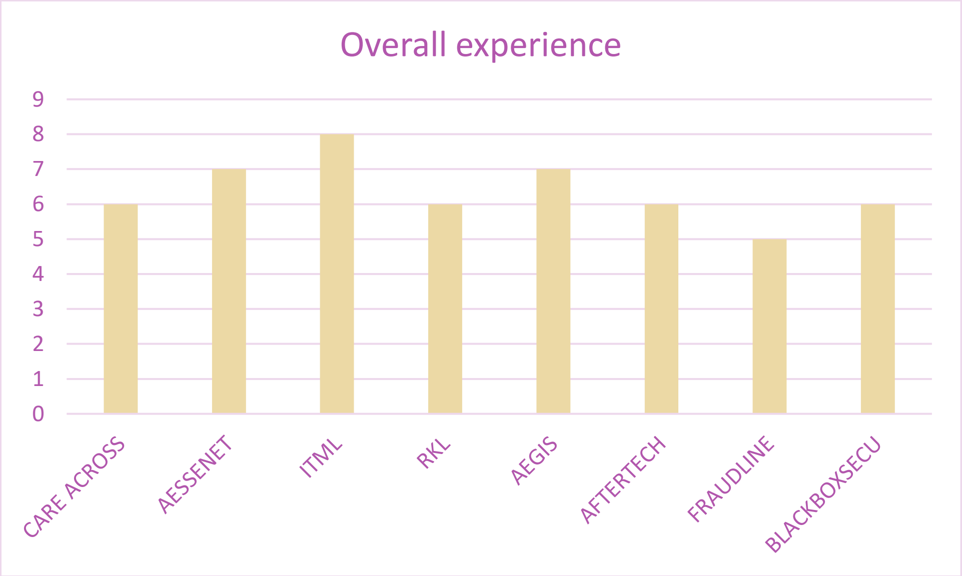


Figure 11: answers from the 8 SMEs on overall experience score from 0 to 10

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

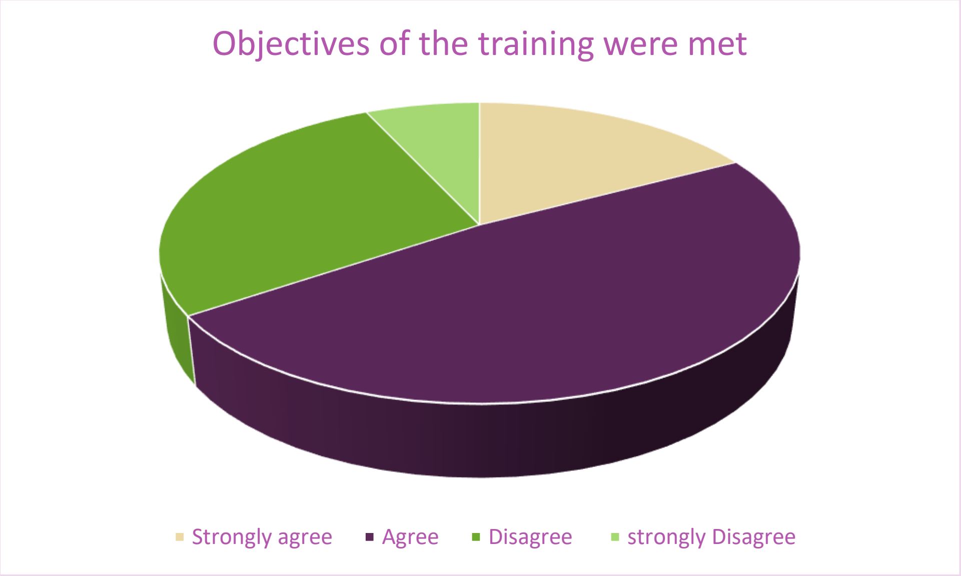


Figure 12: answers whether the objectives of the courses were met

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

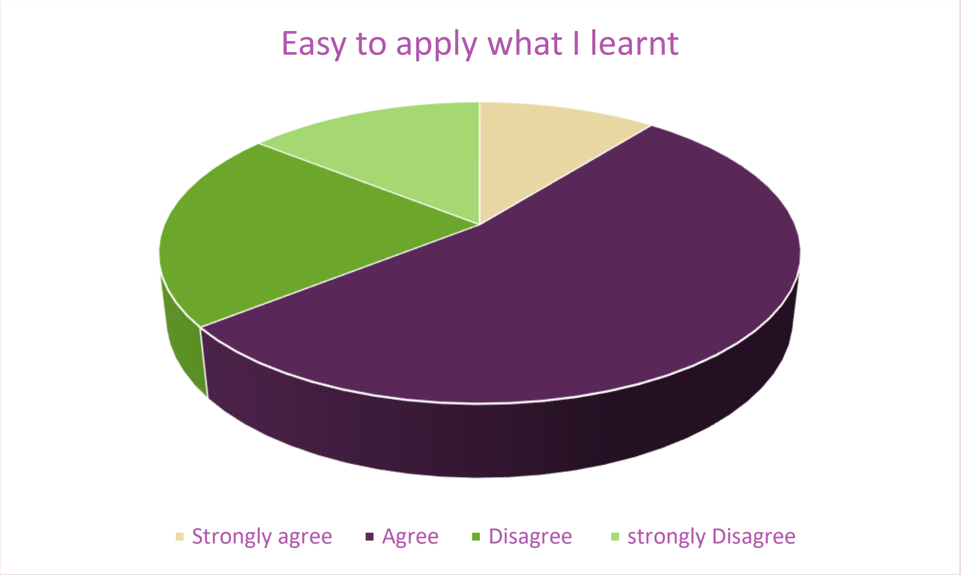


Figure 13 :answer on whether it was easy to apply what was learnt

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

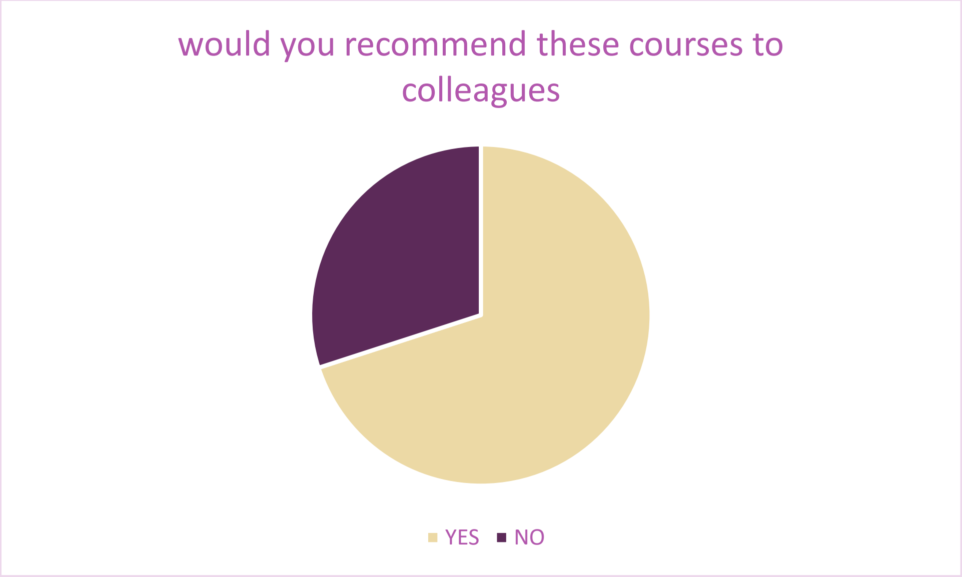


Figure 14: answers on whether SMEs would recommend the courses to collegues

5 Certifications

In addition to technical solutions to improve cybersecurity protection as addressed by the SMESEC framework, weakness of personnel understanding of cybersecurity issues is of utmost importance. SMESEC set a simple self-assessment tool to check skills in understanding cybersecurity in particular in the context of SMEs organization. We decided to give a “certificate” if the person answers more than 50% to the questions. But in order to have a better incentive with the certificate, we decided to ask 3 other EU projects to join the action. In doing that the certificate bears a better Europe context. The self-assessment tool is online at the 4 EU projects websites and the invitation message which was massively promoted is the following:

Start your own SMEs Cybersecurity health-check

Check your cybersecurity skills to better protect your SME and get a certificate of completion issued by 4 European projects

In the modern business world, cybersecurity has quickly become one of the key challenges facing IT companies, especially small firms that need to remain competitive in their markets to stay alive.

Cyber-attacks such as data breaches, distributed denial-of-service (DDoS) attacks and ransomware are increasing, and the consequences can be significant for any organisation, from financial losses to damaged reputations. Despite large companies having increased their budget allocation to face cyber security, when it comes to SMEs, it is still **very hard for them to implement efficient security measures** which are usually perceived as too complex, time consuming and requiring a high level of technical knowledge.

Despite a lot of potential tools to help protecting SMEs, all cybersecurity can be breached if the personal does not understand a minimum of information to control the cybersecurity integrity in a SMEs.
It is important for you to be aware of **main concepts of cybersecurity protection**.

The "**Cybersecurity self-assessment for SMEs**" is specifically designed to tackle this issue, **helping companies staff to increase awareness about basic security guidelines to be applied in their day-to-day routine**.
By answering a set of questions through a simple and quick online self-assessment, SMEs can easily understand where they stand in terms of their cybersecurity posture. The tool quickly helps SMEs to pinpoint security gaps and best practices that should be regularly followed through in terms of:

- Office Firewalls and Internet Gateways
- Secure Configuration
- Software Patching
- User and Administrative accounts best practices
- Malware protection
- Awareness of Password weaknesses
- Basic risk assessment

The "**Cybersecurity self-assessment for SMEs**" is available free of charge at https://intg.taas.eglobalmark.com/certif/best-practices-smes.html and can be completed in less than 15 minutes.
Measure your cybersecurity awareness skill, pinpoint your security gaps and implement the best practices to avoid being a victim of a cyber-attack.

About the Cybersecurity self-assessment for SMEs

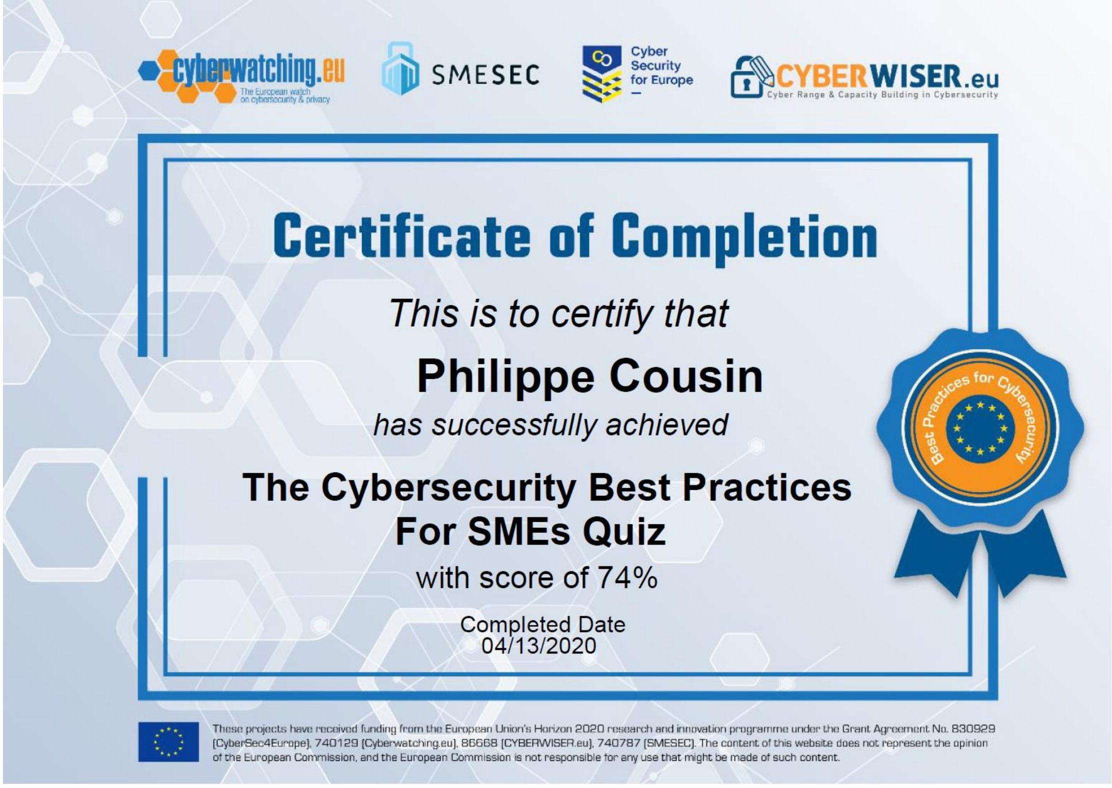
The assessment was developed as a joint effort by four H2020 initiatives namely CyberSec4Europe, Cyberwatching.eu, CYBERWISER.eu and SMESEC. All four initiatives are tackling cybersecurity and privacy from complementary perspectives, with the aim of providing European SMEs with key resources to boost their online security. Beyond the assessment each project provide a set of cybersecurity tools to increase SMEs online security:

- CyberSec4Europe is one of the four recently funded competence pilot projects aiming at setting up a European network of centres of cybersecurity expertise.
- The project activities range from combining formal, professional and non-traditional cybersecurity skills sand capacity building to open-source tools development to support cybersecurity education, software testing, and certification of hardware and software products.
- Cyberwatching.eu provides an European cybersecurity and privacy Marketplace consolidated collection of outputs from completed, EU-funded research projects. It is also a shop window for innovative products and services offered by small and medium sized providers across Europe. As such, organisations may use the Marketplace as a platform to display the products which have been developed through internal research and innovation activities.
- CYBERWISER.eu delivers a flexible, risk-centred, capacity-building platform, combining a theoretical and practical approach to cybersecurity with innovative features (including a cutting edge cyber range). CYBERWISER.eu implements customisable training pathways in cybersecurity to fit a broad range of needs and capacity building targets.
- SMESEC proposes a cost-effective framework composed of specific cyber-security tool-kits to support SMEs in managing network information security risks and threats including: detection and alerting tools, threat protection and response as well as awareness and training tutorials.

More information: https://www.smesec.eu/smequiz.html

To attract interest for SMESEC online, as opposed to interacting with the public at a fair or conference, the consortium of cybersecurity projects offered a quiz on cybersecurity best practices for SMEs. SMESEC social media generated 76 conversions for this quiz.

Those who were successful and passed the quiz received a certificate as shown below.



cyberwatching.eu The European watch on cybersecurity & privacy

SMESEC

Cyber Security for Europe

CYBERWISER.eu Cyber Range & Capacity Building in Cybersecurity

Certificate of Completion

This is to certify that

Philippe Cousin

has successfully achieved

The Cybersecurity Best Practices For SMEs Quiz

with score of 74%

Completed Date
04/13/2020

Best Practices for Cybersecurity

These projects have received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No. 830929 (CyberSec4Europe), 740129 (Cyberwatching.eu), 86668 (CYBERWISER.eu), 740787 (SMESEC). The content of this website does not represent the opinion of the European Commission, and the European Commission is not responsible for any use that might be made of such content.

End of May about **30 certificates** have been issued but the programme is only recently in place. All the 4 EU projects have the information in place and will continue to promote it beyond the end of SMESEC project.

6 Assessment of cybersecurity awareness and maturity of SMEs

ARE SMALL AND MEDIUM-SIZED COMPANIES UNDER FIRE?

Please join us in bringing together the facts on cyber threats.

TAKE THE SURVEY

(multiple languages supported)

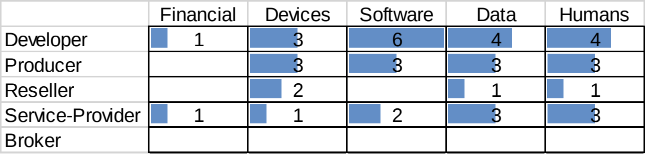
The original SMESEC survey was evolved to capture the knowledge gained during the first 2.5 years in the project, including the early results from the open call. The update to V2.0 was motivated by asking questions of even higher relevance for SMEs and offering guidance for the potential exploitation scenarios of the SMESEC framework.

We here present the answers that we have obtained for this second version of the survey.

Respondents

We have received 12 answers. 7 were micro companies with less than 10 employees, 3 were small companies with less than 50 employees, one was a medium-sized company, and one was a government agency or public organisation. 5 respondents were CEOs, 4 had a director position, 3 were consultants, and 1 was a developer.

The respondents were active in the following domains: 3 ICT, 2 professional services, 1 administration, 1 agriculture, 1 construction, 1 education, 1 manufacturing, 1 water supply, and 1 other. Within these domains, they pursued the following business models. Most common were development activities, and most common was the focus on software.



	Financial	Devices	Software	Data	Humans
Developer	1	3	6	4	4
Producer		3	3	3	3
Reseller		2		1	1
Service-Provider	1	1	2	3	3
Broker					

6 SMEs insourced software development (including the ICT companies), and 5 SMEs outsourced software development; only 1 the administration did both about equally. 6 SMEs hosted its software externally (including the ICT companies), 5 SMEs hosted some of its software internally and some externally, and the administration hosted all software internally.

10 of the 12 respondents were responsible for cybersecurity of their company, at least partly. However, only 4 had received any cybersecurity education. Accordingly, 8 SMEs had a dedicated person or team responsible for cybersecurity, 2 outsourced cybersecurity, and 2 had nobody responsible.

Exposure to Security Threats

7 of the 12 SMEs were worried about cyber threats. 4 SMEs considered themselves to be a target for hackers. In comparison to the previous year, 6 SMEs were more concerned, and 6 SMEs did not change their opinion.

The organizations depended on information that is available, kept confidential, and is integer. Only 1 organization had low availability requirements, 1 other organization low confidentiality requirements, and 1 other organization low integrity requirements.

Severe attacks that were a threat to operations were absent for all SMEs, however. Only 1 experienced occasional attacks that were moderate and required dedicated attention, and 7 experienced occasional or frequent attacks that were minor without significant impact.

The consequences of the attacks were as follows: 7 reported extra costs, 3 business disruption, 2 reputational damage, and 1 extra effort. 5 reported that most incidents had no consequences.

Role of Cybersecurity in the Respondent SMEs

The business of 7 of the SMEs would have difficulties with ICT outage of less than one day, 4 would still be operational if ICT would be off for more than one day.

0%-5% of the annual turnover was spent on cybersecurity: 4 had no budget, 4 spend 2%, 1 spends 5%. For 8 of the 12 SMEs, the spending on cybersecurity was about 50% of the SME’s total ICT spending.

6 SMEs reported they have a systematic approach to cybersecurity, 4 reported they have not. 5 SMEs believed they can well mitigate cyber risks, 3 believed not. 6 SMEs believed they can easily recover from a cyber-attack, 2 believed not.

Cybersecurity Improvement

6 SMEs could consider pausing or slowing down their operations for improving cybersecurity, 3 could not.

The SMEs reported the following priorities for improving their cybersecurity (the table shows priority by number of SMEs):

Employee training	10
Extra budget	7
Advanced security solution	5
Security specialist	5
Improve tooling	4
Exchange with SMEs	4
Vulnerability search	3
Respond to priority threats	3

In average, the SMEs had the following preferences for sources of cybersecurity knowledge: external experts (Mean Opinion Score MOS 4.2), online courses and videos (MOS 3.8), webpages and online fora (MOS 3.7), and classroom courses (MOS 3.6). News were considered to be rather unattractive (MOS 2.5).

SMESEC Offering

10 SMEs considered SMESEC to be innovative, one considered it to be conservative.

No SME reported anything missing in the SMESEC framework. This indicates that they may not have the required expertise to judge the answer or could not spend the necessary effort in gap analysis of the SMESEC framework for their company.

The questions related to how to offer SMESEC have been answered inconsistently. The price suggestions varied by several orders of magnitude, the potential use of the framework was unclear, and no dominant distribution channel emerged. The heterogeneity of the answers is likely to be the result of the open-ended nature of the questions.

Security Standardization

10 SMEs believed that information security standards improve the quality of their services and products. 4 of these positive respondents did not use any such standard, however. The other 6 positive ones used ISO/IEC 27001 (3x), the ones requested by their customers (1x), or others.

In average, the SMEs neither agreed or disagreed that there would be too many standards (Mean Opinion Score MOS 3.2), they slightly agreed that the standards were technically complex (MOS 3.7), agreed that the cost of standards acquisition is high (MOS 4.1), agreed that the cost of standards implementation is high (MOS 4.2), and neither agreed nor disagreed that the benefits of standards implementation was clear (MOS 3.2).

7 Conclusions

During this 3rd year we have interacted more with SMEs also in showing the SMESEC framework and the Cybersecurity Awareness tool, the CYSEC tool.

While we interacted with many individual SMEs in particular thanks to the open call, we believed that we can reach bigger audience through participations to big events, cooperating with SMEs associations and joining forces with other Cybersecurity related EU projects. This is what we did with major combined event at International Cybersecurity Forum FIC2020 end January 2020. We kept discussing and we planned a series of webinars in the spring period but it was difficult to mobilize stakeholders with the COVID19 crisis. However, from SMESEC initiative we put in place a common self-assessment quiz which is helping people to check their skill and get a certificate

We have also our training portal with many useful training courses

We are now confident that we will leave useful material such as the CYSEC tool, the training courses, the Cybersecurity self-assessment quiz that will continue to live after the end of the SMESEC project. Our other EU partner projects will continue to promote the SMESEC offers.

8 References

[1] AEI Ciberseguridad; Link: https://www.aeiciberseguridad.es/; Last visited: 14.12.2018

[2] CITIC; Link: https://www.citic.es/; Last visited: 14.12.2018

[3] PLANETIC; Link: https://www.planetic.es/; Last visited: 14.12.2018

[4] PESI; Link: https:// http://www.pesi-seguridadindustrial.org/es/; Last visited: 14.12.2018

[5] Albrechtsen, E. (2007) “A qualitative study of users' view on information security”, Computers & Security, 26(4), 276-289.

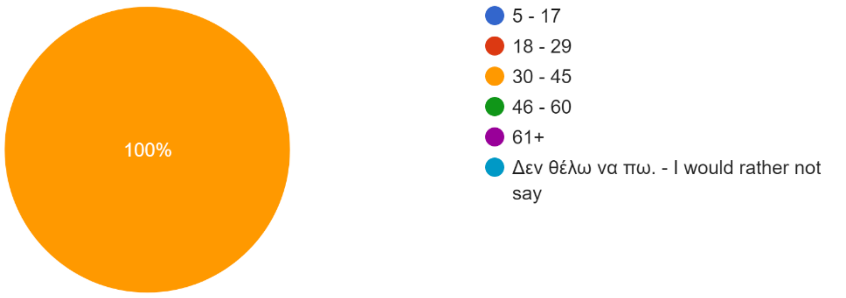
[6] Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010) “Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness” MIS Quarterly, 34(3), 523-548.

[7] Davis F. (1989), “Perceived usefulness, perceived ease of use, and user acceptance of information technology”, MIS Q, 13(3):319-339.

9 ANNEX: Greek Public authorities personnel’s answers

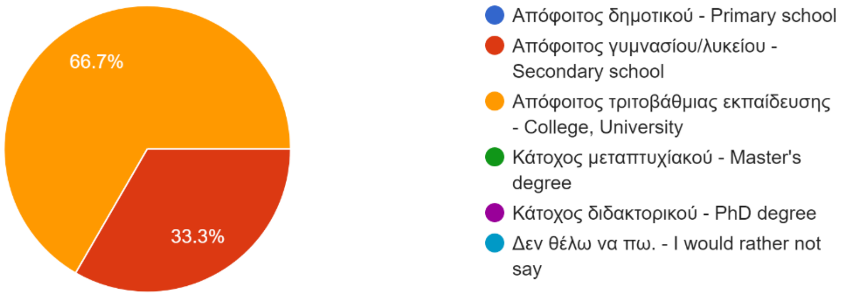
Θέλεις να μας πεις την ηλικία σου; - Do you want to share your age with us?

6 responses



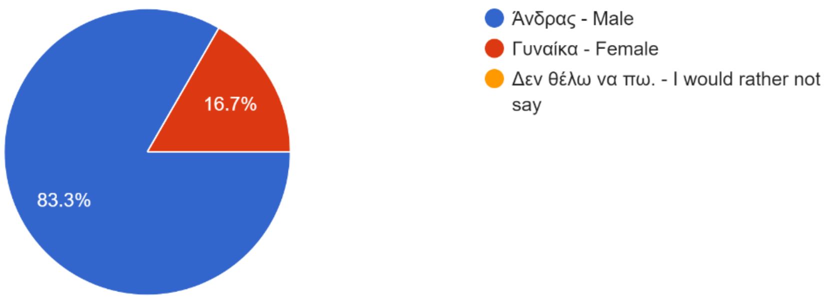
Θέλεις να μας πεις την εκπαίδευσή σου; - Do want to share your education level with us?

6 responses



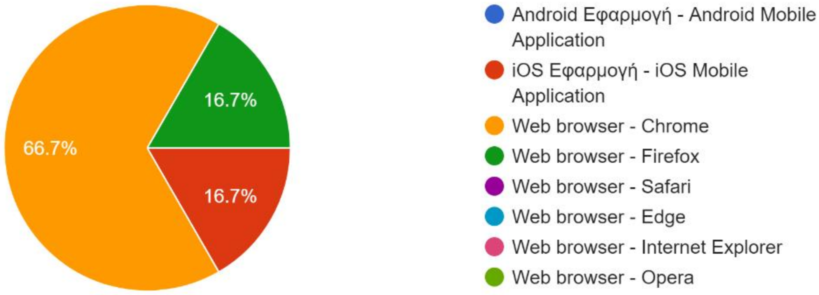
Θέλεις να μας πεις το φύλο σου; - Do want to share your gender with us?

6 responses



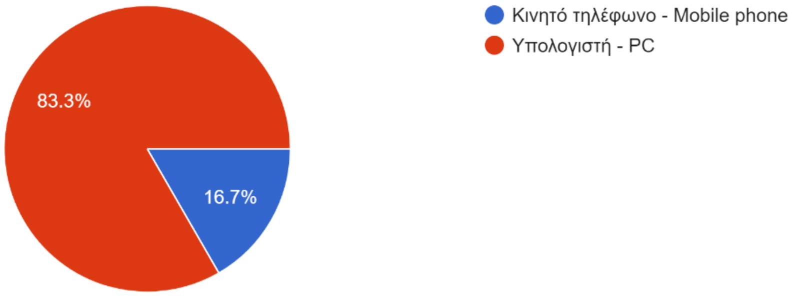
Πως συνδέεσαι στο Sense.city; - How do you connect to Sense.city?

6 responses



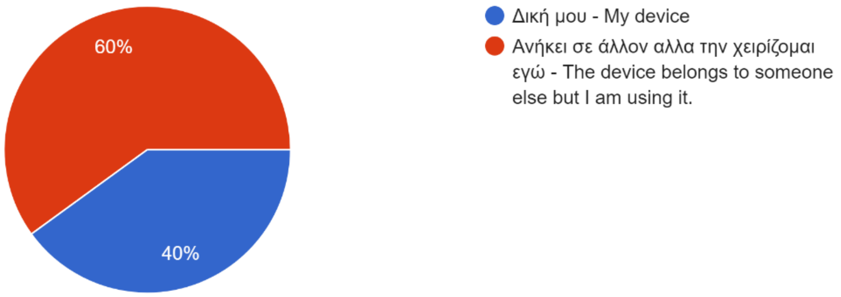
Τι συσκευή χρησιμοποιείς για να συνδεθείς στο Sense.city; - What device you use to connect to Sense.city?

6 responses



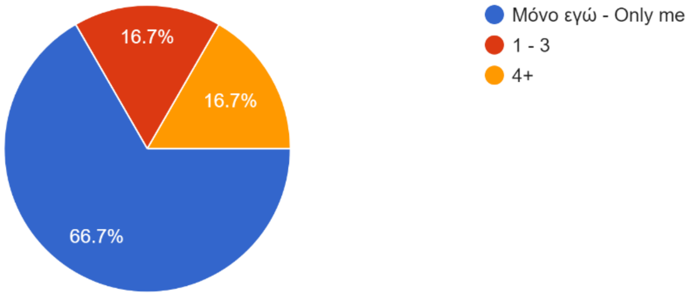
Η συσκευή ανήκει σε σένα ή σε κάποιον άλλον (π.χ. εταιρικό τηλέφωνο, υπολογιστής υπηρεσίας); - Does this d... else (e.g. company mobile, work pc)?

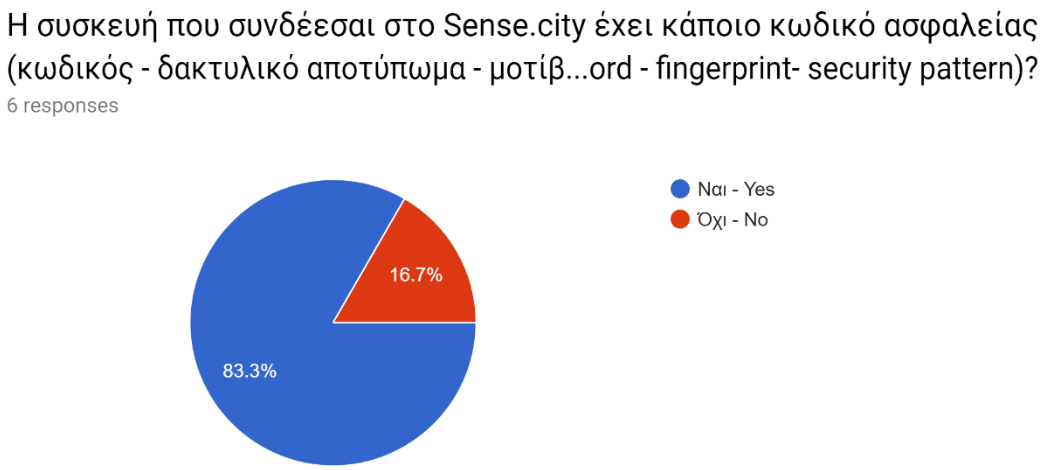
5 responses



Πόσοι άνθρωποι έχουν πρόσβαση στην συσκευή - How many people have access to this device

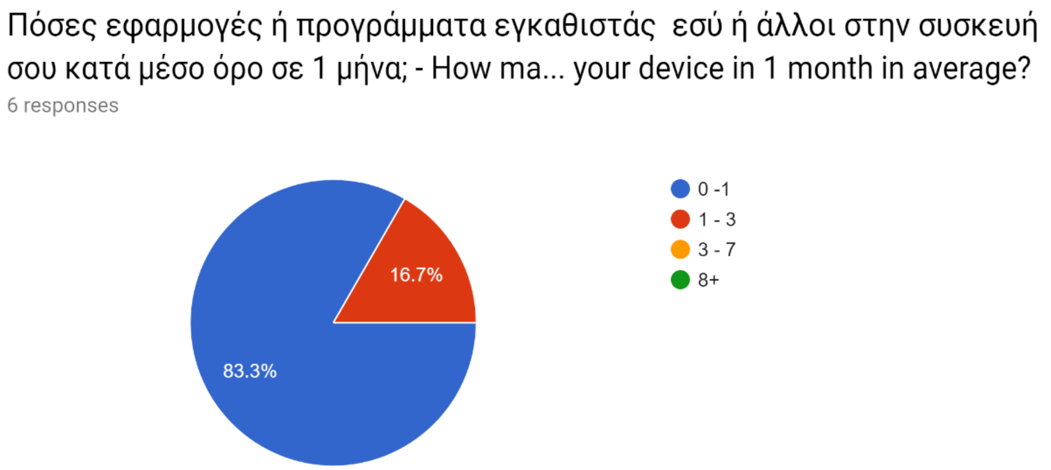
6 responses





Η συσκευή που συνδέεσαι στο Sense.city έχει κάποιο κωδικό ασφαλείας (κωδικός - δακτυλικό αποτύπωμα - μοτίβ...ord - fingerprint- security pattern)?

6 responses

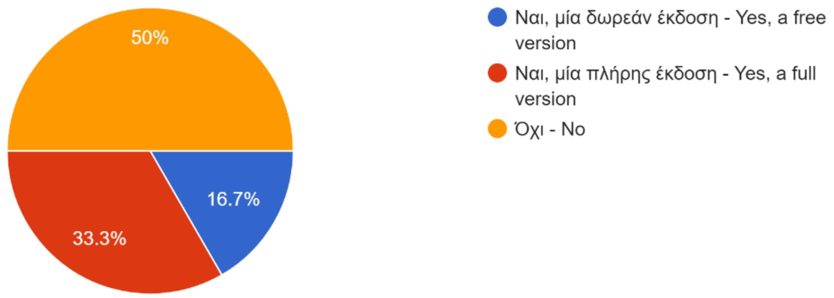


Πόσες εφαρμογές ή προγράμματα εγκαθιστάς εσύ ή άλλοι στην συσκευή σου κατά μέσο όρο σε 1 μήνα; - How ma... your device in 1 month in average?

6 responses

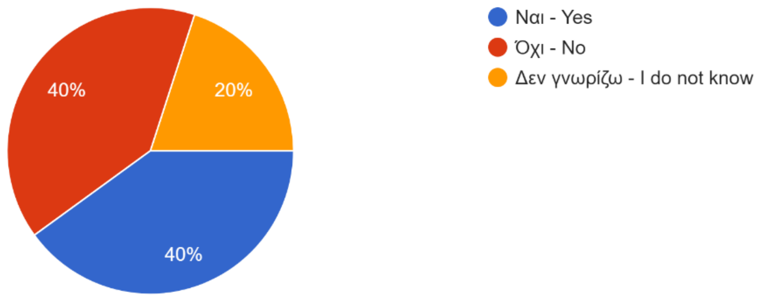
Η συσκευή σου έχει εγκατεστημένο κάποιο antivirus πρόγραμμα; - Does your device have an antivirus program installed?

6 responses



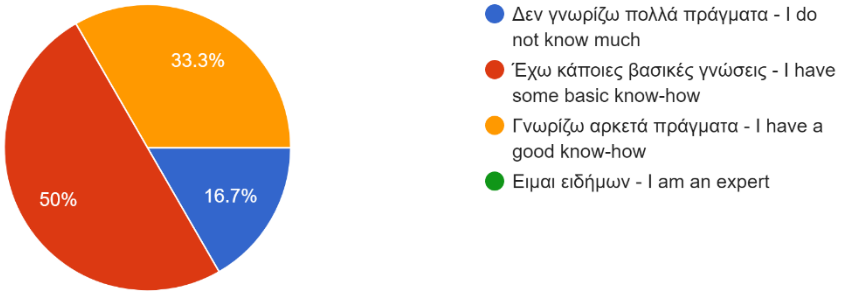
Το antivirus πρόγραμμα ενημερώνεται συχνά (updates); - Is the antivirus program frequently updated?

5 responses



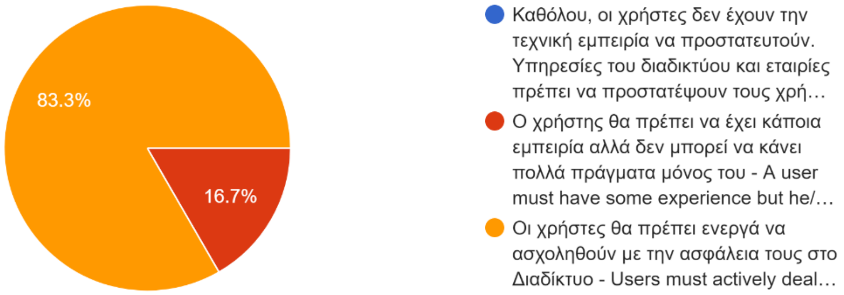
Πως κρίνεις τις γνώσεις σου για την ασφάλεια και την ιδιωτικότητα στο Διαδίκτυο; - How would you rate your b...und on Internet security and privacy?

6 responses



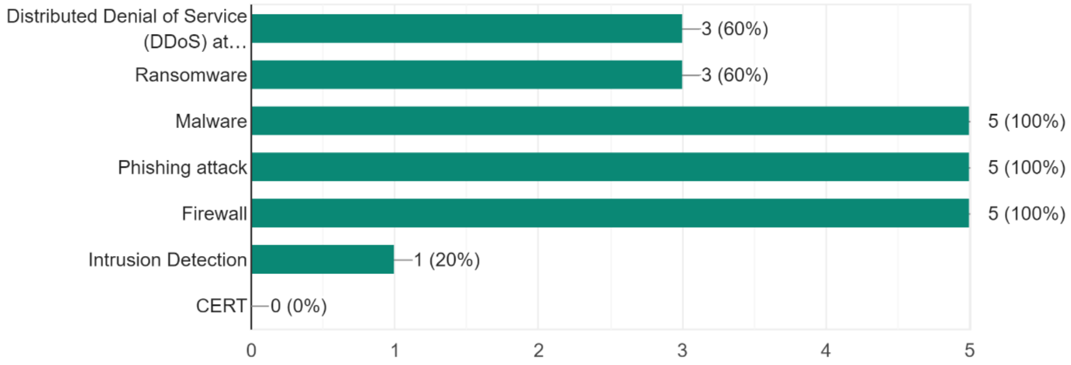
Κατά τη γνώμη σου, πόσο θα πρέπει να ενδιαφέρεται ένας χρήστης για την ασφάλειά του στο Διαδίκτυο; - In y...user care about his Internet security?

6 responses



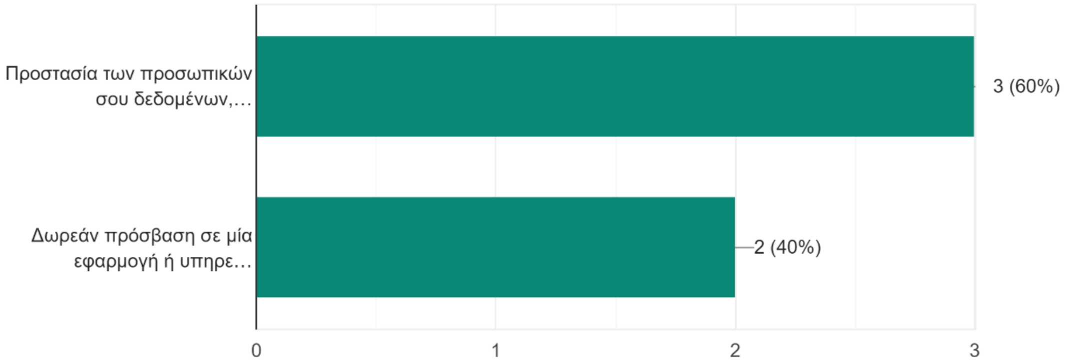
Από την ακόλουθη λίστα επέλεξε τους όρους που γνωρίζεις - From the following list, check the terms you are familiar with.

5 responses



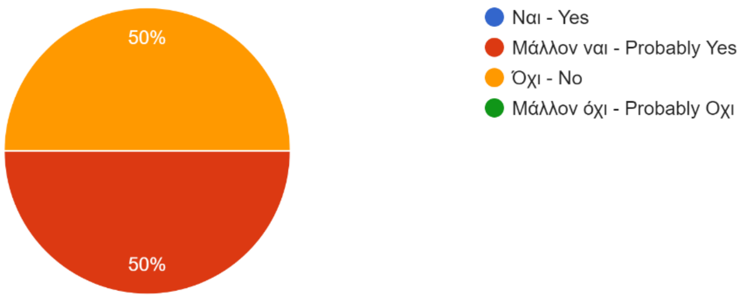
Τι θα διάλεγες; - What would you choose?

5 responses



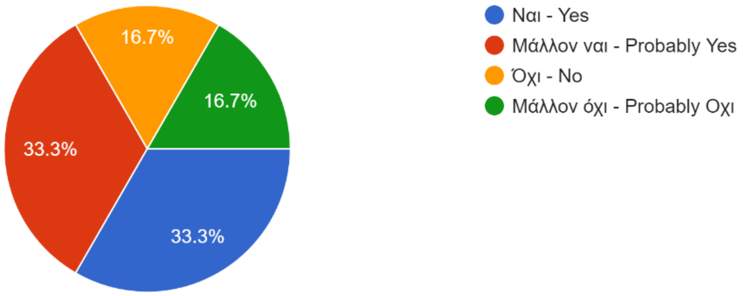
Αν μια εφαρμογή σου ζητούσε να εγκαταστήσεις ένα επιπλέον πρόγραμμα ασφάλειας στην συσκευή σου, θα το έκα...nent to your device would you do it?

6 responses



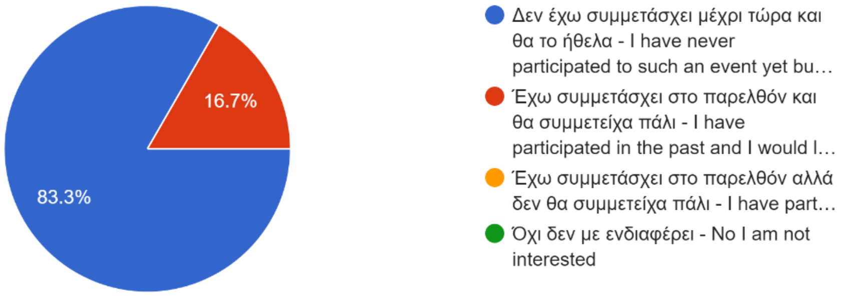
Θα πλήρωνες για ένα πρόγραμμα ασφάλειας στην συσκευή σου; - Would you pay for a security application in your device?

6 responses



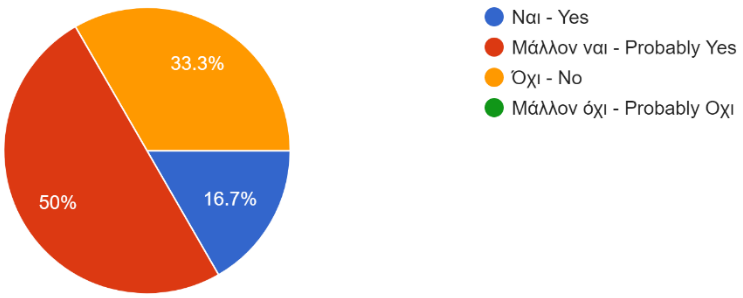
Θα συμμετείχες σε εκδηλώσεις εκπαίδευσης σχετικά με την ασφάλεια στο Διαδίκτυο; - Would you participate in training events for Internet security;

6 responses



Θα πλήρωνες για ένα πρόγραμμα εκπαίδευσης για ασφάλεια στο Διαδίκτυο; - Would you pay for a training program for Internet security?

6 responses


● Ναι - Yes
● Μάλλον ναι - Probably Yes
● Όχι - No
● Μάλλον όχι - Probably Οχι