Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

SMESEC

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

D3.5 Preliminary SMESEC Security Awareness and Training Report

Document Identification			
Status	Final	**Due Date**	30/11/2018
Version	1.0	**Submission Date**	20/12/2018

Related WP	WP3	**Document Reference**	D3.5
Related Deliverable(s)	-----	**Dissemination Level (*)**	PU
Lead Organisation	EGM	**Lead Author**	Philippe Cousin
Contributors	EGM, FHNW, UoP	**Reviewers**	Francisco Fernandez (WoS) Ciprian Oprisa (BD)

Keywords:

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

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.

Document Information

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

Document History			
Version	Date	Change editors	Changes
0.1	24/10/2018	Philippe COUSIN	ToC for discussion and contribution
0.2	5/11/2018	Philippe COUSIN	Revised ToC after contributions FHNW and ATOS
0.3	15/11/2018	Abbas Ahmad	Contribution training template
0.4	21/11	Kostas Lampropoulos	Contribution to training platform
0.5	23/11	Samuel FRICKER	Contribution FNHW
0.6	25/11	Abbas Ahmad	Update contributions EGM
0.7	28/11	Kostas Lampropoulos	Update UoP contribution
0.8	28/11	Philippe COUSIN	EGM contributions to pre-final version
0.9	10/12	Philippe COUSIN	Finalisation first final version for review
0.91	15/12	Jose Ruiz (Atos) Michal Burdzy (Gridpocket)	Contribution from Spain and Poland
1.0	18/12	Cipran Oprisa (Bitdefender) Francisco Hernandez (worldsensing) Philippe COUSIN	Finalisation after internal reviews

Quality Control		
Role	**Who (Partner short name)**	**Approval Date**
Deliverable leader	Philippe Cousin (EGM)	20/12/2018
Technical manager	Christos Tselios (Citrix)	20/12/2018
Quality manager	Rosana Valle Soriano (Atos)	20/12/2018
Project Manager	Jose Fran. Ruíz (Atos)	20/12/2018

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 status of 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 is taking into account 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 preliminary work to develop tools to interact with the SMEs such as the dedicated questionnaires and the Cyber Security Coaching tool (e.g. CYSEC tool). The SMESEC consortium has already started to interact with some SMEs at various events and initiated many contacts with European and National SMEs associations. Such associations are now waiting for SMESEC to present the first iteration of the project solution. Many interactions with SMEs through on-line communication, webinars and workshops are already planned for the 2nd period.

The training platform was successfully developed, and some initial materials and courses were added. We plan to organise a training session at the beginning 2nd project period.

The initial feedback from the SMEs about the understanding of cybersecurity items was provided in the 1st period, but the more we interact with them, the more we expect getting more details in the second period.

1 Introduction of the T3.5 task activity

This report provides an overview of the status of 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 D2.3.

The task takes into account 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 authorities 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 have planned the following tasks in a 2-phase approach:

a) **Develop tools for interacting with SMEs**: the main tool is a Cyber Coaching (CYSEC) tool (see 2.2) but other tools were also developed 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);
- Direct interviews by phone or F2F with selected SME people;
  We will also plan interaction with Public authorities as part of the feedback process

c) **Development of training materials and the organisation of training sessions**: we have put in place a training platform and have started to populate it with specific material. We will also explore interactions with other security related training platform;

d) **Organise a certification programme**: we will develop a plan per training and we will study the feasibility of an overall certification programme for cybersecurity for SMEs.

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

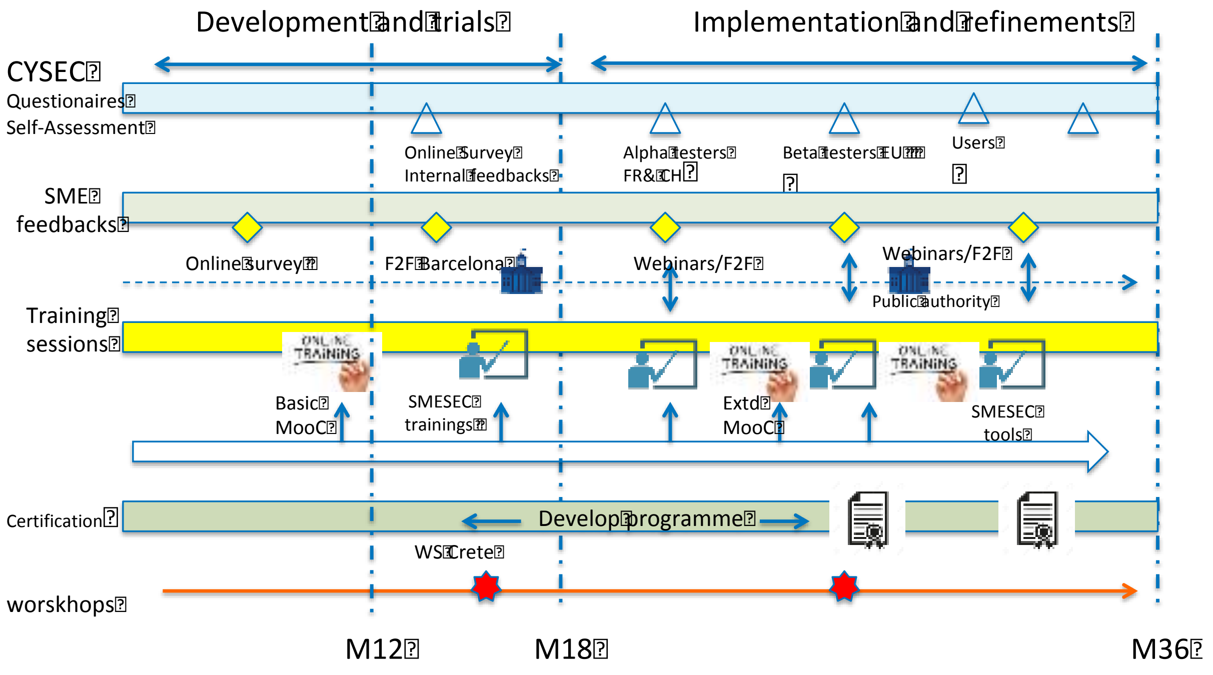


Figure 1: simplified overview of T3.3 activities

The awareness programme activity is aligned with actions organised in the dissemination plan. To reach the SMEs, we will combine 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 (see chapter 3). Individual SMEs will be 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 are approaching 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". We are, therefore, looking at cybersecurity key events. For instance, in the first period we have been present at ETSI security week. More actions are described in Deliverable 6.2.

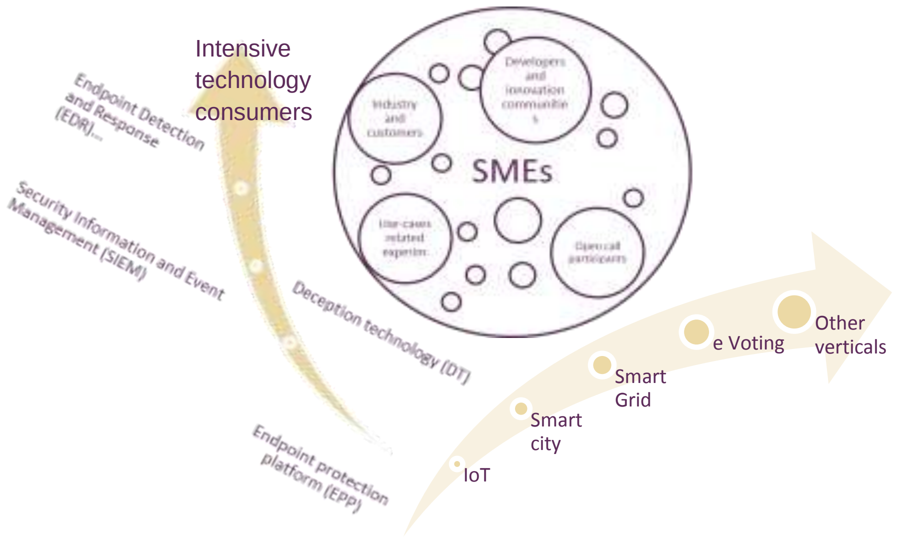

Intensive technology consumers
Endpoint Detection and Response (EDR)...
Security Information and Event Management (SIEM)
Deception technology (DT)
Endpoint protection platform (EPP)
Industry and customers
Developers and innovation communitie s
SMEs
Use-cases related experim.
Open call participants
IoT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

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 1, 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 milestones for the SMESEC awareness and validation plan:

Table 1: Milestones for the SMESEC awareness and validation plan (D2.3)

Milestone	Timing	Elaboration
Cyber threat awareness	Year 1	During this phase, SMESEC dissemination has raised awareness of cyber threats for SMEs. At the same time, the SMESEC brand was established with the values of trust in SMESEC, respect for the expertise of the SMESEC consortium, and simplicity of the SMESEC framework.
Interest in SMESEC	Year 2	During this phase, SMESEC dissemination will communicate results of the SMESEC project and endorsements of SME that were using these results. SMEs will get the opportunity to register in the SMESEC community and apply for the open call.
Adoption of SMESEC	Year 3	During this phase, SMESEC dissemination will communicate results of SMESEC validation to encourage adoption of the SMESEC framework. More SMEs will register in the SMESEC community and enable broad adoption of the framework.

2.2 The status of the CYSEC tool

2.2.1 CYSEC concept and tool

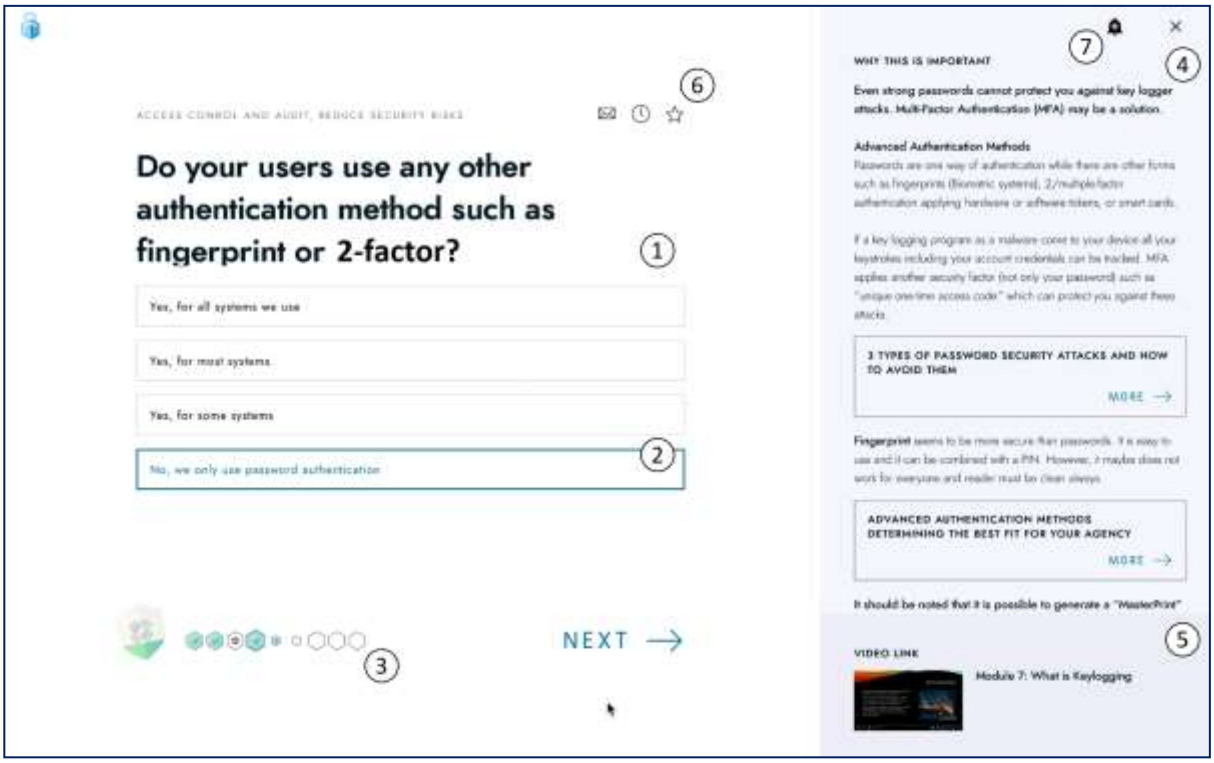
CYSEC is a tool developed by FHNW for helping the SME employee responsible for cybersecurity to learn about cybersecurity and develop capabilities for the SME in the capability areas described in D2.3:

- Fast ramp-up: user training, access control and audit, patch management, malware scans, and code inspection.
- Capability-building: absorption networks, network controls, intrusion prevention, credential management, second opinion defence, security engineering, application change management, compliance audits, and standards compliance.

The use of the CYSEC tools allows the SME to cut the cost of adopting cybersecurity thanks to the support of the simple do-it-yourself cybersecurity assessment and improvement. CYSEC changes the expensive consultant-driven process improvement approach that is well established for large companies to self-reliant, inexpensive cybersecurity assessment and improvement that is also sustainable for cybersecurity vendors because a large number of SMEs can benefit from it.

The overview of features and the technical approach has been described in D3.4 (“FHNW Individual Extensions”), including the capability improvement dashboard that provides the SME employee with the ability to assess the progressing cybersecurity status of the SME and to get recommendations regarding what to do in the next steps.

This section outlines the status of development of the contents for the capability improvement journeys that provide the SME employee with the ability to learn and implement about cybersecurity for each of the capability areas in a simple, step-wise do-it-yourself fashion. The following figure illustrates the user interface of the capability improvement journey and how the cybersecurity feedback and the improvement advice is delivered to the SME employee.



ACCESS CONTROL AND AUDIT, REDUCE SECURITY RISKS

Do your users use any other authentication method such as fingerprint or 2-factor?

- Yes, for all systems we use
- Yes, for most systems
- Yes, for some systems
- [✓ No, we only use password authentication]

WHY THIS IS IMPORTANT

Even strong passwords cannot protect you against key logger attacks. Multi-Factor Authentication (MFA) may be a solution.

Advanced Authentication Methods

Passwords are one way of authentication while there are other forms such as fingerprints (Biometric systems), 2/multiple factor authentication applying hardware or software tokens, or smart cards.

If a key logging program as a malware comes to your device all your keystrokes including your account credentials can be tracked. MFA applies another security factor (not only your password) such as "unique one-time access code" which can protect you against these attacks.

3 TYPES OF PASSWORD SECURITY ATTACKS AND HOW TO AVOID THEM

Fingerprint seems to be more secure than passwords. It is easy to use and it can be combined with a PIN. However, it maybe does not work for everyone and reader must be clean always.

ADVANCED AUTHENTICATION METHODS DETERMINING THE BEST FIT FOR YOUR AGENCY

It should be noted that it is possible to generate a "MasterPrint"

VIDEO LINK

Module 7: What is Keylogging

Figure 3: Example of a screen reflecting a step in the capability improvement journey.

The screen offers the following benefits for the SME employee:

- Assessment of cybersecurity capability: simple assessment question (1) and answers reflecting the implementation degree (2).
- Advice for how to implement cybersecurity: call for action, motivation and facts supporting the action, recommendation for guidelines, and tools (with preference SMESEC framework tools) (4) and training to get introduced into the topic underlying the capability (with preference SMESEC training) (5).
- Management of cybersecurity improvements: instructing colleagues, setting reminders, and starring questions to be remembered (6) and feedback of the CYSEC recommender regarding the SME employee's decisions and actions.

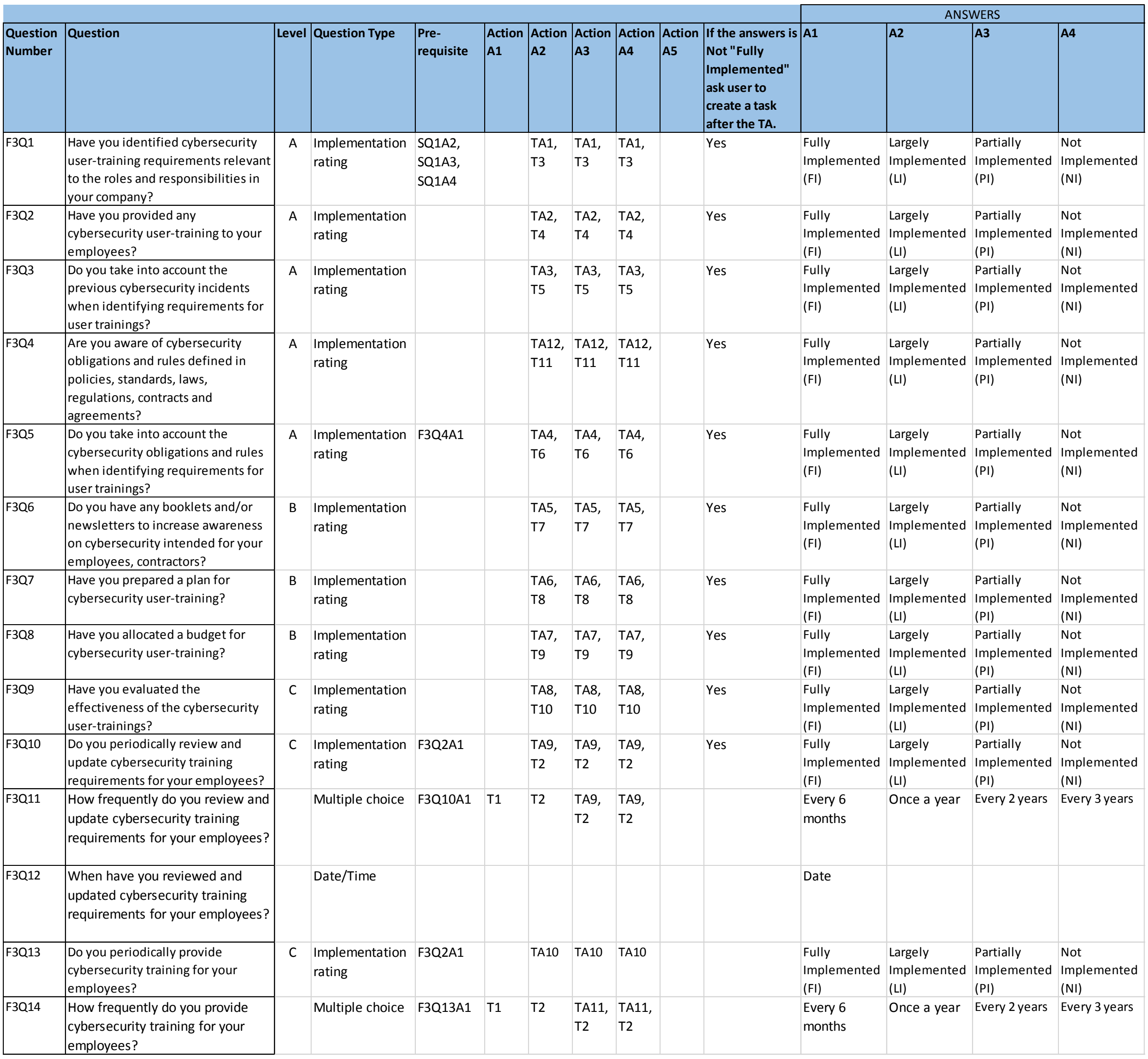
FHNW collaborates with the University of Utrecht in the development of the contents for the CYSEC capability improvement journeys. A 3-step content development approach is being pursued:

- Development Step 1: Definition of scope and questions for each capability area. The definition reflects the state-of-the-art analysis results of cybersecurity in a SMEs performed by the University of Utrecht.

- Development Step 2: Low-Fi prototyping of the journey and how the questions, answers, recommendations, and training are offered. The prototypes reflect the presentation of the capabilities and selection of advice offered to the SME employee in the framework of the CYSEC tool. The prototypes reflect the opinion of cybersecurity experts regarding the application of the CYSEC contents for SMEs.
- Development Step 3: Specification of the XML file used to configure and inject the appropriate cybersecurity coach behaviour into the CYSEC tool. The specifications are rendered by the CYSEC tool, giving the final appearance to the human end user of CYSEC. The rendering offers the full SMESEC user experience for the developed content.

2.2.2 CYSEC content development step 1: scope and question definition

The development step 1 for a CYSEC capability area concerns the definition of scope and questions. The following figure shows an example of the definition of scope and questions for one capability area: the end user training.

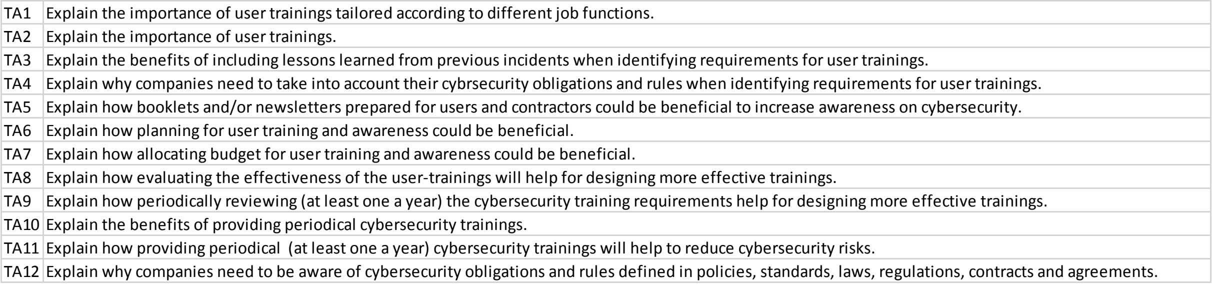


											ANSWERS			
Question Number	Question	Level	Question Type	Pre-requisite	Action A1	Action A2	Action A3	Action A4	Action A5	If the answers is Not "Fully Implemented" ask user to create a task after the TA.	A1	A2	A3	A4
F3Q1	Have you identified cybersecurity user-training requirements relevant to the roles and responsibilities in your company?	A	Implementation rating	SQ1A2, SQ1A3, SQ1A4		TA1, T3	TA1, T3	TA1, T3		Yes	Fully Implemented (FI)	Largely Implemented (LI)	Partially Implemented (PI)	Not Implemented (NI)
F3Q2	Have you provided any cybersecurity user-training to your employees?	A	Implementation rating			TA2, T4	TA2, T4	TA2, T4		Yes	Fully Implemented (FI)	Largely Implemented (LI)	Partially Implemented (PI)	Not Implemented (NI)
F3Q3	Do you take into account the previous cybersecurity incidents when identifying requirements for user trainings?	A	Implementation rating			TA3, T5	TA3, T5	TA3, T5		Yes	Fully Implemented (FI)	Largely Implemented (LI)	Partially Implemented (PI)	Not Implemented (NI)
F3Q4	Are you aware of cybersecurity obligations and rules defined in policies, standards, laws, regulations, contracts and agreements?	A	Implementation rating			TA12, T11	TA12, T11	TA12, T11		Yes	Fully Implemented (FI)	Largely Implemented (LI)	Partially Implemented (PI)	Not Implemented (NI)
F3Q5	Do you take into account the cybersecurity obligations and rules when identifying requirements for user trainings?	A	Implementation rating	F3Q4A1		TA4, T6	TA4, T6	TA4, T6		Yes	Fully Implemented (FI)	Largely Implemented (LI)	Partially Implemented (PI)	Not Implemented (NI)
F3Q6	Do you have any booklets and/or newsletters to increase awareness on cybersecurity intended for your employees, contractors?	B	Implementation rating			TA5, T7	TA5, T7	TA5, T7		Yes	Fully Implemented (FI)	Largely Implemented (LI)	Partially Implemented (PI)	Not Implemented (NI)
F3Q7	Have you prepared a plan for cybersecurity user-training?	B	Implementation rating			TA6, T8	TA6, T8	TA6, T8		Yes	Fully Implemented (FI)	Largely Implemented (LI)	Partially Implemented (PI)	Not Implemented (NI)
F3Q8	Have you allocated a budget for cybersecurity user-training?	B	Implementation rating			TA7, T9	TA7, T9	TA7, T9		Yes	Fully Implemented (FI)	Largely Implemented (LI)	Partially Implemented (PI)	Not Implemented (NI)
F3Q9	Have you evaluated the effectiveness of the cybersecurity user-trainings?	C	Implementation rating			TA8, T10	TA8, T10	TA8, T10		Yes	Fully Implemented (FI)	Largely Implemented (LI)	Partially Implemented (PI)	Not Implemented (NI)
F3Q10	Do you periodically review and update cybersecurity training requirements for your employees?	C	Implementation rating	F3Q2A1		TA9, T2	TA9, T2	TA9, T2		Yes	Fully Implemented (FI)	Largely Implemented (LI)	Partially Implemented (PI)	Not Implemented (NI)
F3Q11	How frequently do you review and update cybersecurity training requirements for your employees?		Multiple choice	F3Q10A1	T1	T2	TA9, T2	TA9, T2			Every 6 months	Once a year	Every 2 years	Every 3 years
F3Q12	When have you reviewed and updated cybersecurity training requirements for your employees?		Date/Time								Date			
F3Q13	Do you periodically provide cybersecurity training for your employees?	C	Implementation rating	F3Q2A1		TA10	TA10	TA10			Fully Implemented (FI)	Largely Implemented (LI)	Partially Implemented (PI)	Not Implemented (NI)
F3Q14	How frequently do you provide cybersecurity training for your employees?		Multiple choice	F3Q13A1	T1	T2	TA11, T2	TA11, T2			Every 6 months	Once a year	Every 2 years	Every 3 years

Figure 4: Definition of scope and questions for a capability area. Here: the end user training.

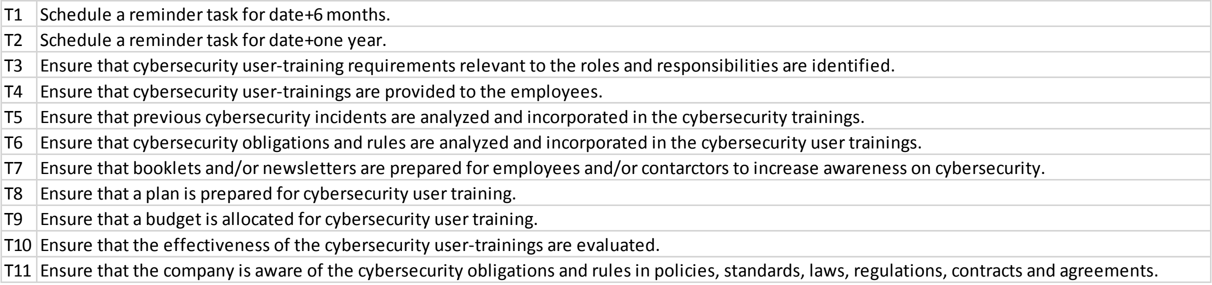
Each capability area is defined with a series of assessment questions that are mapped to a cybersecurity maturity level. The maturity levels from A to C offer a partial ordering of the assessment, giving the SME the ability to approach the assessment and improvement in a step-wise fashion. Each question is associated with training tips that allow the SME employee to learn about the question's topic and actions that are recommended to be implemented for fulfilling the capability. The questions are answered with a statement about the implementation degree of the capability or a decision of when or how frequent a practice will be pursued by the SME.

The following figures show the training tips (TAx) and Tasks (Tx) that are recommended as actions supporting the cybersecurity assessment underlying the CYSEC questions.



TA1	Explain the importance of user trainings tailored according to different job functions.
TA2	Explain the importance of user trainings.
TA3	Explain the benefits of including lessons learned from previous incidents when identifying requirements for user trainings.
TA4	Explain why companies need to take into account their cybrsecurity obligations and rules when identifying requirements for user trainings.
TA5	Explain how booklets and/or newsletters prepared for users and contractors could be beneficial to increase awareness on cybersecurity.
TA6	Explain how planning for user training and awareness could be beneficial.
TA7	Explain how allocating budget for user training and awareness could be beneficial.
TA8	Explain how evaluating the effectiveness of the user-trainings will help for designing more effective trainings.
TA9	Explain how periodically reviewing (at least one a year) the cybersecurity training requirements help for designing more effective trainings.
TA10	Explain the benefits of providing periodical cybersecurity trainings.
TA11	Explain how providing periodical (at least one a year) cybersecurity trainings will help to reduce cybersecurity risks.
TA12	Explain why companies need to be aware of cybersecurity obligations and rules defined in policies, standards, laws, regulations, contracts and agreements.

Figure 5: Recommended actions supporting the assessment: training tips

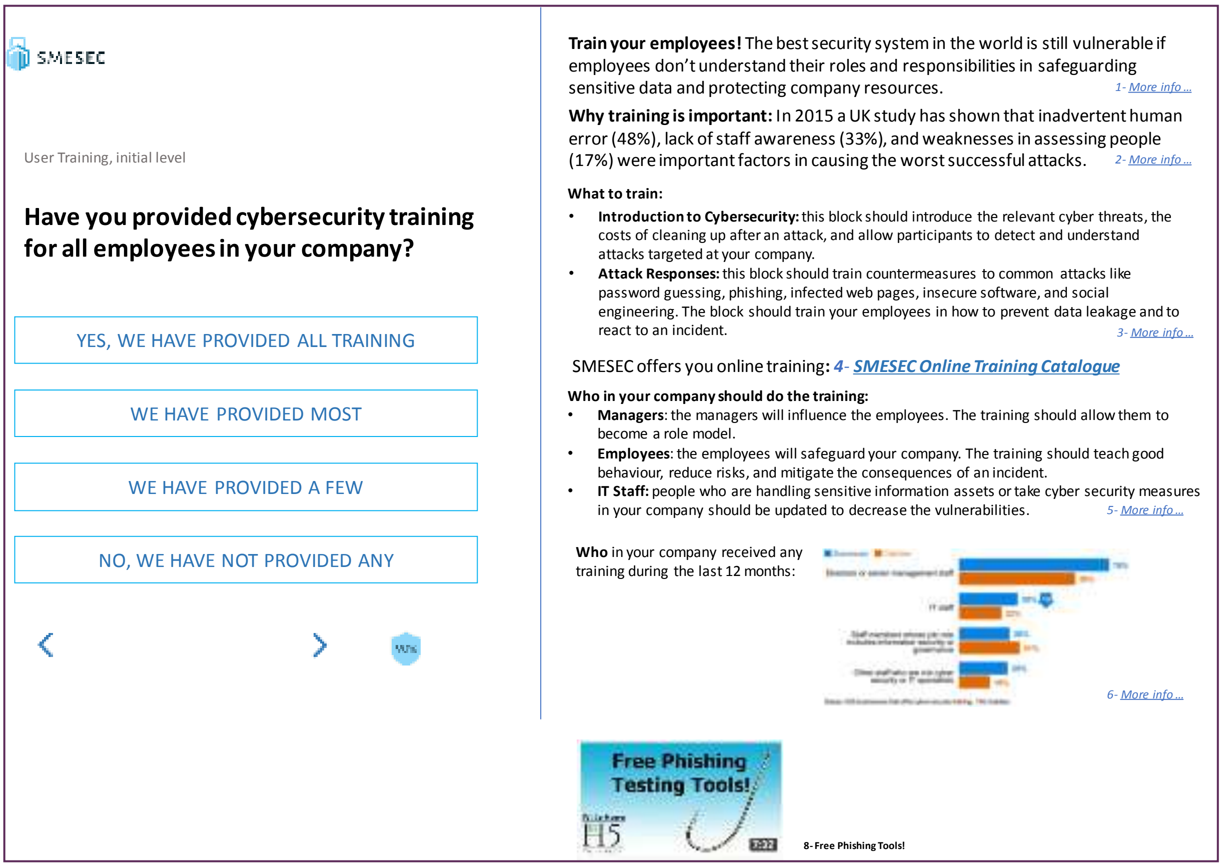


T1	Schedule a reminder task for date+6 months.
T2	Schedule a reminder task for date+one year.
T3	Ensure that cybersecurity user-training requirements relevant to the roles and responsibilities are identified.
T4	Ensure that cybersecurity user-trainings are provided to the employees.
T5	Ensure that previous cybersecurity incidents are analyzed and incorporated in the cybersecurity trainings.
T6	Ensure that cybersecurity obligations and rules are analyzed and incorporated in the cybersecurity user trainings.
T7	Ensure that booklets and/or newsletters are prepared for employees and/or contarctors to increase awareness on cybersecurity.
T8	Ensure that a plan is prepared for cybersecurity user training.
T9	Ensure that a budget is allocated for cybersecurity user training.
T10	Ensure that the effectiveness of the cybersecurity user-trainings are evaluated.
T11	Ensure that the company is aware of the cybersecurity obligations and rules in policies, standards, laws, regulations, contracts and agreements.

Figure 6: Recommended actions supporting the assessment: recommended tasks.

2.2.3 CYSEC content development step 2: prototyping

The development step 2 for a CYSEC capability area concerns the prototyping of the SME employee end user journey and how the questions, answers, recommendations, and training materials are offered. The following screenshots show the series of screens prepared for the CYSEC tool for the capability area user training.



User Training, initial level

Have you provided cybersecurity training for all employees in your company?

YES, WE HAVE PROVIDED ALL TRAINING

WE HAVE PROVIDED MOST

WE HAVE PROVIDED A FEW

NO, WE HAVE NOT PROVIDED ANY

Train your employees! The best security system in the world is still vulnerable if employees don't understand their roles and responsibilities in safeguarding sensitive data and protecting company resources. *1- More info ...*

Why training is important: In 2015 a UK study has shown that inadvertent human error (48%), lack of staff awareness (33%), and weaknesses in assessing people (17%) were important factors in causing the worst successful attacks. *2- More info ...*

What to train:

- **Introduction to Cybersecurity:** this block should introduce the relevant cyber threats, the costs of cleaning up after an attack, and allow participants to detect and understand attacks targeted at your company.
- **Attack Responses:** this block should train countermeasures to common attacks like password guessing, phishing, infected web pages, insecure software, and social engineering. The block should train your employees in how to prevent data leakage and to react to an incident. *3- More info ...*

SMESEC offers you online training: *4- **SMESEC Online Training Catalogue***

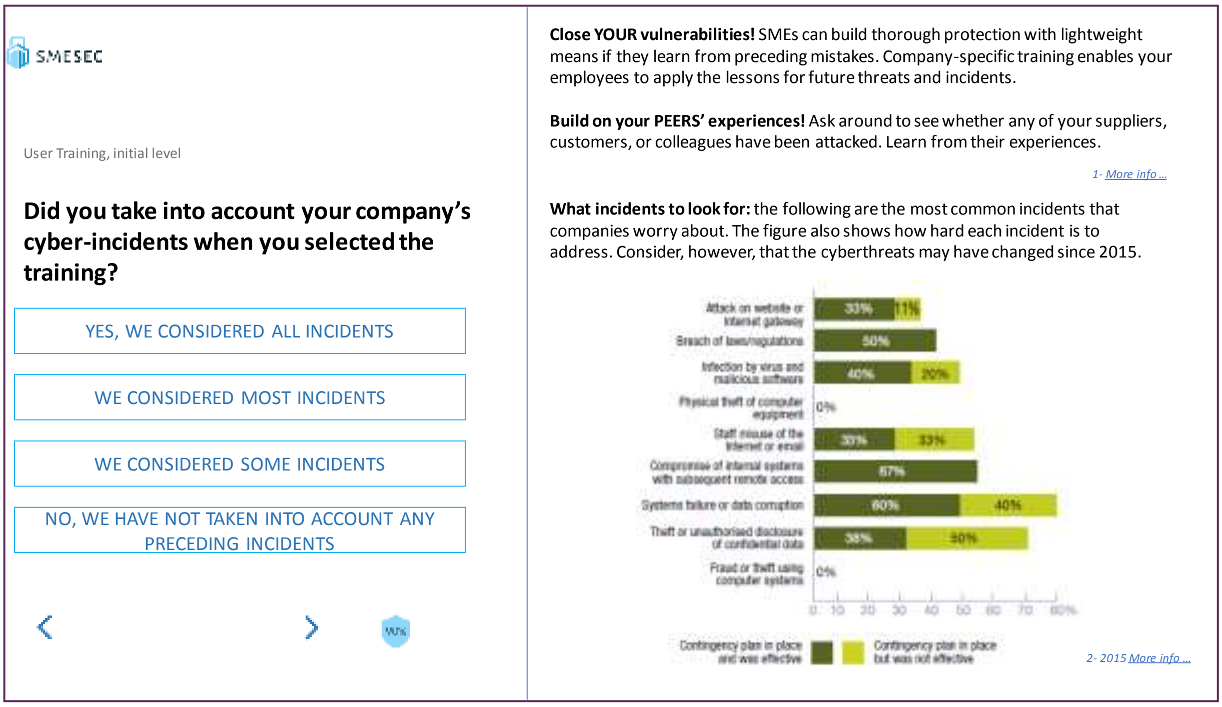
Who in your company should do the training:

- **Managers**: the managers will influence the employees. The training should allow them to become a role model.
- **Employees**: the employees will safeguard your company. The training should teach good behaviour, reduce risks, and mitigate the consequences of an incident.
- **IT Staff:** people who are handling sensitive information assets or take cyber security measures in your company should be updated to decrease the vulnerabilities. *5- More info ...*

Who in your company received any training during the last 12 months:

6- More info ...

8- Free Phishing Tools!



SMESEC
Attack on website or internet gateway
Breach of laws/regulations
Infection by virus and malicious software
Physical theft of computer equipment
Staff misuse of the internet or email
Compromise of internal systems with subsequent remote access
Systems failure or data corruption
Theft or unauthorised disclosure of confidential data
Fraud or theft using computer systems
33%
11%
50%
40%
20%
0%
33%
33%
67%
60%
40%
38%
50%
0%
0
10
20
30
40
50
60
70
80%
Contingency plan in place and was effective
Contingency plan in place but was not effective

User Training, initial level

Did you take into account your company's cyber-incidents when you selected the training?

YES, WE CONSIDERED ALL INCIDENTS

WE CONSIDERED MOST INCIDENTS

WE CONSIDERED SOME INCIDENTS

NO, WE HAVE NOT TAKEN INTO ACCOUNT ANY PRECEDING INCIDENTS

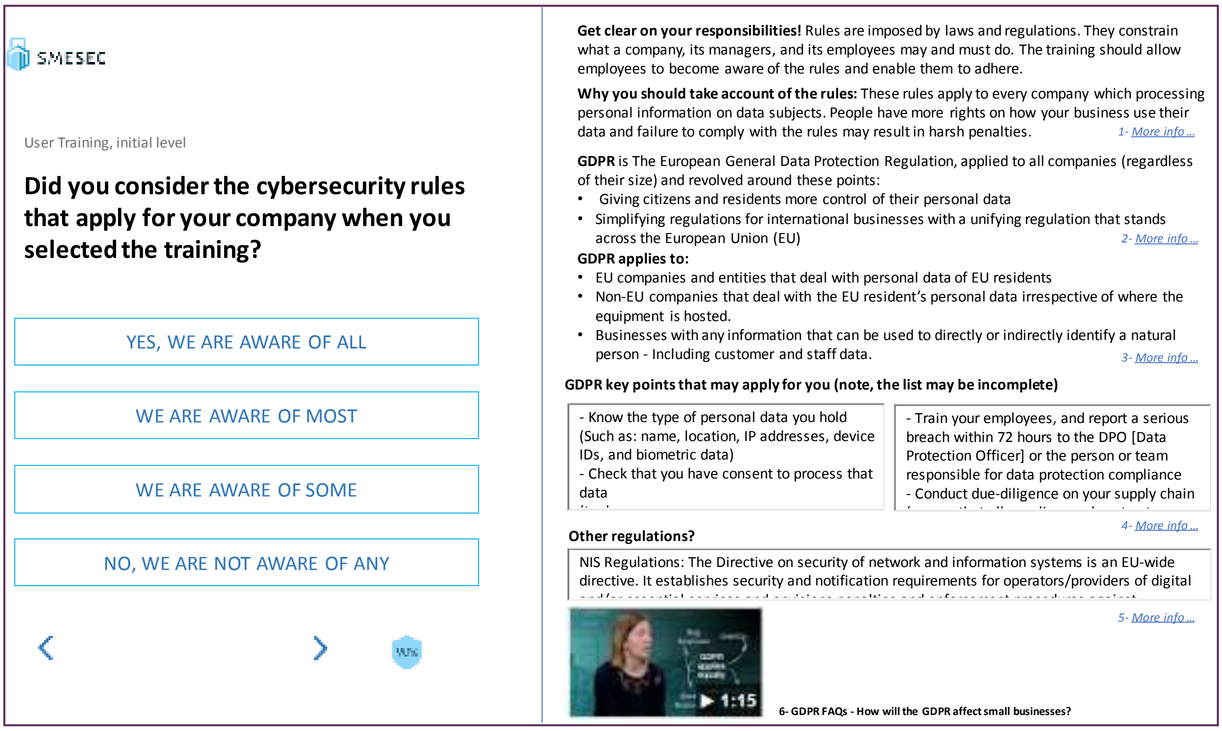
Close YOUR vulnerabilities! SMEs can build thorough protection with lightweight means if they learn from preceding mistakes. Company-specific training enables your employees to apply the lessons for future threats and incidents.

Build on your PEERS' experiences! Ask around to see whether any of your suppliers, customers, or colleagues have been attacked. Learn from their experiences.

1- More info ...

What incidents to look for: the following are the most common incidents that companies worry about. The figure also shows how hard each incident is to address. Consider, however, that the cyberthreats may have changed since 2015.

2- 2015 More info ...



SMESEC

User Training, initial level

Did you consider the cybersecurity rules that apply for your company when you selected the training?

YES, WE ARE AWARE OF ALL

WE ARE AWARE OF MOST

WE ARE AWARE OF SOME

NO, WE ARE NOT AWARE OF ANY

Get clear on your responsibilities! Rules are imposed by laws and regulations. They constrain what a company, its managers, and its employees may and must do. The training should allow employees to become aware of the rules and enable them to adhere.

Why you should take account of the rules: These rules apply to every company which processing personal information on data subjects. People have more rights on how your business use their data and failure to comply with the rules may result in harsh penalties. *1- More info ...*

GDPR is The European General Data Protection Regulation, applied to all companies (regardless of their size) and revolved around these points:

- Giving citizens and residents more control of their personal data
- Simplifying regulations for international businesses with a unifying regulation that stands across the European Union (EU) *2- More info ...*

GDPR applies to:

- EU companies and entities that deal with personal data of EU residents
- Non-EU companies that deal with the EU resident's personal data irrespective of where the equipment is hosted.
- Businesses with any information that can be used to directly or indirectly identify a natural person - Including customer and staff data. *3- More info ...*

GDPR key points that may apply for you (note, the list may be incomplete)

- Know the type of personal data you hold (Such as: name, location, IP addresses, device IDs, and biometric data)
- Check that you have consent to process that data

- Train your employees, and report a serious breach within 72 hours to the DPO [Data Protection Officer] or the person or team responsible for data protection compliance
- Conduct due-diligence on your supply chain

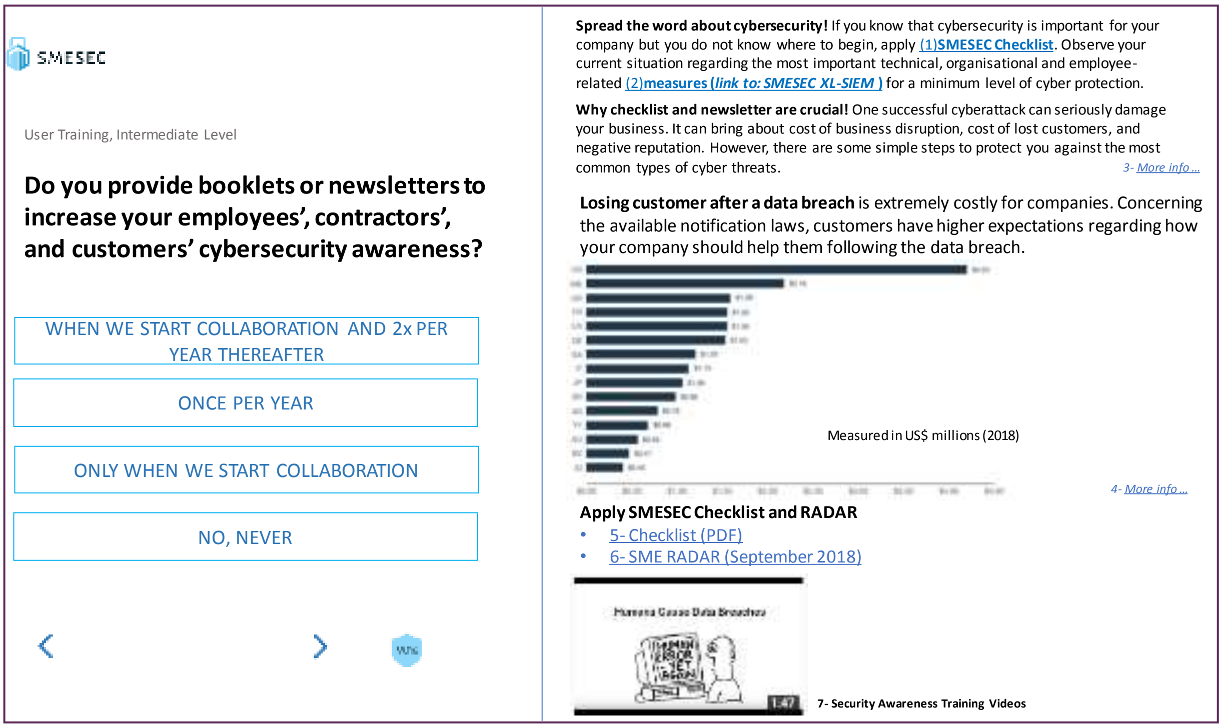
4- More info ...

Other regulations?

NIS Regulations: The Directive on security of network and information systems is an EU-wide directive. It establishes security and notification requirements for operators/providers of digital

5- More info ...

6- GDPR FAQs - How will the GDPR affect small businesses?



SMESEC

User Training, Intermediate Level

Do you provide booklets or newsletters to increase your employees', contractors', and customers' cybersecurity awareness?

WHEN WE START COLLABORATION AND 2x PER YEAR THEREAFTER

ONCE PER YEAR

ONLY WHEN WE START COLLABORATION

NO, NEVER

Spread the word about cybersecurity! If you know that cybersecurity is important for your company but you do not know where to begin, apply (1)**SMESEC Checklist**. Observe your current situation regarding the most important technical, organisational and employee-related (2)**measures (*link to: SMESEC XL-SIEM*)** for a minimum level of cyber protection.

Why checklist and newsletter are crucial! One successful cyberattack can seriously damage your business. It can bring about cost of business disruption, cost of lost customers, and negative reputation. However, there are some simple steps to protect you against the most common types of cyber threats. *3- More info ...*

Losing customer after a data breach is extremely costly for companies. Concerning the available notification laws, customers have higher expectations regarding how your company should help them following the data breach.

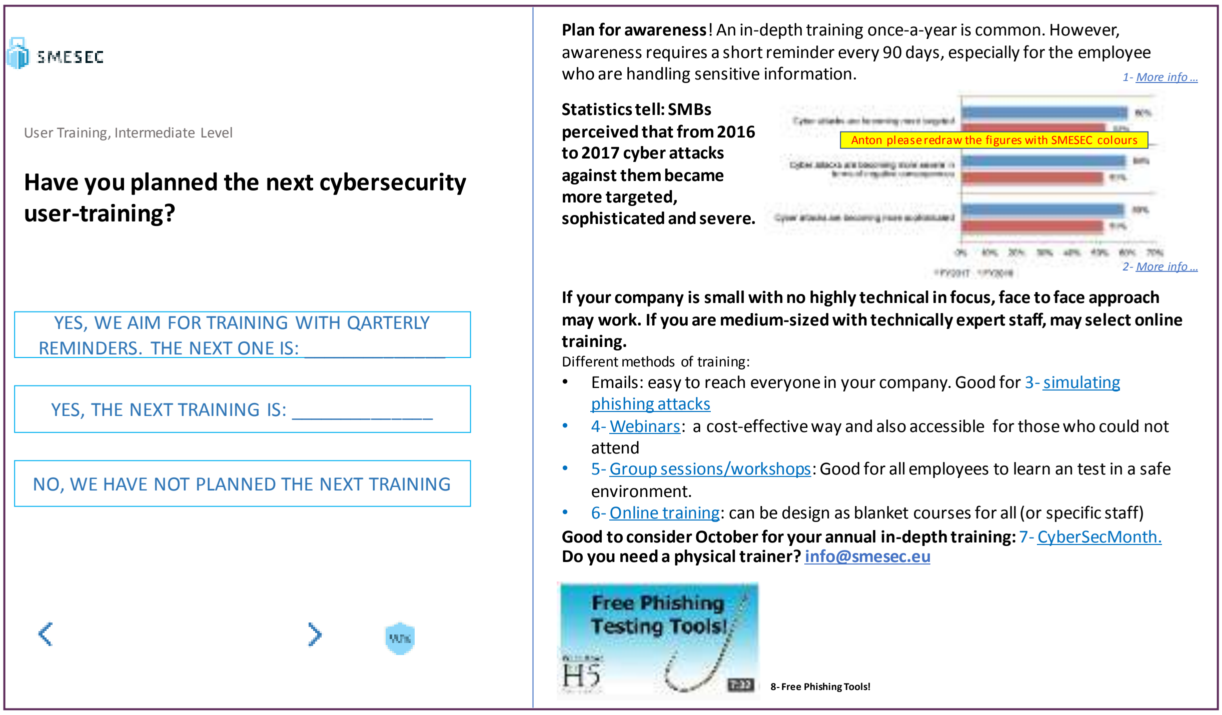
Measured in US$ millions (2018)

4- More info ...

Apply SMESEC Checklist and RADAR

- 5- Checklist (PDF)
- 6- SME RADAR (September 2018)

7- Security Awareness Training Videos



SMESEC

User Training, Intermediate Level

Have you planned the next cybersecurity user-training?

YES, WE AIM FOR TRAINING WITH QARTERLY REMINDERS. THE NEXT ONE IS: _______________

YES, THE NEXT TRAINING IS: _______________

NO, WE HAVE NOT PLANNED THE NEXT TRAINING

Plan for awareness! An in-depth training once-a-year is common. However, awareness requires a short reminder every 90 days, especially for the employee who are handling sensitive information.

1- More info …

Statistics tell: SMBs perceived that from 2016 to 2017 cyber attacks against them became more targeted, sophisticated and severe.

Cyber attacks are becoming more targeted
Cyber attacks are becoming more severe in terms of negative consequences
Cyber attacks are becoming more sophisticated
60%
59%
0%
10%
20%
30%
40%
50%
60%
70%
FY2017
FY2016

Anton please redraw the figures with SMESEC colours

2- More info …

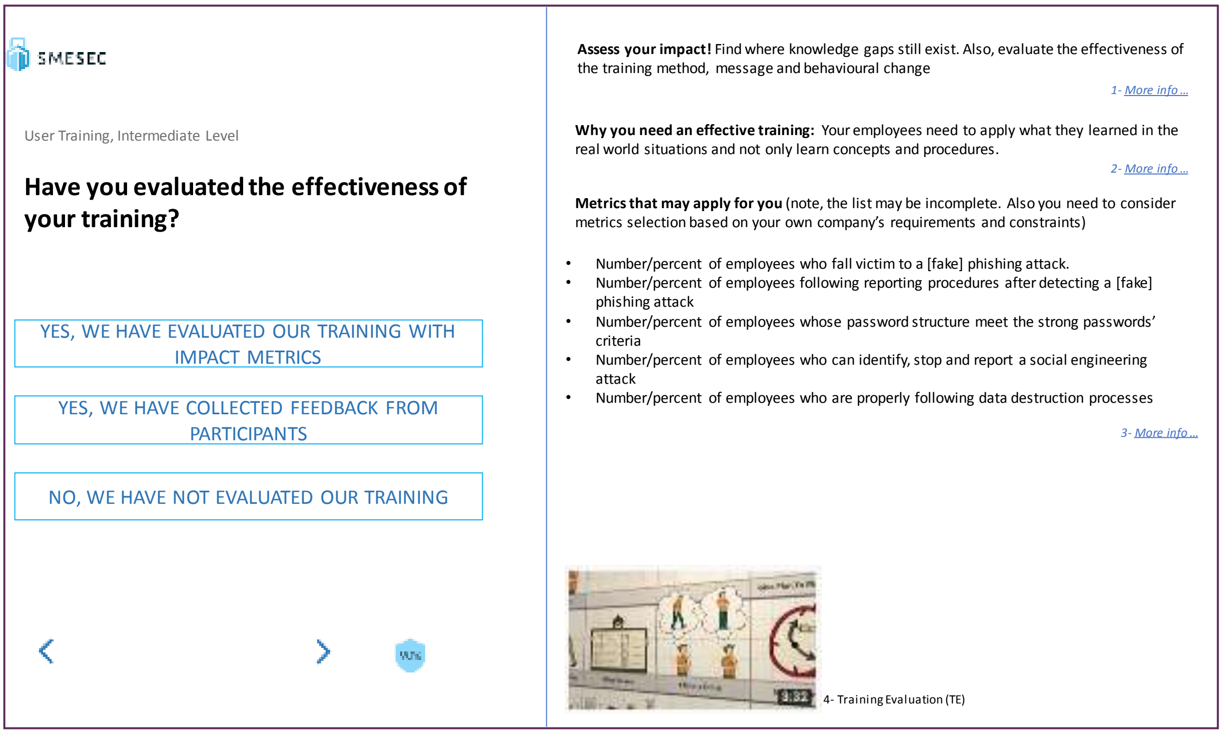
If your company is small with no highly technical in focus, face to face approach may work. If you are medium-sized with technically expert staff, may select online training.

Different methods of training:

- Emails: easy to reach everyone in your company. Good for 3- simulating phishing attacks
- 4- Webinars: a cost-effective way and also accessible for those who could not attend
- 5- Group sessions/workshops: Good for all employees to learn an test in a safe environment.
- 6- Online training: can be design as blanket courses for all (or specific staff)

Good to consider October for your annual in-depth training: 7- CyberSecMonth.
Do you need a physical trainer? **info@smesec.eu**

8- Free Phishing Tools!



SMESEC

User Training, Intermediate Level

Have you evaluated the effectiveness of your training?

YES, WE HAVE EVALUATED OUR TRAINING WITH IMPACT METRICS

YES, WE HAVE COLLECTED FEEDBACK FROM PARTICIPANTS

NO, WE HAVE NOT EVALUATED OUR TRAINING

Assess your impact! Find where knowledge gaps still exist. Also, evaluate the effectiveness of the training method, message and behavioural change

1- More info …

Why you need an effective training: Your employees need to apply what they learned in the real world situations and not only learn concepts and procedures.

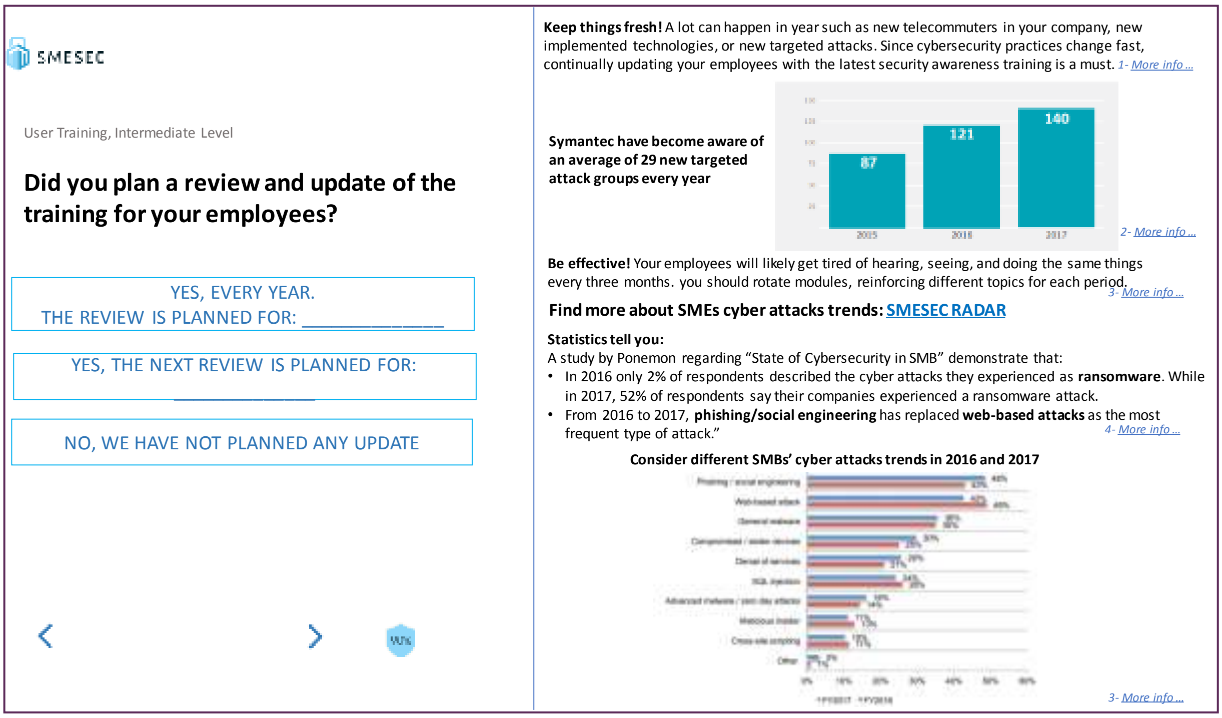
2- More info …

Metrics that may apply for you (note, the list may be incomplete. Also you need to consider metrics selection based on your own company's requirements and constraints)

- Number/percent of employees who fall victim to a [fake] phishing attack.
- Number/percent of employees following reporting procedures after detecting a [fake] phishing attack
- Number/percent of employees whose password structure meet the strong passwords' criteria
- Number/percent of employees who can identify, stop and report a social engineering attack
- Number/percent of employees who are properly following data destruction processes

3- More info …

4- Training Evaluation (TE)



User Training, Intermediate Level

Did you plan a review and update of the training for your employees?

YES, EVERY YEAR.
THE REVIEW IS PLANNED FOR: _______________

YES, THE NEXT REVIEW IS PLANNED FOR:
____

NO, WE HAVE NOT PLANNED ANY UPDATE

Keep things fresh! A lot can happen in year such as new telecommuters in your company, new implemented technologies, or new targeted attacks. Since cybersecurity practices change fast, continually updating your employees with the latest security awareness training is a must. *1- More info …*

Symantec have become aware of an average of 29 new targeted attack groups every year

2- More info …

Be effective! Your employees will likely get tired of hearing, seeing, and doing the same things every three months. you should rotate modules, reinforcing different topics for each period. *3- More info …*

Find more about SMEs cyber attacks trends: SMESEC RADAR

Statistics tell you:

A study by Ponemon regarding "State of Cybersecurity in SMB" demonstrate that:

- In 2016 only 2% of respondents described the cyber attacks they experienced as **ransomware**. While in 2017, 52% of respondents say their companies experienced a ransomware attack.
- From 2016 to 2017, **phishing/social engineering** has replaced **web-based attacks** as the most frequent type of attack." *4- More info …*

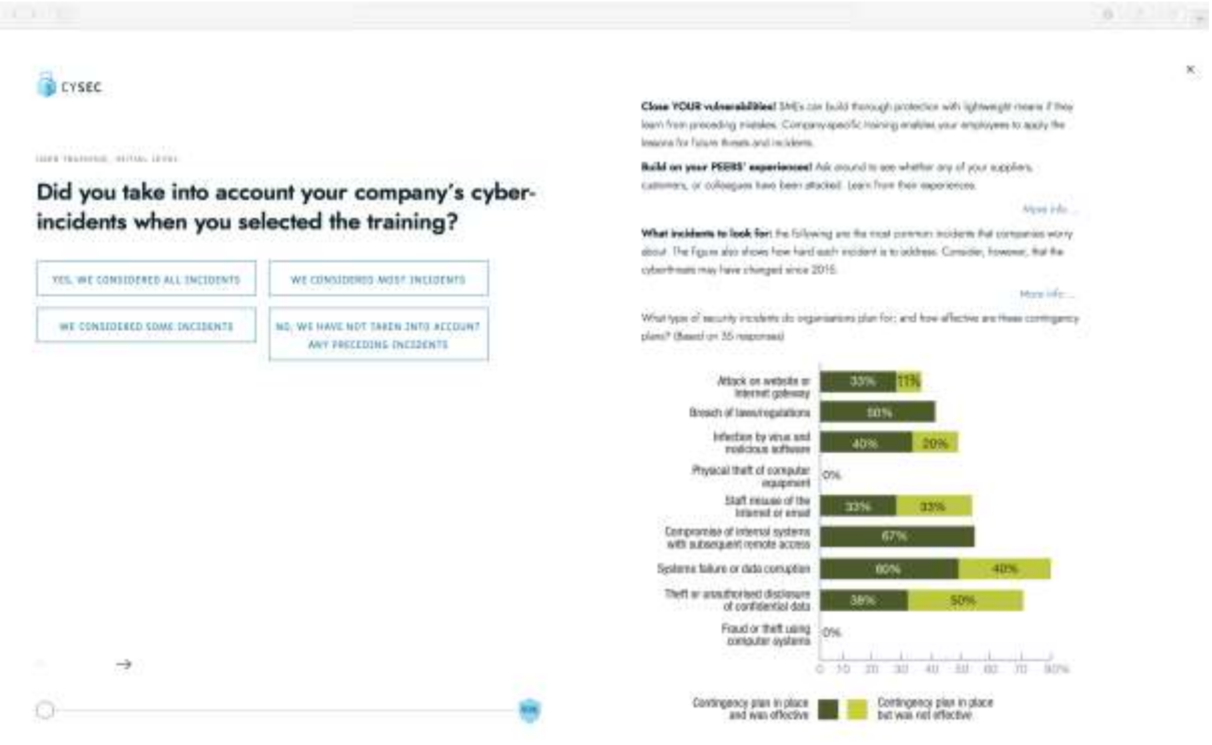
Consider different SMBs' cyber attacks trends in 2016 and 2017

3- More info …

Figure 7: Low-Fi prototypes for preparing the contents of the CYSEC tool.

2.2.4 CYSEC content development step 3: XML specification

The development step 2 for a CYSEC capability area concerns the prototyping of the SME employee end user journey and how the questions, answers, recommendations, and training materials are offered. The XSD-based metamodel and an example of a compliant XML were described in the deliverable D3.5 The following screenshots show screens rendered by the CYSEC tool for the capability area user training.



CYSEC

USER TRAINING, INITIAL LEVEL

Did you take into account your company's cyber-incidents when you selected the training?

YES, WE CONSIDERED ALL INCIDENTS
WE CONSIDERED MOST INCIDENTS
WE CONSIDERED SOME INCIDENTS
NO, WE HAVE NOT TAKEN INTO ACCOUNT ANY PRECEDING INCIDENTS

Close YOUR vulnerabilities! SMEs can build thorough protection with lightweight means if they learn from preceding mistakes. Company-specific training enables your employees to apply the lessons for future threats and incidents.

Build on your PEERS' experiences! Ask around to see whether any of your suppliers, customers, or colleagues have been attacked. Learn from their experiences.

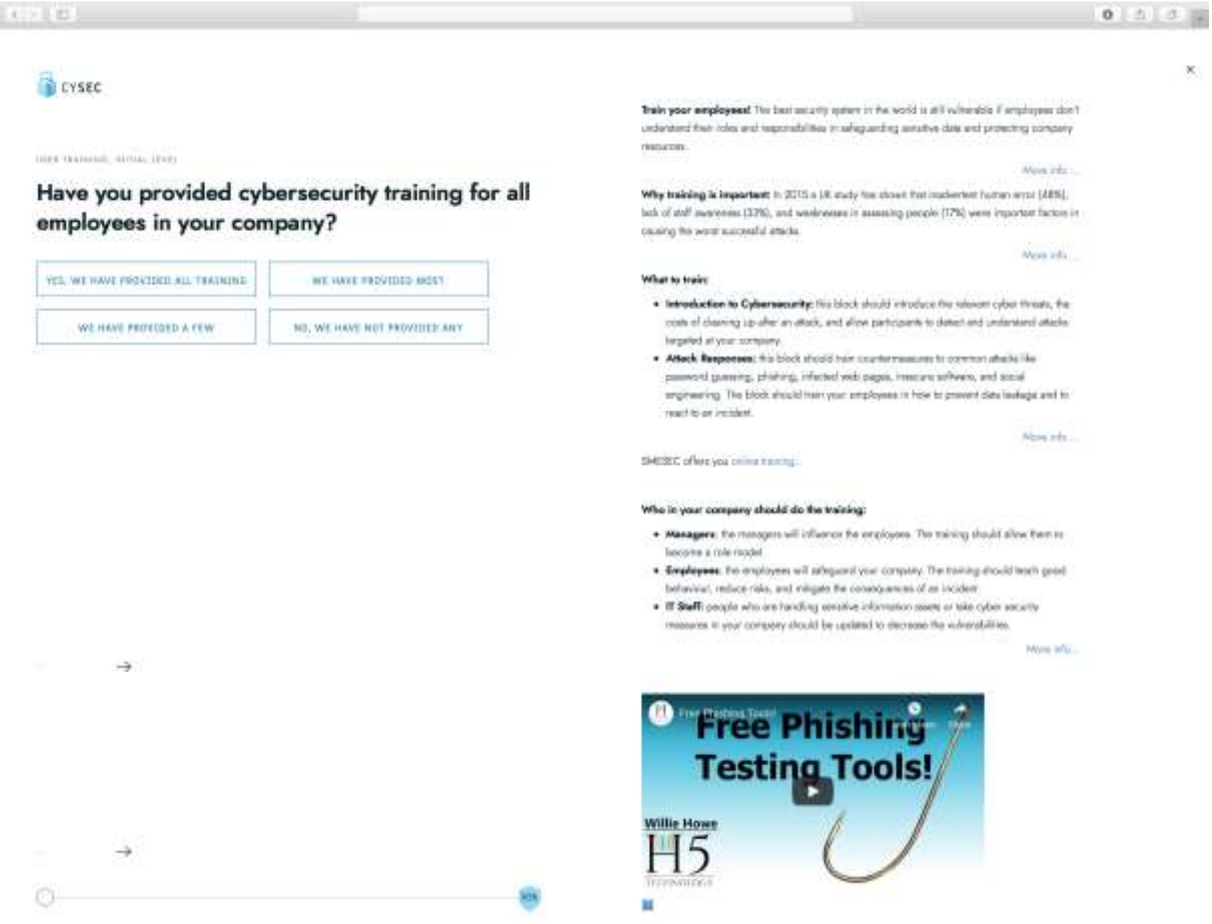
More info ...

What incidents to look for: the following are the most common incidents that companies worry about. The figure also shows how hard each incident is to address. Consider, however, that the cyberthreats may have changed since 2015.

More info ...

What type of security incidents do organisations plan for; and how affective are these contingency plans? (Based on 35 responses)

Attack on website or internet gateway
33%
11%
Breach of laws/regulations
50%
Infection by virus and malicious software
40%
20%
Physical theft of computer equipment
0%
Staff misuse of the internet or email
33%
33%
Compromise of internal systems with subsequent remote access
67%
Systems failure or data corruption
60%
40%
Theft or unauthorised disclosure of confidential data
38%
50%
Fraud or theft using computer systems
0%
0
10
20
30
40
50
60
70
80%
Contingency plan in place and was effective
Contingency plan in place but was not effective



CYSEC

USER TRAINING, INITIAL LEVEL

Have you provided cybersecurity training for all employees in your company?

YES, WE HAVE PROVIDED ALL TRAINING
WE HAVE PROVIDED MOST
WE HAVE PROVIDED A FEW
NO, WE HAVE NOT PROVIDED ANY

Train your employees! The best security system in the world is still vulnerable if employees don't understand their roles and responsibilities in safeguarding sensitive data and protecting company resources.

More info ...

Why training is important: In 2015 a UK study has shown that inadvertent human error (48%), lack of staff awareness (33%), and weaknesses in assessing people (17%) were important factors in causing the worst successful attacks.

More info ...

What to train:

- **Introduction to Cybersecurity:** this block should introduce the relevant cyber threats, the costs of cleaning up after an attack, and allow participants to detect and understand attacks targeted at your company.
- **Attack Responses:** this block should train countermeasures to common attacks like password guessing, phishing, infected web pages, insecure software, and social engineering. The block should train your employees in how to prevent data leakage and to react to an incident.

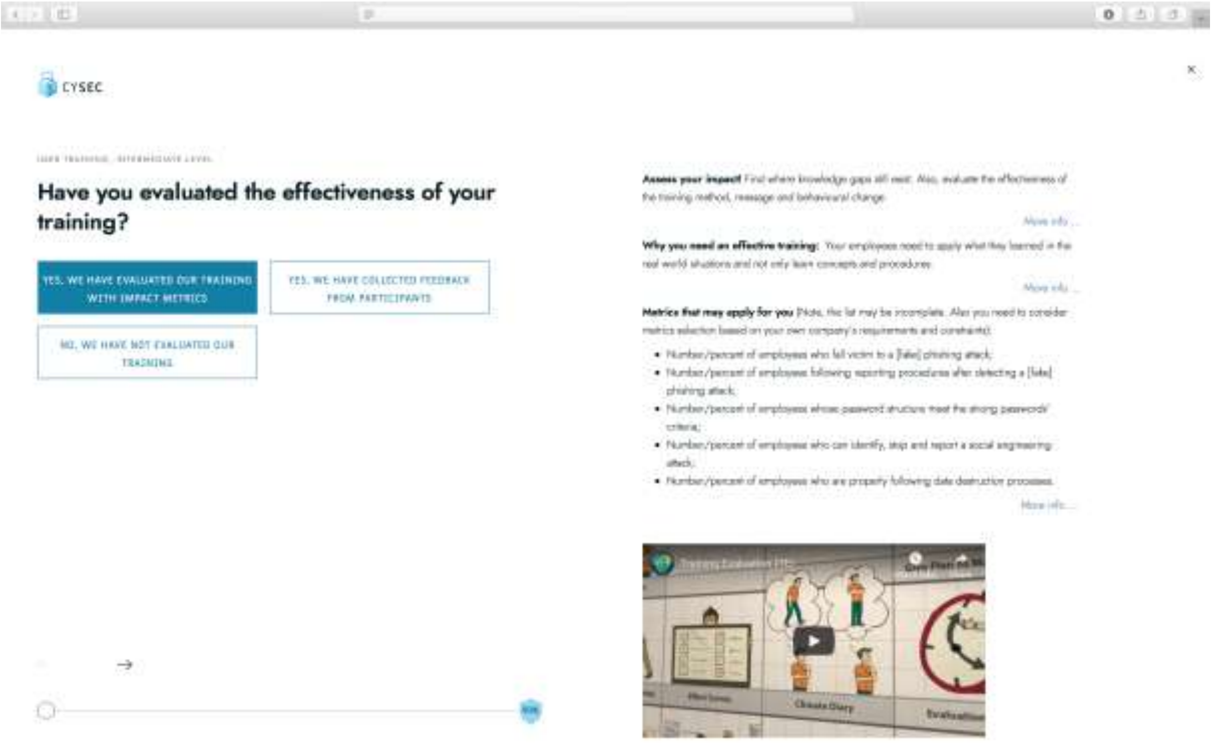
More info ...

SMESEC offers you online training...

Who in your company should do the training:

- **Managers:** the managers will influence the employees. The training should allow them to become a role model.
- **Employees:** the employees will safeguard your company. The training should teach good behaviour, reduce risks, and mitigate the consequences of an incident.
- **IT Staff:** people who are handling sensitive information assets or take cyber security measures in your company should be updated to decrease the vulnerabilities.

More info...


CYSEC
USER TRAINING · INTERMEDIATE LEVEL
YES, WE HAVE EVALUATED OUR TRAINING WITH IMPACT METRICS
YES, WE HAVE COLLECTED FEEDBACK FROM PARTICIPANTS
NO, WE HAVE NOT EVALUATED OUR TRAINING
More info ...
Training Evaluation (T...
Pilot Survey
Climate Diary
Evaluation

Have you evaluated the effectiveness of your training?

Assess your impact! Find where knowledge gaps still exist. Also, evaluate the effectiveness of the training method, message and behavioural change.

Why you need an effective training: Your employees need to apply what they learned in the real world situations and not only learn concepts and procedures.

Metrics that may apply for you (Note, the list may be incomplete. Also you need to consider metrics selection based on your own company's requirements and constraints):

- Number/percent of employees who fall victim to a [fake] phishing attack;
- Number/percent of employees following reporting procedures after detecting a [fake] phishing attack;
- Number/percent of employees whose password structure meet the strong passwords' criteria;
- Number/percent of employees who can identify, stop and report a social engineering attack;
- Number/percent of employees who are properly following data destruction processes.

Figure 8: Screens of the User Training capability area rendered by the CYSEC tool (note: some screens involve scrolling and could not be shown here completely.

2.2.5 CYSEC content development status

The development of the CYSEC content requires a systematic state-of-the-art mapping and validation through discussions with cybersecurity experts and feedback from the SMEs that use the content. Accordingly, the CYSEC content development is split over the duration of the SMESEC project with the following milestones:

- Start of SMESEC evaluation as part of the SMESEC open call: all fast ramp-up capability areas specified in XML and rendered by the CYSEC tool. All capability-building areas defined with scope and questions.
- End of the SMESEC project: all capability-building areas specified in XML and rendered by the CYSEC tool.

The following table shows the progress of the CYSEC content development at the moment of the submission of the deliverable D3.5.

Table 2: CYSEC content development status.

Capability area	Scope and Question Definition	Prototyping	XML-based Specification
Fast Ramp-Up			
User Training	Done	Done	Done
Access Control and Audit	Done	Done	Ongoing

Capability area	Scope and Question Definition	Prototyping	XML-based Specification
Patch Management	Done	Ongoing	In backlog
Malware Scans	Done	Ongoing	In backlog
Code Inspection	Done	Ongoing	In backlog
Capability-Building			
Absorption Networks	Ongoing	In backlog	In backlog
Network Controls	Ongoing	In backlog	In backlog
Intrusion Prevention	Ongoing	In backlog	In backlog
Credential Management	Ongoing	In backlog	In backlog
Second Opinion Defence	Ongoing	In backlog	In backlog
Security Engineering	Ongoing	In backlog	In backlog
Application Change Management	Ongoing	In backlog	In backlog
Compliance Audits	Ongoing	In backlog	In backlog
Standards Compliance	Ongoing	In backlog	In backlog

To validate the CYSEC contents, the scope, questions, and prototypes are discussed with cybersecurity experts drawn from the SMESEC consortium as well as from the open cybersecurity community. These discussions are held in physical and online webinar meetings performed as part of the tasks T3.3 and T6.2. The full implementation of CYSEC will be first validated with the SMESEC use case SMEs in the tasks T5.1-3 and secondly within the beta tests performed in conjunction with the SMESEC open call in the tasks T5.4-5. The respective results will be reported in deliverables D3.6, D5.1-3, D5.4-5, and D6.3-4.

3 Increasing SME awareness in security

3.1 Reaching overall SMEs community

As explained in Chapter 1, we are carrying out combined actions to reach a maximum number of SMEs. To achieve this objective, we work together with **SMEs associations and Security National Authorities** which are also organising actions towards SMEs. At this moment, we have identified the following key associations:

At EU level:

- CYBERWATCHING https://www.cyberwatching.eu
- Digital SMEs https://www.digitalsme.eu/
- EU SMEs http://www.cea-pme.com
- EASME https://ec.europa.eu/easme/en
- COSME https://ec.europa.eu/easme/en/cosme

At National Level

- France: contact active with AFDEE (http://afdee.eu/)and recently ONTPE (https://ontpe.org/)
- Spain: contact established with ANPME
- Switzerland contact active with SKV
- Greece contacts in progress
- Netherlands contacts in progress
- Romania: contacts in progress
- Israel: contact in progress

Besides, we have already organised a webinar with Cyberwatching (see 3.2.1) and we have ongoing discussions with these organisations for organising new webinars and workshops in 2019.

Authorities

At this moment, we have established contact with ANSSI (French National Agency for Information Security) for undertaking common actions (key meeting schedule December 19th).

ESOs: European Standardisation Organisations

Through activities in task 6.2 on standardisation, we are also touching SMEs such as at the ETSI security week even organised in June (https://www.etsi.org/news-events/events/1250-2018-06-security-week) . we are now in contact also with CEN-CENELEC (https://www.cencenelec.eu/standards/sectors/defencesecurityprivacy/security/pages/cybersecurity.aspx)and ETSI TC CYBER (https://www.etsi.org/technologies-clusters/technologies/cyber-security) for discussing SMESEC involvement to reach SMEs.

Combining forces with EU-funded GDPR related projects: GDPR is an important concern for SMEs . In this context, some EU projects have also the duty to interact with SMEs to help addressing GDPR implementation. For instance, we contacted the SMOOTH project (https://smoothplatform.eu/) This project has the objective to assist micro enterprises with GDPR adaptation, and we are already discussing synergies between SMOOTH and SMESEC on a combined effort to reach European SMEs.

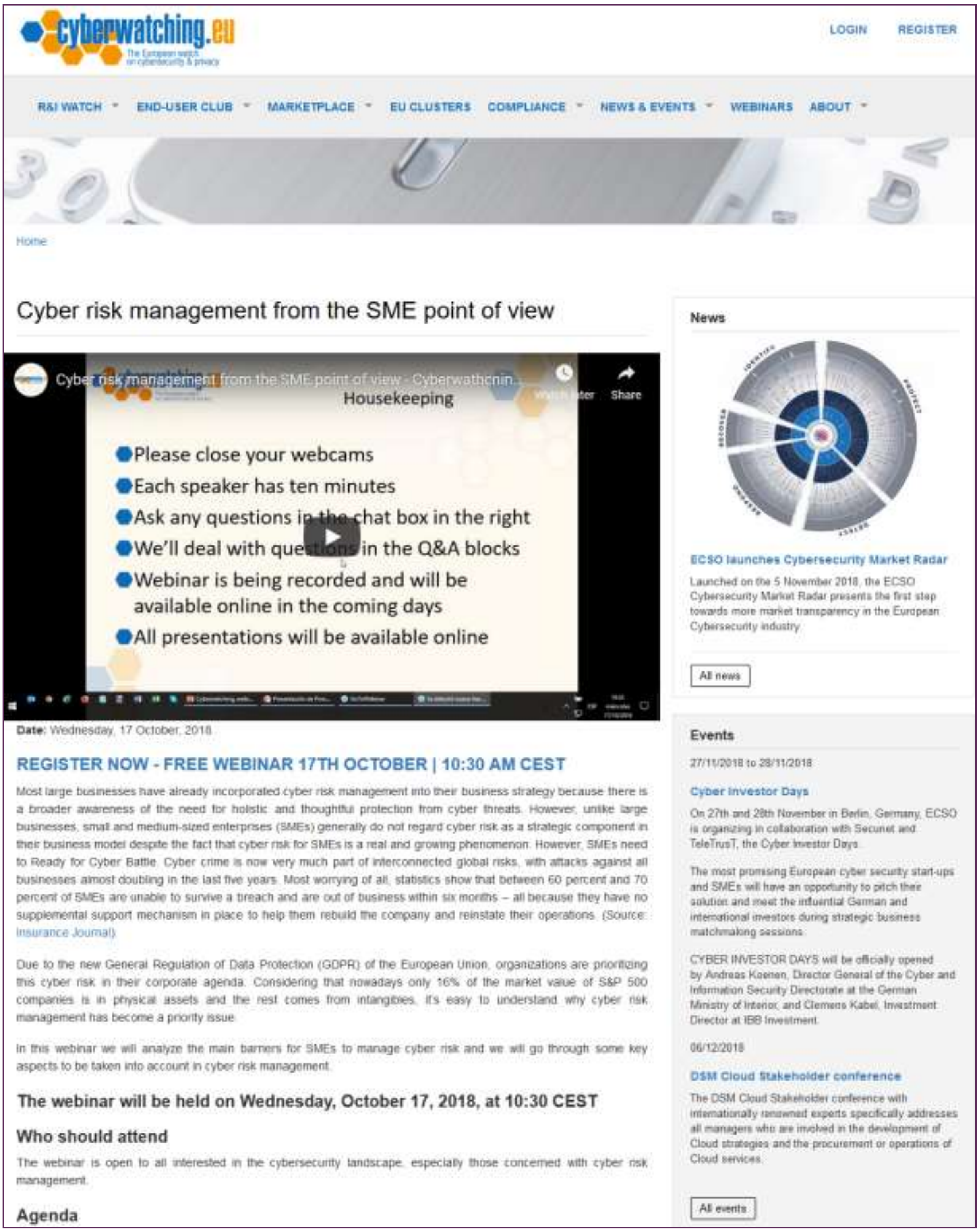
3.2 Campaigns for cyber threat awareness and interest in SMESEC

3.2.1 Setting up raising cyber threat awareness (Milestone Year 1)

The SMESEC consortium has cooperated with influencers at the European, national, and local levels to reach SME.

At the European level, SMESEC supports the campaigns of cyberwatching.eu, a European observatory of research and innovation in the field of cybersecurity and privacy. The following figure shows the homepage of the webinar that was performed with the support of SMESEC.[1]

[1] https://www.cyberwatching.eu/cyber-risk-management-sme-point-view



Cyber risk management from the SME point of view

Housekeeping

- Please close your webcams
- Each speaker has ten minutes
- Ask any questions in the chat box in the right
- We'll deal with questions in the Q&A blocks
- Webinar is being recorded and will be available online in the coming days
- All presentations will be available online

Date: Wednesday, 17 October, 2018

REGISTER NOW - FREE WEBINAR 17TH OCTOBER | 10:30 AM CEST

Most large businesses have already incorporated cyber risk management into their business strategy because there is a broader awareness of the need for holistic and thoughtful protection from cyber threats. However, unlike large businesses, small and medium-sized enterprises (SMEs) generally do not regard cyber risk as a strategic component in their business model despite the fact that cyber risk for SMEs is a real and growing phenomenon. However, SMEs need to Ready for Cyber Battle. Cyber crime is now very much part of interconnected global risks, with attacks against all businesses almost doubling in the last five years. Most worrying of all, statistics show that between 60 percent and 70 percent of SMEs are unable to survive a breach and are out of business within six months – all because they have no supplemental support mechanism in place to help them rebuild the company and reinstate their operations. (Source: Insurance Journal)

Due to the new General Regulation of Data Protection (GDPR) of the European Union, organizations are prioritizing this cyber risk in their corporate agenda. Considering that nowadays only 16% of the market value of S&P 500 companies is in physical assets and the rest comes from intangibles, it's easy to understand why cyber risk management has become a priority issue.

In this webinar we will analyze the main barriers for SMEs to manage cyber risk and we will go through some key aspects to be taken into account in cyber risk management.

The webinar will be held on Wednesday, October 17, 2018, at 10:30 CEST

Who should attend

The webinar is open to all interested in the cybersecurity landscape, especially those concerned with cyber risk management.

Agenda

News

ECSO launches Cybersecurity Market Radar

Launched on the 5 November 2018, the ECSO Cybersecurity Market Radar presents the first step towards more market transparency in the European Cybersecurity industry.

Events

27/11/2018 to 28/11/2018

Cyber Investor Days

On 27th and 28th November in Berlin, Germany, ECSO is organizing in collaboration with Secunet and TeleTrusT, the Cyber Investor Days.

The most promising European cyber security start-ups and SMEs will have an opportunity to pitch their solution and meet the influential German and international investors during strategic business matchmaking sessions.

CYBER INVESTOR DAYS will be officially opened by Andreas Koenen, Director General of the Cyber and Information Security Directorate at the German Ministry of Interior, and Clemens Kabel, Investment Director at IBB Investment.

06/12/2018

DSM Cloud Stakeholder conference

The DSM Cloud Stakeholder conference with internationally renowned experts specifically addresses all managers who are involved in the development of Cloud strategies and the procurement or operations of Cloud services.

Figure 9: Cyberwatching webinar page "Cyber risk management form the SME point of view."

Prof. Dr. Samuel Fricker offered an introduction to cybersecurity for SMEs and the main motivation to adopt the SMESEC solution. To conclude the webinar, the SMEs were encouraged to use a quick check tool to assess their maturity and as result, initiate the first improvement actions (see separate section in this deliverable, with the self-assessment questionnaire in 3.3.1).

The ETSI Security Week 2018, hosted in Sophia Antipolis, France from June 11th to 15th, was an event encompassing all parts of cybersecurity stakes gathering key experts, companies interested in contributing in standardization, policies, and solutions. It offered the opportunity to discuss the underlying cybersecurity challenges and resulting technical and standardization actions taken or needed to reach them.

Easy Global Market participated in the ETSI Security Week. On behalf of the SMESEC project, the team presented the main principles of the SMESEC cybersecurity framework dedicated to SMEs. The audience favorably welcomed the project approach during the poster session in the programming part entitled Security and Trust in ICT: The Value of Distributed Ledger Technology.

For SMESEC, the working conference offered the opportunity of networking, feedback, and discussion of the SMESEC framework with a leading standardization community.

More information: https://www.etsi.org/news-events/events/1250-2018-06-security-week

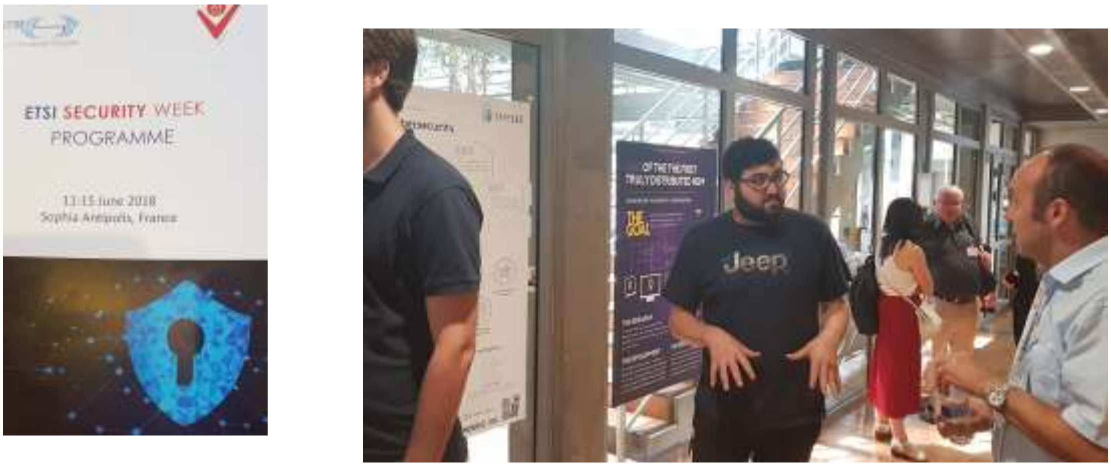


Figure 10: presence of SMESEC at ETSI Security week 2018

At the national level, SMESEC cooperates with influencers to encourage a public opinion that welcomes SMEs to become secure and makes the SMESEC initiative visible. SMESEC has started to be active in France, Spain, Greece and Switzerland. For example, in Switzerland, SMESEC cooperates with the Swiss Academy of Engineering Sciences, SATW, the most important network of experts for engineering sciences in the country[2]. SATW is in contact with the highest Swiss bodies for science, politics, and industry.

Coordinated by SATW, the Swiss population has been made aware of cyber threats for SMEs by raising the topic in top Swiss news, including the Tagesschau programme of the National television provider SRF (600'000 watchers) and newspapers. The following figure shows a screenshot of the Tagesschau contribution. The storyline concerned an SME that was experiencing a ransomware attack

[2] https://www.satw.ch/en/ueber-satw/the-satw/

that was initiated through fishing. The company succeeded to counter the attack with the help of a recent backup of their systems.

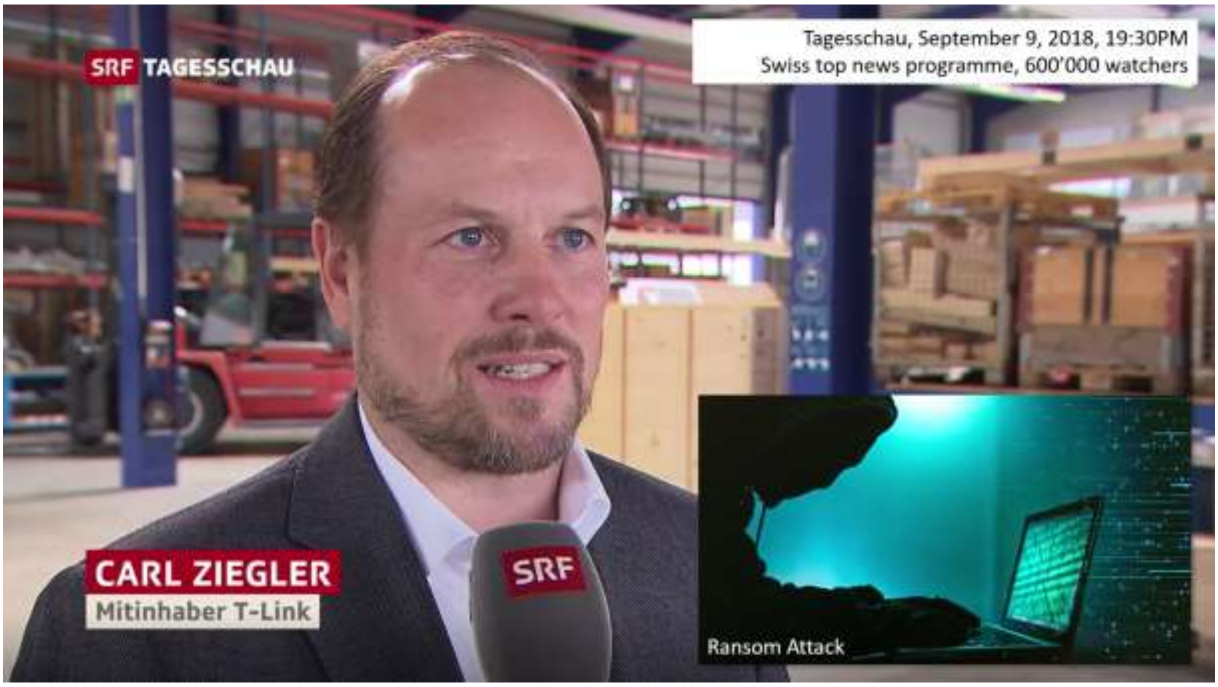
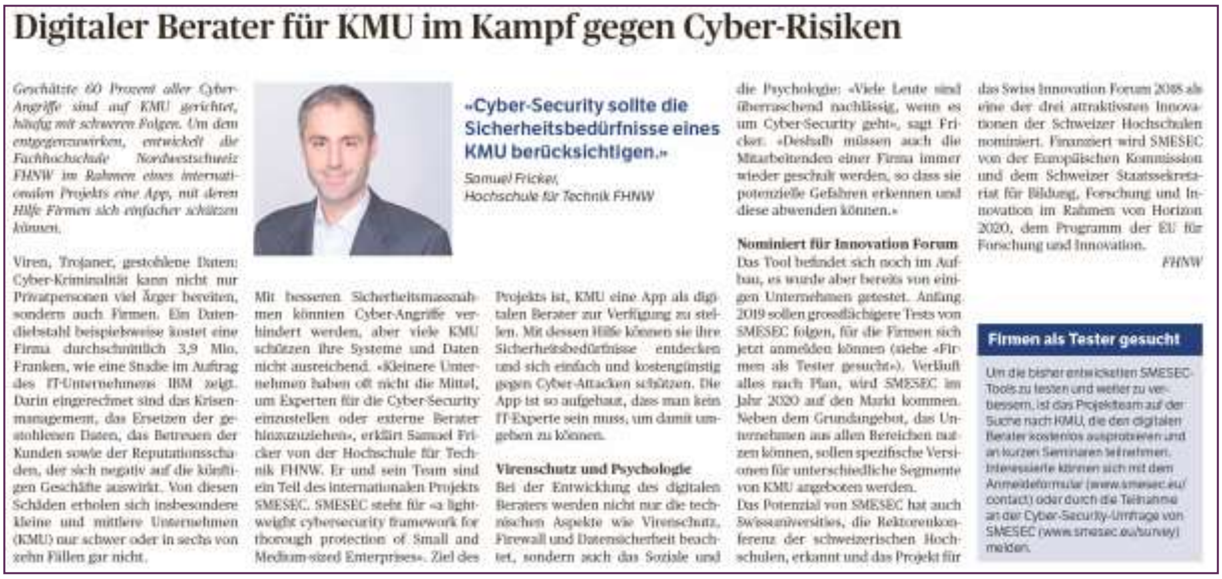

SRF TAGESSCHAU
Tagesschau, September 9, 2018, 19:30PM
Swiss top news programme, 600'000 watchers
CARL ZIEGLER
Mitinhaber T-Link
SRF
Ransom Attack

Figure 11: Owner of the SME T-Link telling his company's experience of cybersecurity in the leading Swiss news TV program.

The following figure shows an entry published by the leading newspapers in Northwestern Switzerland, addressing 550'000 newspaper readers. The storyline motivated SMESEC, described the CYSEC tool and its use for easy do-it-yourself cybersecurity improvement, and invited for cooperation, e.g. as part of the beta program that will be launched in 2019 with the SMESEC open call.



Digitaler Berater für KMU im Kampf gegen Cyber-Risiken

Geschätzte 60 Prozent aller Cyber-Angriffe sind auf KMU gerichtet, häufig mit schweren Folgen. Um dem entgegenzuwirken, entwickelt die Fachhochschule Nordwestschweiz FHNW im Rahmen eines internationalen Projekts eine App, mit deren Hilfe Firmen sich einfacher schützen können.

Viren, Trojaner, gestohlene Daten: Cyber-Kriminalität kann nicht nur Privatpersonen viel Ärger bereiten, sondern auch Firmen. Ein Datendiebstahl beispielsweise kostet eine Firma durchschnittlich 3,9 Mio. Franken, wie eine Studie im Auftrag des IT-Unternehmens IBM zeigt. Darin eingerechnet sind das Krisenmanagement, das Ersetzen der gestohlenen Daten, das Betreuen der Kunden sowie der Reputationsschaden, der sich negativ auf die künftigen Geschäfte auswirkt. Von diesen Schäden erholen sich insbesondere kleine und mittlere Unternehmen (KMU) nur schwer oder in sechs von zehn Fällen gar nicht.

«Cyber-Security sollte die Sicherheitsbedürfnisse eines KMU berücksichtigen.»

Samuel Fricker, Hochschule für Technik FHNW

Mit besseren Sicherheitsmassnahmen könnten Cyber-Angriffe verhindert werden, aber viele KMU schützen ihre Systeme und Daten nicht ausreichend. «Kleinere Unternehmen haben oft nicht die Mittel, um Experten für die Cyber-Security einzustellen oder externe Berater hinzuzuziehen», erklärt Samuel Fricker von der Hochschule für Technik FHNW. Er und sein Team sind ein Teil des internationalen Projekts SMESEC. SMESEC steht für «a lightweight cybersecurity framework for thorough protection of Small and Medium-sized Enterprises». Ziel des Projekts ist, KMU eine App als digitalen Berater zur Verfügung zu stellen. Mit dessen Hilfe können sie ihre Sicherheitsbedürfnisse entdecken und sich einfach und kostengünstig gegen Cyber-Attacken schützen. Die App ist so aufgebaut, dass man kein IT-Experte sein muss, um damit umgeben zu können.

Virenschutz und Psychologie

Bei der Entwicklung des digitalen Beraters werden nicht nur die technischen Aspekte wie Virenschutz, Firewall und Datensicherheit beachtet, sondern auch das Soziale und die Psychologie: «Viele Leute sind überraschend nachlässig, wenn es um Cyber-Security geht», sagt Fricker. «Deshalb müssen auch die Mitarbeitenden einer Firma immer wieder geschult werden, so dass sie potenzielle Gefahren erkennen und diese abwenden können.»

Nominiert für Innovation Forum

Das Tool befindet sich noch im Aufbau, es wurde aber bereits von einigen Unternehmen getestet. Anfang 2019 sollen grossflächigere Tests von SMESEC folgen, für die Firmen sich jetzt anmelden können (siehe «Firmen als Tester gesucht»). Verläuft alles nach Plan, wird SMESEC im Jahr 2020 auf den Markt kommen. Neben dem Grundangebot, das Unternehmen aus allen Bereichen nutzen können, sollen spezifische Versionen für unterschiedliche Segmente von KMU angeboten werden.

Das Potenzial von SMESEC hat auch Swissuniversities, die Rektorenkonferenz der schweizerischen Hochschulen, erkannt und das Projekt für das Swiss Innovation Forum 2018 als eine der drei attraktivsten Innovationen der Schweizer Hochschulen nominiert. Finanziert wird SMESEC von der Europäischen Kommission und dem Schweizer Staatssekretariat für Bildung, Forschung und Innovation im Rahmen von Horizon 2020, dem Programm der EU für Forschung und Innovation.

FHNW

Firmen als Tester gesucht

Um die bisher entwickelten SMESEC-Tools zu testen und weiter zu verbessern, ist das Projektteam auf der Suche nach KMU, die den digitalen Berater kostenlos ausprobieren und an kurzen Seminaren teilnehmen. Interessierte können sich mit dem Anmeldeformular (www.smesec.eu/contact) oder durch die Teilnahme an der Cyber-Security-Umfrage von SMESEC (www.smesec.eu/survey) melden.

Figure 12: Raising awareness of cyber risks and information about the SMESEC project in the leading newspaper Aargauer Zeitung.

The impact of these media campaigns was visible through proactive contact that was initiated by professionals and companies seeking to a differentiated business value in fostering cybersecurity for SMEs. Especially, the newspaper article in the Aargauer Zeitung generated contacts with local networkers and the SME community managers that were interested in helping to spread SMESEC to SMEs.

Communication activities with SMEs and SME associations in Spain

The work for communicating with SMEs and associations in Spain was done early in the project in order to start creating contacts as soon as possible and identify with them joint opportunities.

In this section we describe, on the one hand, the identified activities that we aim to fulfill with the SMEs and associations and, on the other hand, the initial list of associations Spain we have contacted in Spain and initial joint work we plan to do.

Activities to be performed with SMEs

The activities that were identified aimed to both increase the impact of SMESEC and to have initial feedback that could be used in the technical, dissemination and exploitation areas. Following, we describe an initial list of activities we plan to perform with SMEs and associations:

- List of cybersecurity needs, constraints and status of SMEs: although we already identified needs using the expertise and knowledge of the use cases of the project, we wanted to expand this information with as much feedback as possible. This information was not only about technical requirements but also from the day-to-day business point of view. For example, knowing the economic limitations of different types of companies (based in their market preferences or size) could allow us to better plan the exploitation strategy of SMESEC. Also, it is very useful for us to know the type of cybersecurity solutions used by each company according to their business and cybersecurity requirements.
- Cybersecurity expertise and knowledge of SMEs: in order to provide a robust solution, we also wanted to know what is the normal situation of cybersecurity expertise and resources in SMEs. We prepared an initial questionnaire about cybersecurity awareness that was shared with external organizations and users in order to have an initial idea of their situation. We have developed now a second one, with more information, that will guide us further on how to continue working in SMESEC from the points of view of technical implementation, usability, user-friendly, information provided, etc.
- Interest for adopting a different solution and why: for SMESEC it is important not only to create a robust, and usable solution but also to facilitate SMEs to adopt it. We are aware when an organization uses an application it is difficult for them to move to a new one (technical integration, training of personnel, etc.) so it is very interesting for us to know how we could make any SME adopt our solution. This way we will guide the technical development and business orientation in order to increase the adoption of our approach.
- Participation for the open call: the open call of SMESEC aims to allow several external SMEs of the project to integrate, use, test and evaluate our approach. For this reason, the bigger the number of SMEs involved in the open call the more diversity of types of business, size, area of expertise, countries, cybersecurity needs, possible collaborations, etc. Therefore, we think we have to start contacting SMEs and associations in order to increase the list of contacts as soon as possible and make it grow with additional networking we do.

- Dissemination of the activities of the project: along the lifecycle of the project we plan to organize different activities: advisory board meetings, workshops, technical presentations, participate in webinars and presentations, etc. This way, it is important to have a large number of contacts for increasing the impact of the project, make them aware of the updates and possibilities of our approach, do networking with them for increasing the reach of the project in more areas or type of business, etc.
- Business plan of SMESEC: as abovementioned, we think having feedback of SMEs about their business opportunities and constraints would allow us to better refine the final business plan of our approach. This is planned to be done in several iterations after designing a mature version of the project and their business needs.

Spanish SME associations

As we described before, we have identified an initial list of Spanish SME associations that we have contacted and have shown interest in collaborating with SMESEC. This list is a living one and we plan to increase it as the project evolves and we have more outputs to present. Finally, we would like to mention that together with these associations we are also contacting individual SMEs. Following we present the more important Spanish organizations we have contacted:

- AEI Ciberseguridad [1] (Agrupación Empresarial Innovadora Ciberseguridad): the Spanish cybersecurity innovation cluster is composed of organizations of different type: industry, universities, research centers, etc. It has more than 80 organizations of the public and private sector. Any organization with the aim of promoting new technologies at industry or research level is welcome to join and participate in the activities. The cluster is supported by the Spanish National Cyber Security Institute (INCIBE), providing operational support to any company interested in the promotion and development of business technology areas. The organization has a special focus in SMEs and communicates directly with that area in the Ministry of Industry. The initial contact with this partner has been satisfactory and we are looking forward for involving them in the work with SMEs in Spain. We already participated together in the Cybersec 2018 (Krakov, Poland) discussing in a workshop about how to support SMEs in cybersecurity.
- CITIC [2] (Centro Andaluz de Innovación y Tecnologías de la Información y las Comunicaciones): this institution focuses in the research, development and innovatoin of ICT technologies and acting as a bridge for providing them to public and private organizations. They work mainly with organizations from Andalucia (south of Spain), and are in charge of the organization cluster of cybersecurity chapter. Among a long list of activities for closing the gap between innovation and industry they organize cybersecurity workshops for start-ups and SMEs, joint conferences with other chapters of Spain for sharing knowledge, networking with other organizations, etc. Our initial contact with them has been very positive and we plan to participate with them in a workshop of cybersecurity for SMEs where we can present our approach and solutions.
- PLANETIC [3] (Plataforma Tecnológica Española para la Adopción y Difusión de las Tecnologias Electrónicas, de la Información y la Comunicación): the main objective of this cluster (Spanish platform for the adoption and dissemination of ICT) is to promote the dissemination and adoption of ICT. For this objective they have different groups for academy, research institutions and industry and work in various areas of application: energy, IoT, smart cities, etc. This way, we think it will be a good addition in order to reach more sectors and types of SMEs.

- PESI [4] (Plataforma Tecnológica Española de Seguridad Industrial): this platform (Spanish platform of cybersecurity for industry) is an organization led by industry and with the main goa lof involve organizations, research centers, and universities of european and national level focusing in cybersecurity for industry. The partners of the platform are able to work together with other agencies of cybersecurity, participate in research projects, promote cybersecurity for industry, etc. This organization contains both large industry and SMEs so we will focus in this area as the members are always open to use and adopt new cybersecurity solutions.

In Poland Gridpocket.S.A has worked dynamically on creating cybersecurity awareness among SME's in our country. They attended meetings and conferences, also informed our followers via our social media. We also posted an article in 'New Energy' Monthly, where we described SMESEC project. This year Gridpocket's chairman, Jerzy Gluszak attended the cybersecurity conference in Kazimierz (PL), where he presented ideas and targets of the SMESEC. Also, last week all our polish team attended IT meeting, 'SparkCamp', where mr. Jerzy also presented the SMESEC framework. I am attaching the illustrative screenshot of our LinkedIn posts.

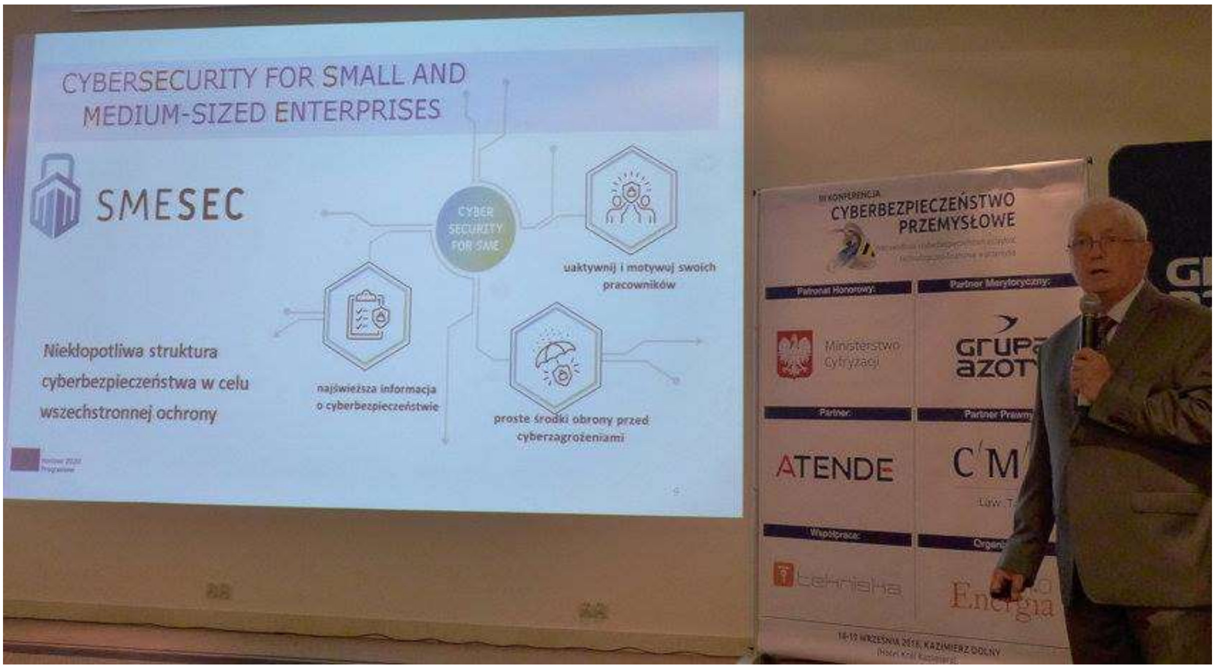

CYBERSECURITY FOR SMALL AND MEDIUM-SIZED ENTERPRISES
SMESEC
CYBER SECURITY FOR SME
uaktywnij i motywuj swoich pracowników
Niekłopotliwa struktura cyberbezpieczeństwa w celu wszechstronnej ochrony
najświeższa informacja o cyberbezpieczeństwie
proste środki obrony przed cyberzagrożeniami
CYBERBEZPIECZEŃSTWO PRZEMYSŁOWE
Patronat Honorowy:
Partner Merytoryczny:
Ministerstwo Cyfryzacji
Grupa Azoty
Partner:
ATENDE
Współpraca:
Energia

Figure 13: presentation at Smart Camp, Poland conference on Reliablility, cybersecurity and technological-financial continuity in industry". 18-19 September 2018

At the local/regional level, SMESEC has started to cooperate with local networkers and SMEs associations. These latter have given the opportunities to meet with SMEs, get to know them, and discuss about cyber threats and how to address them. As an example, one of these local networkers is a senior lawyer who offers seminars in cybersecurity for SMEs and suggested to include SMESEC concept in his courses. Another example is set by insurance companies which offer seminars on cybersecurity for SMEs and are testing protection for cyber threats as a product. Examples of local

SMEs associations are the Swiss Association of SMEs “SKV”[3] and the SMEs Region Brugg “KMUREGIONBRUGG”[4]. The national organization SKV is organizing a series of entrepreneur meetings in different Swiss regions that allow SMEs to present themselves and get introduced to each other. SMEs Region Brugg is an example of an organization that performs meetings series at just one location.

In France, SMESEC has interacted with the national Secure Communication Cluster (Pole SCS, https://www.pole-scs.org/en/). SCS is a world-class competitiveness cluster dedicated to digital technologies.

Created in 2005 in the Provence Alpes Côte d’Azur region in the South of France, it brings together an ecosystem of more than 300 industrial players, large multi-national groups, **SMEs and startups,** research laboratories and leading universities in their fields. They are working together to develop and market products and innovative services with the aim to generate growth and jobs in high growth markets.

SCS WORLD-CLASS CLUSTER

A LEADING EUROPEAN ECOSYSTEM

IN SECURITY & DIGITAL IDENTITIES TECHNOLOGIES, MOBILE NETWORKS AND SERVICES, IOT AND CONTACTLESS

SCS cluster already forwarded SMESEC questionnaire to their members and they are ready to help in further actions. In particular, the French security authorities ANSSI asked them to help organising actions toward SMEs and SCS cluster put us in contact with ANSSI for discussions on common actions.

3.3 Meeting the SMEs

We have met SMEs in many contexts: in particular, through participation to events (see Dissemination report in D6.2). However, we were also pro-active to meet face2face SMEs in having booth at the key events.

To meet SMEs, FHNW and EGM have been participating at large-scale events that offered visibility across Europe and small-scale events that allowed connecting with the locally oriented SMEs.

The largest event was the IoT Solutions World Congress[5] that took place on October 29-31 in Barcelona. SMESEC was present with a booth offering talks about cybersecurity for SMEs (Prof. Dr. Samuel Fricker) and allowed spreading information about the SMESEC offering. The congress recorded 16’250 visitors with many SMEs being present. The following figure illustrates the SMESEC presence.

[3] http://www.kmuverband.ch/unternehmertreffen.html

[4] http://www.kmuregionbrugg.ch/

[5] https://www.iotsworldcongress.com/

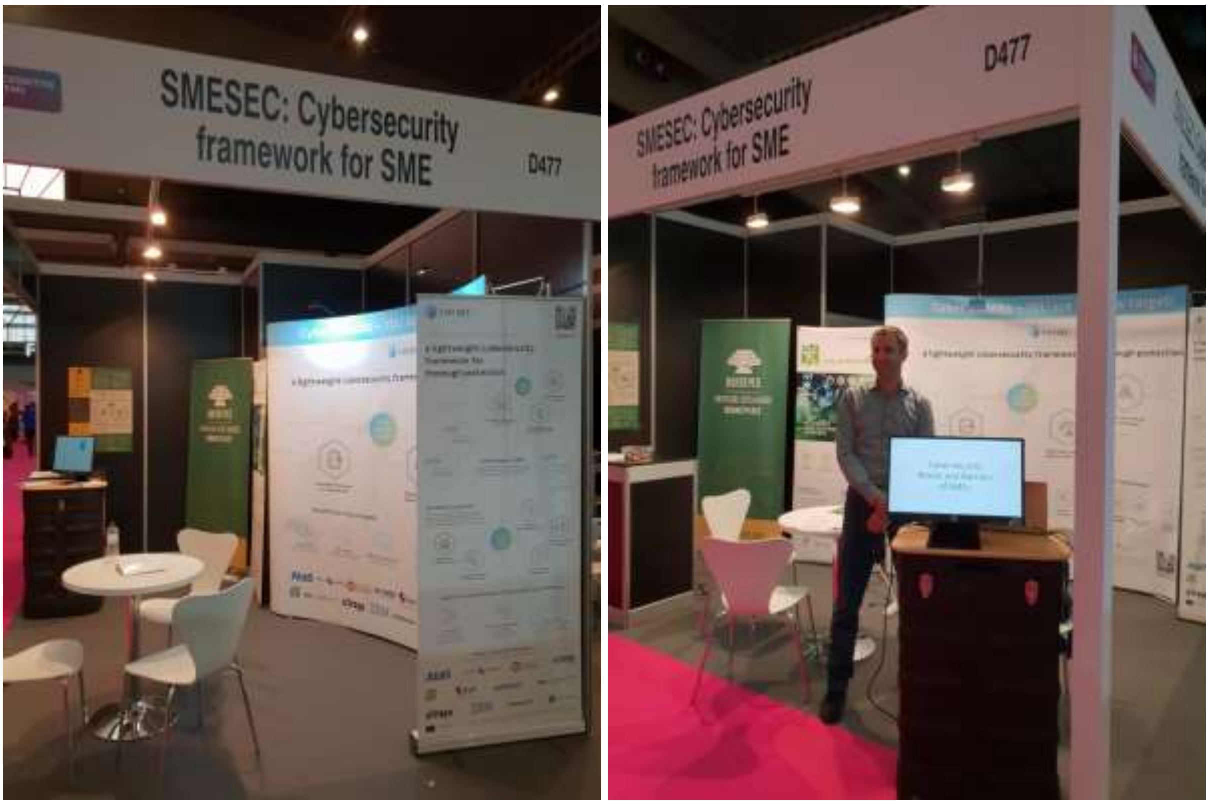

SMESEC: Cybersecurity framework for SME
D477
SMESEC: Cybersecurity framework for SME
D477

Figure 14: Booth at IoT Solutions World congress (left) and talk about cybersecurity for SME (right).

As result of the presence, there were many discussions with SMEs that visited the congress or were present themselves with a booth. The most significant ones were discussions with people who experienced cyberattacks and leaders of local networks offering access to the SME communities.

An example of an interaction with local SMEs is the SKV entrepreneur meeting visited in Winterthur on August 30th 2018[6]. The figure below shows the venue of that meeting. SMESEC was present with a booth. There, cybersecurity aspects were discussed with the present local SMEs. The SKV meetings are organized since 2006 and are held in various regions in Switzerland, such as in the cantons of Basel, Zug, and Zurich. The meetings of the KMU Region Brugg usually take place at FHNW.

Figure 15: Local SME event organized by SKV in Winterthur, Switzerland.

[6] http://www.kmuverband.ch/unternehmertreffen.html

The result of the presence in the local SMEs events is an in-depth understanding of the SMEs, their business models, the degree of maturity in cybersecurity, and their reasons for adoption or non-adoption of cybersecurity tools. The local SME events visited so far, showed a broad diversity of SMEs at European level. Some of these SMEs were successful companies, operated in the IT domain, and showed in-depth understanding and good practice of cybersecurity aspects. Other SMEs directly fight for their survival, struggled with IT issues, and they have heard about cybersecurity, but in general they do not implement cybersecurity practices or have misconceptions about basic concepts. A big difference was also observed between small and medium-sized companies. The medium-sized ones usually organize their activity between IT and business parts and have a clear definition of the responsibility for cybersecurity aspects.

A third type of events covered by the SMESEC project was the industry event “Swiss Innovation Forum” (SIF), which took place on November 22nd 2018 in Basel, Switzerland[7]. The figure below shows the booth of SMESEC at SIF. A next such event is the European ICT-2018 conference[8], which took place on December 4-6 in Vienna, Austria.

07
SMESEC
Cybersecurity für KMU
SMESEC
a lightweight cybersecurity framework for thorough protection
Atos
CITRIX
IBM

Figure 16: Innovation-oriented fair.

The participation at the event allowed meeting people and organizations that are interested in innovation. For SMESEC, these meetings allowed identifying themes related to the project, such as cyber threat monitoring, certification, and insurance, establishing links for cooperation within the SMESEC open call or beyond.

Meeting SMEs at Key security event, Monaco October 9th 2018

[7] https://www.swiss-innovation.com/

[8] https://ec.europa.eu/digital-single-market/en/events/ict-2018-imagine-digital-connect-europe

135 representatives of SMEs located in the French Riviera participated at the Sophia Security Camp on October 9th 2018 to understand the operating modes of hackers and data security techniques. The contents were presented by various experts in cybersecurity including SMESEC.

On the eve of the 18th edition of the “Assises de la Sécurité” in Monaco and in this European month of cybersecurity, Telecom Valley and its partners (CCI Nice Côte d'Azur, ANSSI, Clusir Côte d'Azur and the Gendarmerie Alpes-Maritimes) have also organised the event at Inria Sophia-Antipolis campus.

Formerly less concerned than large firms, French SMEs are now plagued by acts of cybercrime, a scenario that can seriously damage their businesses.

Organized in two phases, Sophia Security Camp began with a workshop "Hacking Lab" led by the cybersecurity expert Marc Arnaert, followed by the Chief Warrant Officer Barré and the adjutant Citérin of the Economic Intelligence section of the Gendarmerie of the Alps -Maritimes. All three slipped the participants into the shoes of a hacker, then into a team of forensic investigators, to illustrate and understand the mechanisms of a cyber-attack and the management of digital crime scenes.

The event continued during a conference focused on data security technologies and cyber-malice protection devices available to SMEs:

- **Frédérik Aouizerats**, lead architect VMWare at IBM, presented an overview of the security of cloud solutions based on "VMWARE" technologies,
- **Abbas Ahmad** Engineer at Easy Global Market, presented **SMESC**, a European Cybersecurity Toolkit dedicated to SMEs,
- **Patrick Chambet**, RSSI of Nice Côte d'Azur Metropolis and representative of Clusir Côte d'Azur, showed multiple examples of cybersecurity risks related to connected objects scattered throughout a city of the future,
- **Cédric Vamour**, Cyber Security Architect at Renault Software Labs, made the link with the previous presentation by showing a specific application for the autonomous vehicle,
- **Marjorie Billaud**, Economic Intelligence Advisor at the Nice Côte d'Azur CCI and Moise Moyal, Regional Delegate of ANSSI, presented a reminder of the European Data Protection Regulation and its "data security" aspect,
- Finally, **Moise Moyal** concluded the evening with a presentation of the national system of assistance to the victims of cyber malice acts "Cybermalveillance.gouv.fr".

Figure 17 : Easy Global Market, presenting SMESEC at the Sophia Security Camp

The representatives of the SMEs present in the event exchanged points of view and concerns long after the conference. Edmond Cissé (Uraeus Consult), host of the day and co-host with Lionel Faure (TAS Group) of the Telecom Valley Safety & Cloud community, will meet them all year long to continue sharing on the themes of security and cloud management.

3.3.1 Pursuing raising interest in SMESEC (Milestone Year 2)

For raising awareness of cyber threats and generating interest in SMESEC, FHNW has been developing a quick check instrument for SMEs. The quick check can be printed on one double-paged A4 paper and handed out to SMEs. It provides the SME employee responsible for cybersecurity to check the SME's cybersecurity practices in 10 capability areas with three yes/no/don't know questions. In just about 10 minutes, the employee can calculate a score indicating how mature the SME is.

The quick check questionnaire offers the following elements. It raises the awareness question of "how well is your company protected against cyber-attacks?" and invites the respondent to check immediately whether they meet minimum standards for small and medium-sized companies. It covers the topics of task, powers, and responsibilities, awareness, data protection, backups, password and user administration, malware protection, updates, secure communication, software and device development, and emergency response.

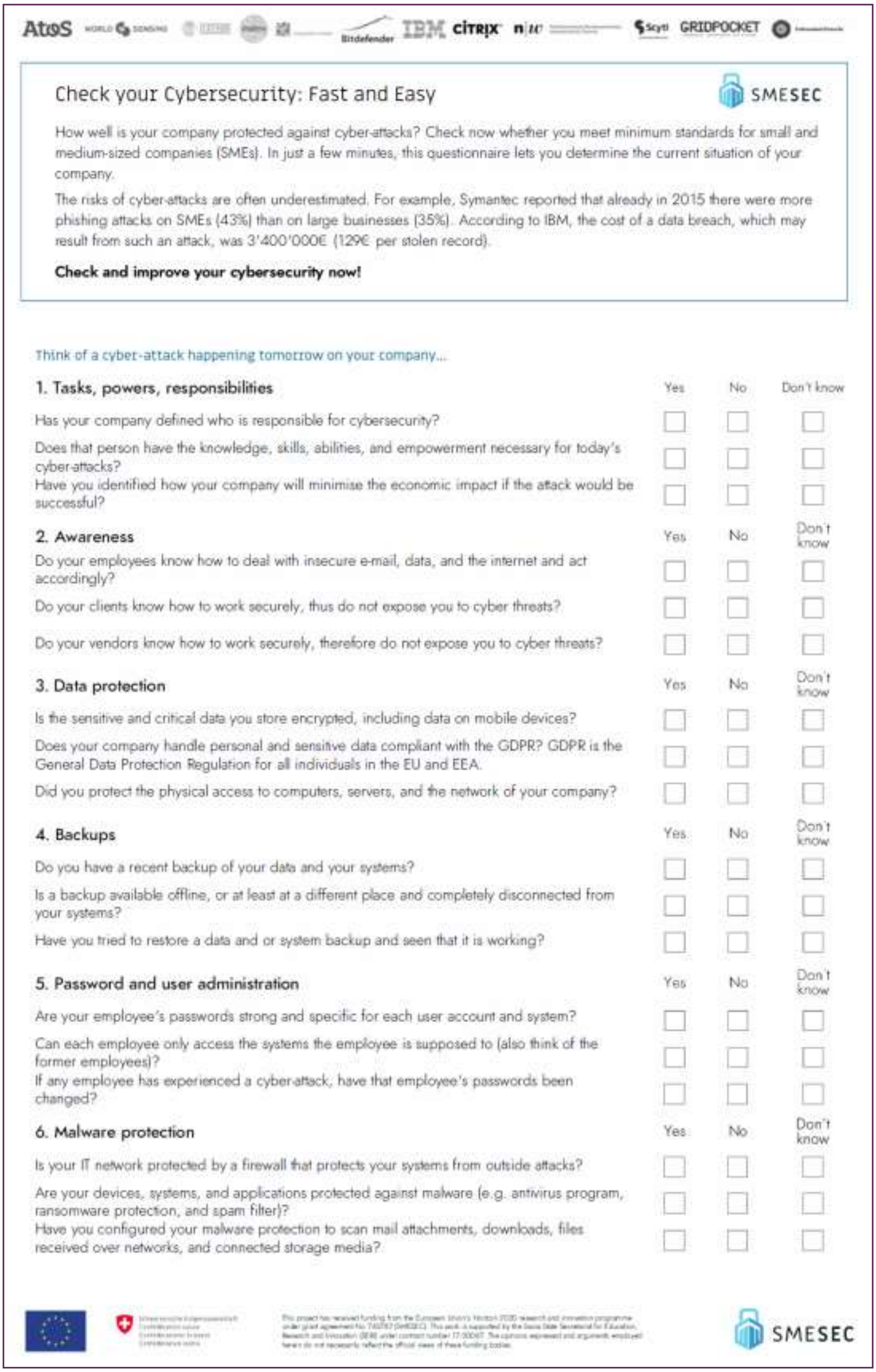
The definition of that standard is based on campaigns from peer organizations, such as the Swiss satw and SwissICT organizations, that has been adapted to meet the SMESEC values and completed to address all-over-the cybersecurity concerns. For example, SMESEC does not assume that an SME would be able to define guidelines and baselines for cybersecurity themselves but takes a proactive approach of proposing concrete recommendations that allow easy do-it-yourself cybersecurity capability developments. Also, SMESEC supports a diversity of SME business models, such as the development of software or devices that need to be protected.

The quick check questionnaire contains questions that encourage a snowballing approach of talking about SMESEC. The questions "Do your clients know how to work securely, thus do not expose you to cyber threats?" and "Do your vendors know how to work securely, therefore do not expose you to cyber threats?" encourage discussion about cybersecurity within the company's supply network and spread the word about SMESEC, e.g. by forwarding the quick check questionnaire.

The quick check questionnaire offers guidance and support for the SME. It provides the SME with the ability to calculate the number of YES answers and encourages the following actions:

- 0-9 points (out of 30 points): identify the questions that would be easy to turn to a YES, hence immediately work on improving cybersecurity.
- 10-23 points (out of 30 points): share their contact information with the SMESEC consortium and register for a newsletter that regularly reminds them about cybersecurity and offers a way to know about SMESEC.EU.
- 24-29 points (out of 30 points): share their contact information with the SMESEC consortium and register their interest for the SMESEC beta program that will be launched with the open call.
- 30 points (out of 30 points): share their contact information with the SMESEC consortium and indicate that they are so mature that they are an interesting candidate to share lessons-learned with other SMEs.

The following figure shows the questionnaire.



Check your Cybersecurity: Fast and Easy

How well is your company protected against cyber-attacks? Check now whether you meet minimum standards for small and medium-sized companies (SMEs). In just a few minutes, this questionnaire lets you determine the current situation of your company.

The risks of cyber-attacks are often underestimated. For example, Symantec reported that already in 2015 there were more phishing attacks on SMEs (43%) than on large businesses (35%). According to IBM, the cost of a data breach, which may result from such an attack, was 3'400'000€ (129€ per stolen record).

Check and improve your cybersecurity now!

Think of a cyber-attack happening tomorrow on your company...

1. Tasks, powers, responsibilities	Yes	No	Don't know
Has your company defined who is responsible for cybersecurity?	□	□	□
Does that person have the knowledge, skills, abilities, and empowerment necessary for today's cyber-attacks?	□	□	□
Have you identified how your company will minimise the economic impact if the attack would be successful?	□	□	□

2. Awareness	Yes	No	Don't know
Do your employees know how to deal with insecure e-mail, data, and the internet and act accordingly?	□	□	□
Do your clients know how to work securely, thus do not expose you to cyber threats?	□	□	□
Do your vendors know how to work securely, therefore do not expose you to cyber threats?	□	□	□

3. Data protection	Yes	No	Don't know
Is the sensitive and critical data you store encrypted, including data on mobile devices?	□	□	□
Does your company handle personal and sensitive data compliant with the GDPR? GDPR is the General Data Protection Regulation for all individuals in the EU and EEA.	□	□	□
Did you protect the physical access to computers, servers, and the network of your company?	□	□	□

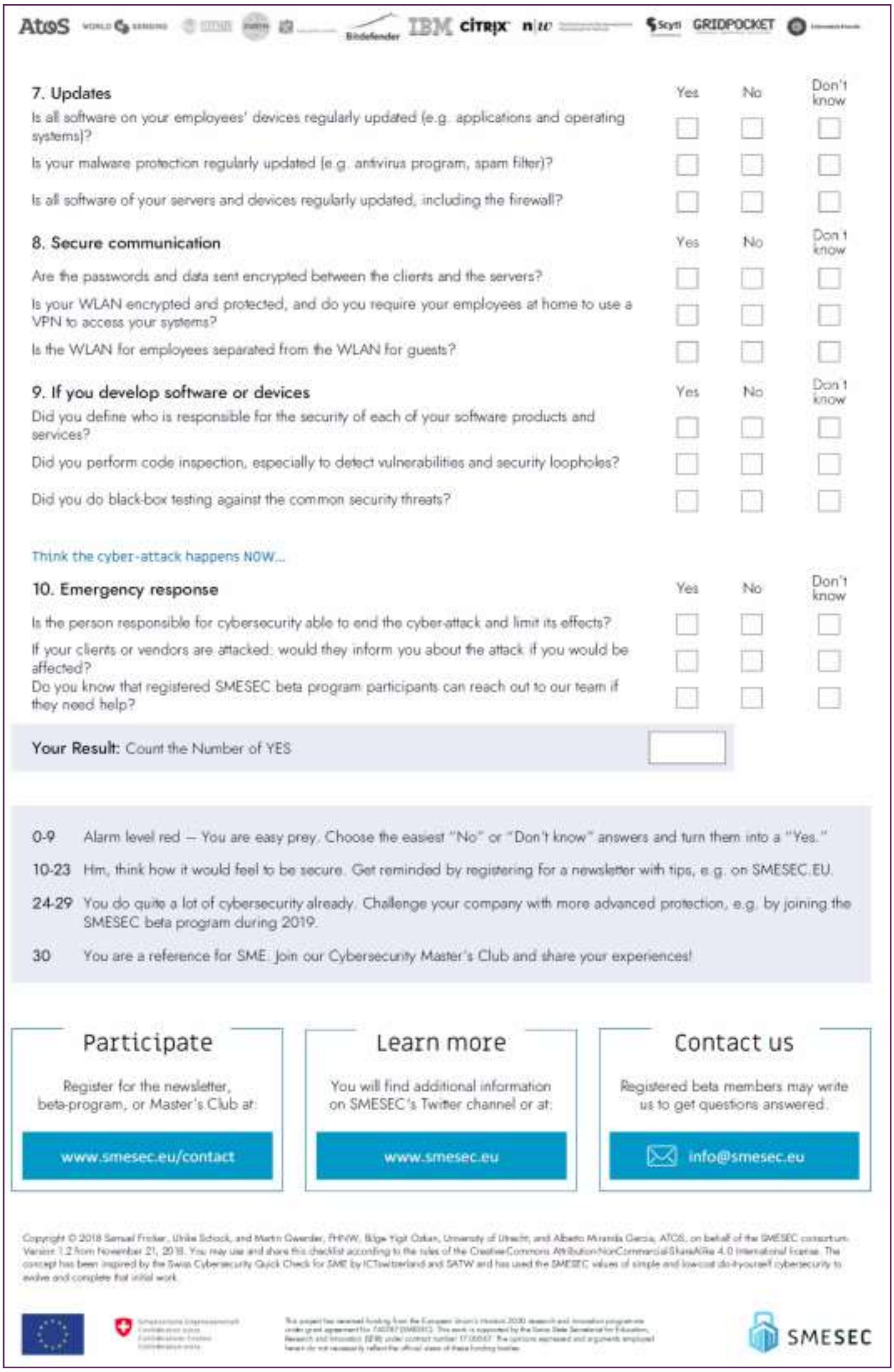
4. Backups	Yes	No	Don't know
Do you have a recent backup of your data and your systems?	□	□	□
Is a backup available offline, or at least at a different place and completely disconnected from your systems?	□	□	□
Have you tried to restore a data and or system backup and seen that it is working?	□	□	□

5. Password and user administration	Yes	No	Don't know
Are your employee's passwords strong and specific for each user account and system?	□	□	□
Can each employee only access the systems the employee is supposed to (also think of the former employees)?	□	□	□
If any employee has experienced a cyber-attack, have that employee's passwords been changed?	□	□	□

6. Malware protection	Yes	No	Don't know
Is your IT network protected by a firewall that protects your systems from outside attacks?	□	□	□
Are your devices, systems, and applications protected against malware (e.g. antivirus program, ransomware protection, and spam filter)?	□	□	□
Have you configured your malware protection to scan mail attachments, downloads, files received over networks, and connected storage media?	□	□	□

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740787 (SMESEC). This work is supported by the 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 these funding bodies.



7. Updates	Yes	No	Don't know
Is all software on your employees' devices regularly updated (e.g. applications and operating systems)?	□	□	□
Is your malware protection regularly updated (e.g. antivirus program, spam filter)?	□	□	□
Is all software of your servers and devices regularly updated, including the firewall?	□	□	□

8. Secure communication	Yes	No	Don't know
Are the passwords and data sent encrypted between the clients and the servers?	□	□	□
Is your WLAN encrypted and protected, and do you require your employees at home to use a VPN to access your systems?	□	□	□
Is the WLAN for employees separated from the WLAN for guests?	□	□	□

9. If you develop software or devices	Yes	No	Don't know
Did you define who is responsible for the security of each of your software products and services?	□	□	□
Did you perform code inspection, especially to detect vulnerabilities and security loopholes?	□	□	□
Did you do black-box testing against the common security threats?	□	□	□

Think the cyber-attack happens NOW...

10. Emergency response	Yes	No	Don't know
Is the person responsible for cybersecurity able to end the cyber-attack and limit its effects?	□	□	□
If your clients or vendors are attacked: would they inform you about the attack if you would be affected?	□	□	□
Do you know that registered SMESEC beta program participants can reach out to our team if they need help?	□	□	□

Your Result: Count the Number of YES □

0-9	Alarm level red – You are easy prey. Choose the easiest "No" or "Don't know" answers and turn them into a "Yes."
10-23	Hm, think how it would feel to be secure. Get reminded by registering for a newsletter with tips, e.g. on SMESEC.EU.
24-29	You do quite a lot of cybersecurity already. Challenge your company with more advanced protection, e.g. by joining the SMESEC beta program during 2019.
30	You are a reference for SME. Join our Cybersecurity Master's Club and share your experiences!

Participate

Register for the newsletter, beta-program, or Master's Club at:

www.smesec.eu/contact

Learn more

You will find additional information on SMESEC's Twitter channel or at:

www.smesec.eu

Contact us

Registered beta members may write us to get questions answered.

info@smesec.eu

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740787 (SMESEC). This work is supported by the 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 these funding bodies.

SMESEC

Figure 18: cybersecurity quick check questionnaire for SMEs.

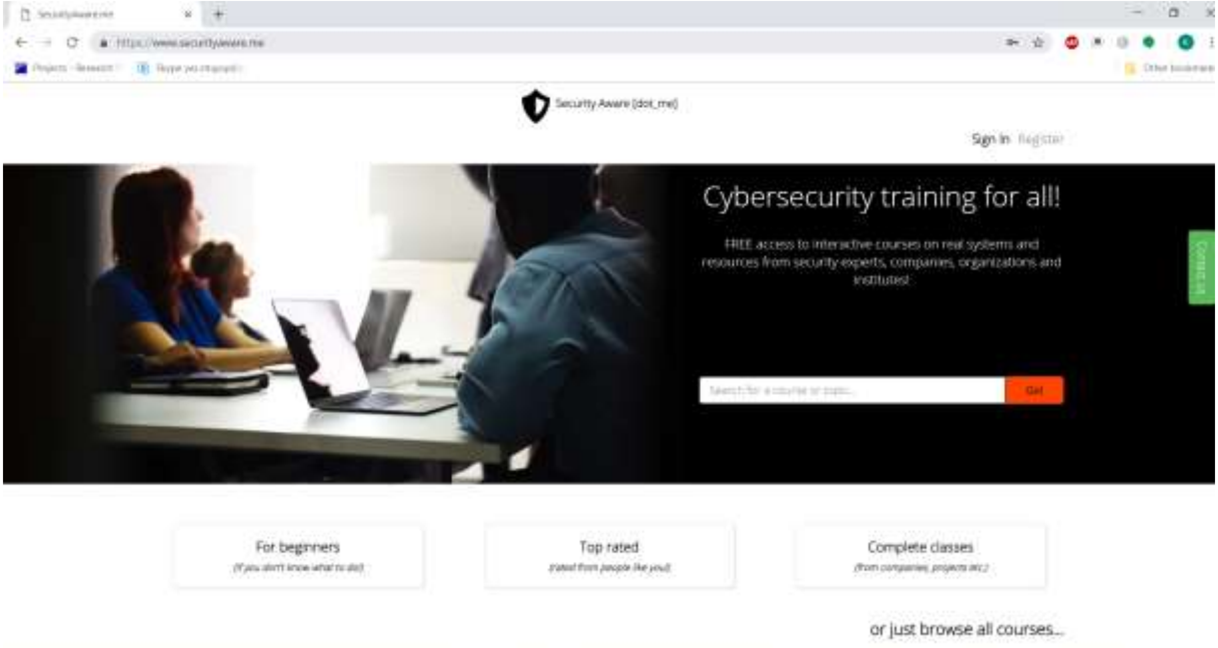
The feedback from SMEs on the questionnaire was overwhelmingly positive. The recipients were immediately studying it, and those who had experience in cybersecurity considered the quick check questionnaire to be reasonable. All of them were promising to either answer the questionnaire themselves or to test their employee responsible for cybersecurity to determine how good their company performs. The recipient most experienced in cybersecurity gave the feedback that it would be interesting to have such a questionnaire written for all employees in the SME, hence allow spreading good practice as suggested by an independent body like SMESEC (an EU project) within the company.

Several recipients asked for multiple copies of the questionnaire, indicating that the questionnaire was interesting to have and be distributed. At the time of this writing, it is still too early to assess the impact of the quick check questionnaire on the SMEs registrations for SMESEC. The deliverable D3.6 will report about the final figures.

4 SMESEC training platform and trainings

SMESEC project will create and publish a complete set of online courses to increase security awareness for its users and also train them on how to configure and operate the SMESEC framework. To provide these courses, the project will make use of a 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!

https://www.securityaware.me
Security Aware (dot_me)
Sign in
Register
Search for a course or topic...
Go!
Contact us
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 19 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 feature 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.

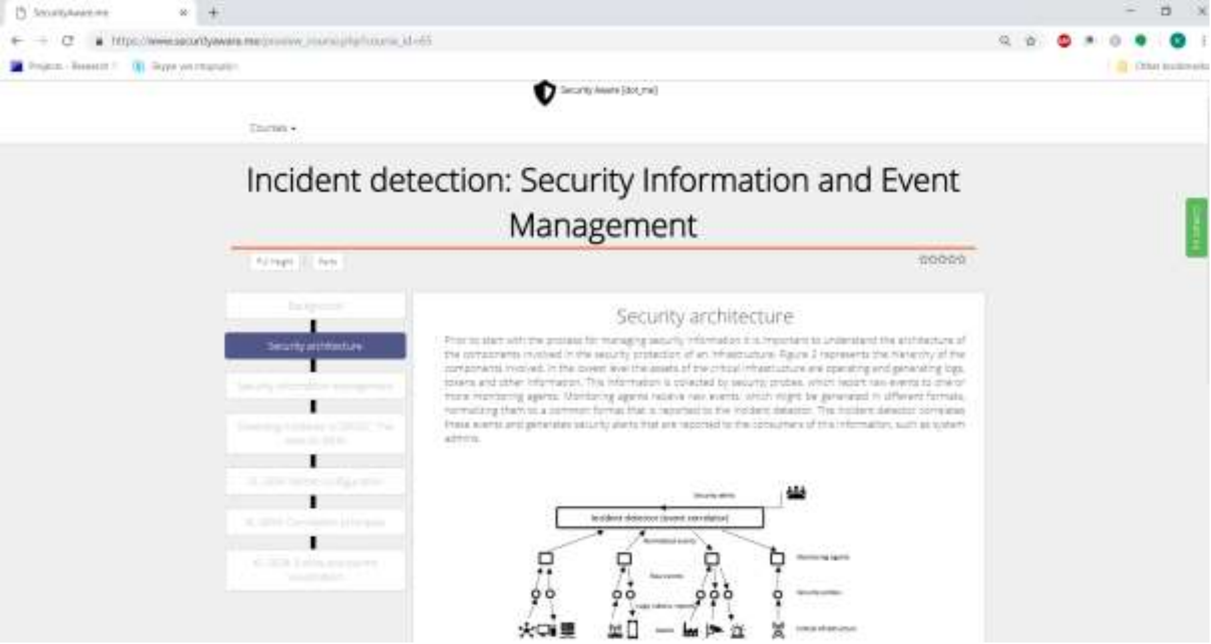
Hosted courses can be executed directly in this platform or exported in various formats to be inserted in other LMS (e.g. Moodle). In this point we must mention that SecurityAware.me is based on FORGEBox, an e-learning platform that was created in the context of the EU project FORGEBox (www.forgebox.eu). Since SecurityAware.me is an updated instance of FORGEBox it has adopted all the additional software tools, widgets and services that were created for that platform. Such tools include webssh components, visual log reports, automated resource allocation tools etc. More information these tools can be found in http://forgestore.eu/

SMESEC and SecurityAware.me: As mentioned above, one of the SecurityAware.me platform's feature is the ability to allow companies, projects etc. create their own space (page in the website). SMESEC has taken advantage of this feature and has already created its own training webpage with private courses provided by its security partners. Access to this webpage is only possible through the SMESEC framework platform.

4.1 The training platform

The SecurityAware.me training platform already hosts a set of courses which focus on various cybersecurity topics like Intrusion Detection, Digital Forensics, SIEM (Security Information and Event Management) systems, Hardware Security, Ethical Hacking etc.

A course is organized and presented in separate sections thus providing an experience similar to a presentation slideshow. The content of a course can be anything e.g. text, figures, graphs, videos etc. An example of such a course in presented in the following figure.



Incident detection: Security Information and Event Management

Security architecture

Prior to start with the process for managing security information it is important to understand the architecture of the components involved in the security protection of an infrastructure. Figure 2 represents the hierarchy of the components involved. In the lowest level the assets of the critical infrastructure are operating and generating logs, tokens and other information. This information is collected by security probes, which report raw events to one or more monitoring agents. Monitoring agents receive raw events, which might be generated in different formats, normalizing them to a common format that is reported to the incident detector. The incident detector correlates these events and generates security alerts that are reported to the consumers of this information, such as system admins.

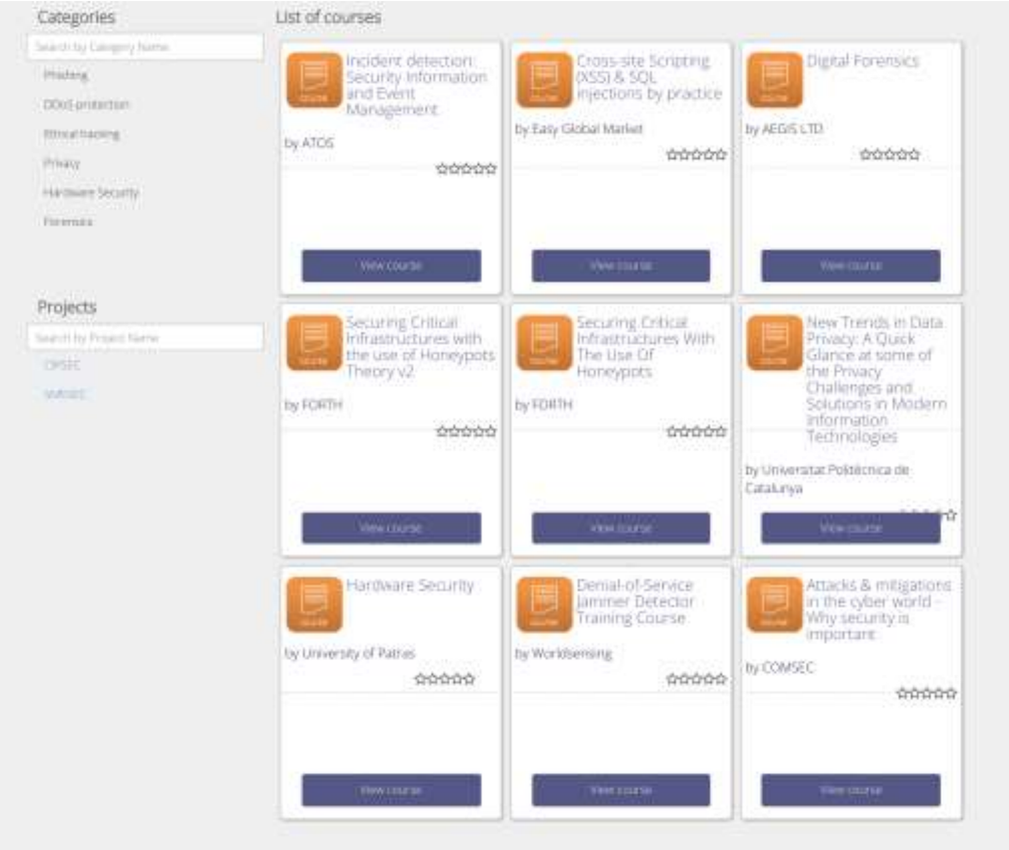
Figure 20 A course module for SIEM

One of the SecurityAware.me platform's innovations is its ability to support interactive content. The term interactive content refers to parts of the training courses that offer a "hands-on experience" to the trainees through connection to real resources, servers, networks and testbeds as well as access to various security products. In these interactive parts, users are asked to perform tests and exercises based on the theory of the overall training course (and usually precedes the hands-on part). Such an interactive part where a trainee is asked to configure a honeypot for intrusion detection is presented in the following figure 21.

Figure 21: configuration of Honey pot for intrusion

4.2 The training modules

End November 2018 we provide 9 training modules. SMESEC partners who provide tools are working on the training on their use and besides a few overall training materials on the SMESEC platform as a whole are also expected to be ready in the coming months.



Categories

Search by Category Name

- Phishing
- DDoS-protection
- Ethical hacking
- Privacy
- Hardware Security
- Forensics

Projects

Search by Project Name

- CIPSEC
- SMESEC

List of courses

Course	By
Incident detection: Security Information and Event Management	by ATOS
Cross-site Scripting (XSS) & SQL injections by practice	by Easy Global Market
Digital Forensics	by AEGIS LTD
Securing Critical Infrastructures with the use of Honeypots Theory v2	by FORTH
Securing Critical Infrastructures With The Use Of Honeypots	by FORTH
New Trends in Data Privacy: A Quick Glance at some of the Privacy Challenges and Solutions in Modern Information Technologies	by Universitat Politècnica de Catalunya
Hardware Security	by University of Patras
Denial-of-Service Jammer Detector Training Course	by Worldsensing
Attacks & mitigations in the cyber world - Why security is important	by COMSEC

Over the next months of the project, the SMESEC partners will create all the necessary training courses required to support the framework. These courses will include general cybersecurity training for inexperienced users, training material for the various tools provided by SMESEC and finally an overall course for SMEs that want to install and configure the SMESEC unified security framework.

These courses will be uploaded to the selected training platform (SecurityAware.me) to be evaluated by various types of users and employees of the pilots. Furthermore, at the consortium's suggestion, the SMESEC training webpage in SecurityAware.me platform will be visually adjusted to the project's templates to offer a unified final experience to the end-users.

4.3 The process to add training

The main goal of SMESEC is to identify what the needs from the SME perspective are and translate them into requirements for a unified framework, which will eventually consist of the SMESEC partners' contributed products.

The proposed products are often complicated to understand and be deployed if no cloud solution is provided. With respect to the goal of proposing to all SMESEC partner the ability to add a training on the Security Aware platform, the Consortium decided to have a common document in order to unify the way we add trainings into the platform.

The basic process of adding a new training to the platform is realised in three steps:

1. Write the Training.
2. Send the Training to the Training platform via mail.
3. The training platform responsible adds the new course.

The first part of adding a new training process is to write it. The preferred format is an editable Word document. The document is composed of two parts: information's and training parts.

The information's part must include the following:

- **Author**
- **Company**
- **Contact**
- **Training Title**
- **Difficulty Level** (Hard/Medium/Easy)
- **Small Description**
- **Category** (Example: Cybersecurity)
- **Key Words**

Then the training body must be separated in distinct PART's in order to guide the end users.

Each part must begin by the keyword "**PART**" and be followed by its part number: PART 1, PART 2, PART 3….

The final result from the Word document into the web training platform is a **WYSIWYG** (What You See, Is What You Get) approach. All listings and numeration including picture placement is reproduced visually in the training platform. As well as for external link.

Nevertheless, one specific part must be annotated: the code block part. If required in the training, including a code block must be clearly annotated by the tags: **<CODE> (Include Code here) </CODE>**

We have created a training course "*Cross-site Scripting (XSS) & SQL injections by practice*" that has been added into the Security Aware platform:

https://www.securityaware.me/preview_course.php?course_id=60.

Annex A provides the complete Word document.

5 Assessment of cybersecurity awareness and maturity of SMEs

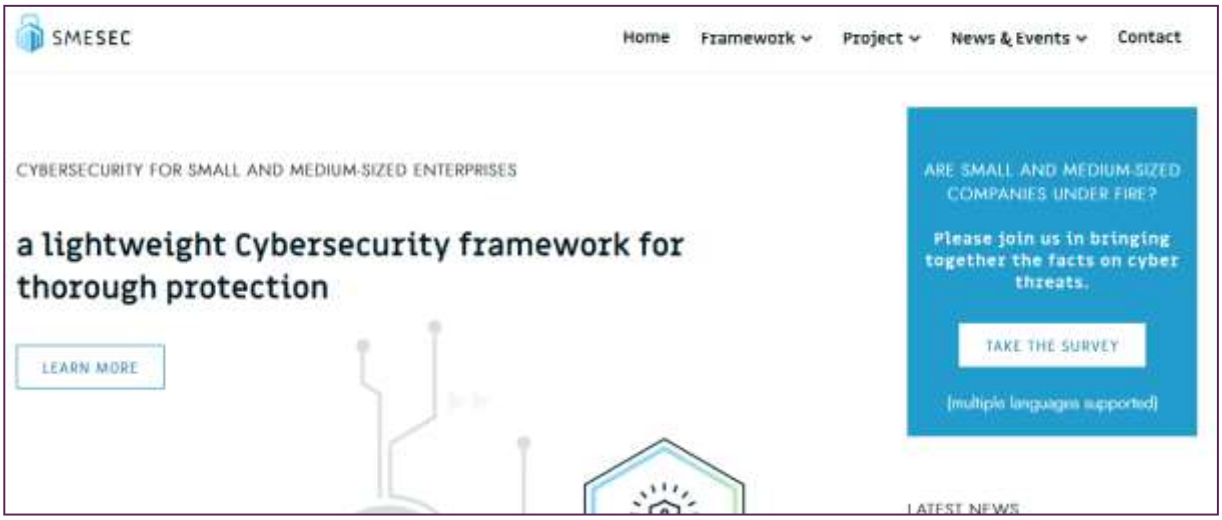
SMESEC offers cybersecurity awareness and improvement to SME and reports for the open cybersecurity community about the state-of-the-practice of cybersecurity in SME. The questions that will be addressed by the community report will include the following:

- What are the cyber threats that SMEs are exposed to?
- How common are the respective attacks?
- How common is a cybersecurity practice in use among the SMEs?
- How much do SMEs appreciate a given cybersecurity practice?
- What are the enablers and hindrances for cybersecurity practice adoption by SMEs?
- How long time does an SME need to complete the improvement work for a given capability area?
- How fast does an SME respond to an experienced cyber incident with incident response and improvement of the associated capabilities?

The community report is built with the participating SMEs. So far, the SMEs that participated are the SMEs that participated in the SMESEC online survey and the four SMESEC use case SMEs. SMESEC continuous to grow the community of participants through the dissemination activities described in WP6 and the validation activities in WP5.

5.1 Survey: investigating the cyber threat exposure and awareness of SMEs

SMESEC has been creating and is continuously advertising a survey to understand the exposure of SMEs to cyber threats and awareness of these SMEs about these threats and how to address the threats with cybersecurity. The survey is offered in English, German, French, Spanish, and Greek. The following figure shows the call for joining the survey on the SMESEC.EU homepage.



CYBERSECURITY FOR SMALL AND MEDIUM-SIZED ENTERPRISES

a lightweight Cybersecurity framework for thorough protection

ARE SMALL AND MEDIUM-SIZED COMPANIES UNDER FIRE?

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

(multiple languages supported)

Figure 22: Call for joining the SMESEC survey on www.smesec.eu (blue box on the right-hand side).

The survey tries to find out the company profile, the threat exposure, and optionally the cybersecurity practices and priorities of the SME. The survey is anonymous, and contact information is collected with a form separate from the survey form. The survey includes the questions described in the following table.

Table 3: Survey questions.

Question group	**Questions**	**Comments**
Respondent profile	What is the job title stated on your business card? Are you responsible for the cybersecurity of your company? Did you receive any training in the field? Your pseudonymous identifier	To collect information about the respondent to judge the credibility of the answers and connect the received answer with answers in future survey.
Company profile	Company Size Type of Business Domain of Business	To collect information about contextual factors that may influence the threat exposure and practices.
Cyber threats	Does your company consider itself to be a target for hackers? What cyber-attacks or data breaches did your company experience in the past 12 months? What were the consequences of the attacks on your company? Is your company worried about cyber threats? In comparison to 12 months ago, did your company's worries about cyber threats change as follows.	To collect subjective and objective information about the SME’s cyber threat exposure.

Question group	Questions	Comments
Protection and practices	Can your company well mitigate cyber risks, vulnerabilities, and attacks? Can your company easily recover from a cyber-attack? Does your company have a systematic approach to ensuring cybersecurity? Who does cybersecurity for your company? What budget is allocated to cybersecurity?	To collect subjective and objective information about the SME's cybersecurity practices.
Cybersecurity improvement	Sources of knowledge about cybersecurity May your company consider slowing or pausing operations for some days and improve cybersecurity? How could your company improve cybersecurity?	To collect information about the SME's preferences to improve cybersecurity.

The survey form was used in an online self-answering mode by the respondents as well as in structured interviews that FHNW was performing with many SMEs.

5.2 1st Community report: mapping of cyber threat exposure and awareness of SMEs

Based on 22 answers, the first SMESEEC community report "Cybersecurity Radar for Small and Medium-sized Enterprises (SMESEC Radar)" has been created. It summarizes the SME's opinion about cybersecurity, offers an interpretation from the SMESEC consortium's perspective, and invites for joining the SMESEC activities.

Cybersecurity Radar for Small and Medium-sized Enterprises (SMESEC Radar)

With the SMESEC Radar, we want to find out about the start of cybersecurity for small and medium-sized enterprises. We have received 22 answers on a structured questionnaire (which can be found below). 64% were micro companies, and 27% small companies. The companies were active in development, trading, or service provision with hardware, software, data, human-based offerings. 48% were active in the ICT domain, 13% in education, and the rest covered 6 further business domains.

Are SMEs Targets for Hackers?

The SMEs tended to have a positive view of their potential exposure to hackers. 41% did not have an opinion. Of those who had an opinion, only 38% thought that they are a target.

This positive view corresponded with the experience of the SMEs. 47% of the respondents could not remember any attack in the previous year. The SME attack profile shows that the large majority had experienced mild attacks, while moderate or severe attacks were rare or inexistent.

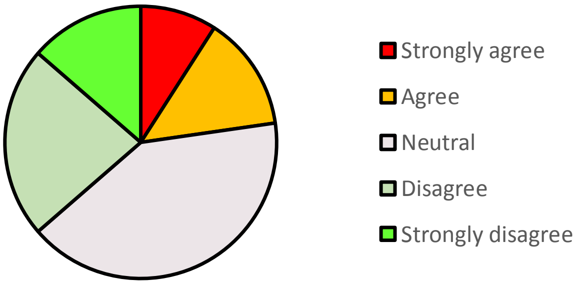


Figure 23: Perception of being a target for hackers

What are the Consequences of Attacks?

23% of the respondents did not know the consequences of the attacks their enterprise had experienced. Of those who knew, 59% encountered incident costs or business disruptions. 41% did not observe any consequences of attacks. The SMEs felt better prepared to address threats than to recover from an incident. 45% of the enterprises believed that they could address cyber threats, and 23% indicated they would have low ability. In comparison, only 33% feel they would be able to recover with 24% feeling they would have low ability.

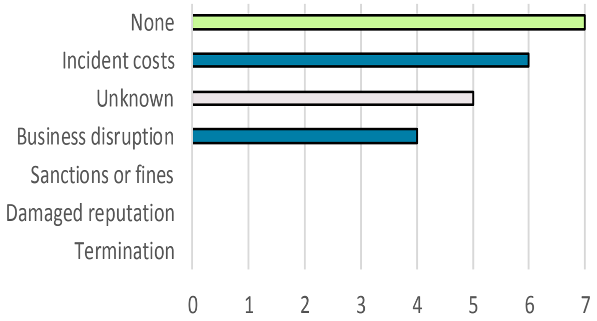


Figure 24: consequences of attacks experienced by the participating SME

Are SMEs Worried?

The SMEs tended to be worried about cyber threats, and the worries tended to increase over the last year. 63% of the SMEs who had an opinion stated they would be worried, while only 38% disagreed with that statement. 27% did not have an opinion. 50% of the SME stated that their worries increased over the last year, while another 50% indicated that their worries were the same.

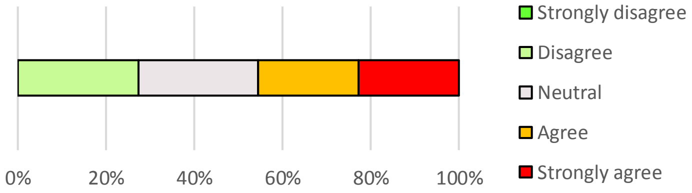


Figure 25: degree of worry among the SMEs

How do the SMEs do Cybersecurity?

SMEs tended to consider their cybersecurity practices as being unsystematic. Of the respondents who could judge, 67% indicated that their practices were unsystematic, while 33% indicated that their practices were systematic. Nevertheless, most SMEs had clear assigned responsibility for cybersecurity. 64% of the SMEs had appointed an internal person or team to be responsible for cybersecurity. From the rest, 67% let everybody do a bit of cybersecurity. Only a few SMEs outsourced cybersecurity (8%) or had nobody doing cybersecurity (4%).

However, SMEs did not spend on cybersecurity or had just little spending. Of the respondents who could estimate the spending, 65% did not devote any budget to cybersecurity. 29% spent a maximum of 2% of their turnover, and 6% a maximum of 5%.

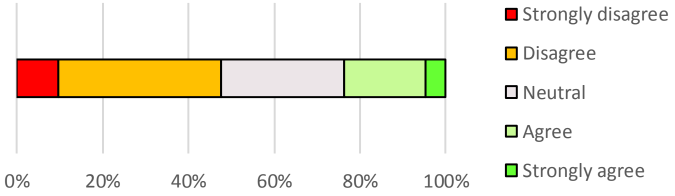


Figure 26: systematicity of cybersecurity practices in SMEs.

Would SMEs Improve Cybersecurity, and How?

Almost half of the SMEs considered cybersecurity to be critical enough to slow or pause business for developing their cybersecurity capabilities. Of the respondents who had an opinion, 44% strongly agreed, and 22% agreed. Only 33% disagreed. 40% had no opinion.

The priorities for improvement should be on training employees (68% of the respondents), followed by systematising vulnerability search (45%) and improved tooling (41%). Interesting for the community is that some SMEs would participate in exchanging lessons-learned (36%). Figure 27 gives a complete overview of the priorities for improvement.

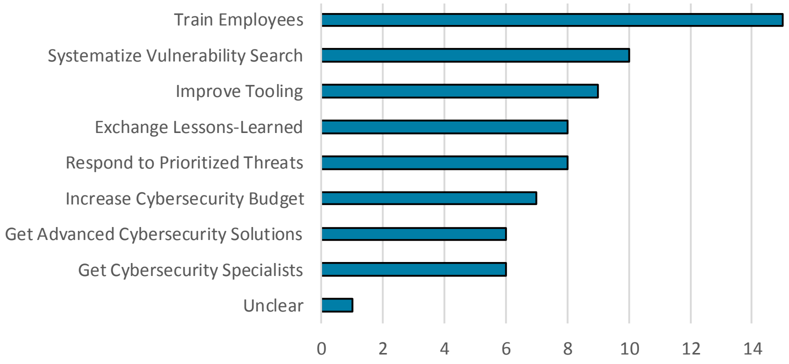


Figure 27: priorities for improving cybersecurity in SMEs.

SMEs are open to a variety of channels to receive support. Most would welcome websites or forums as knowledge sources, and many would accept external experts and webinars. Just some appreciated classroom training, and only a few considered the media as an adequate knowledge source. For anybody wanting to help SMEs, interesting to know is that most SMEs would like to do own research. Thus, enabling their research may be attractive and effective for assisting an SME.

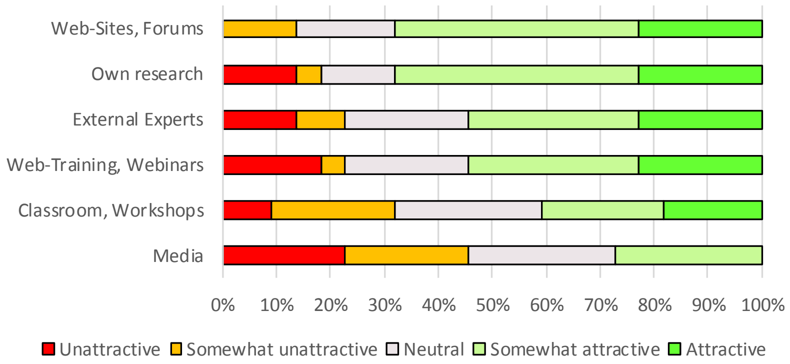


Figure 28: attractiveness of source for cybersecurity knowledge as perceived by SME.

https://www.smesec.eu/survey

SMESEC complements the radar with in-depth case studies. In such a case study, SMESEC is studying an SME from the inside out and is testing prototypes of the tools to evaluate the acceptance and effect of the SMESEC solution.

The consortium is looking for SMEs that are interested in joining the SMESEC beta programme, which launches in 2019. As a benefit, the participating SMEs can use the SMESEC tools early and without cost during the beta testing phase. SMESEC foresees two levels of beta testing: lightweight with minimal obligations, and premium with financial support for the SMEs. Please register at:

https://www.smesec.eu/contact

The presented 1st Community Report shows how the open community of cybersecurity experts may benefit from the data collected in SMESEC. The SMESEC consortium will be adapting the survey based on the observed results and obtained feedback. Further adaptations of the community report will be based on the CYSEC tools that will offer insights about the adoption of cybersecurity practices in addition to the introductory-level questions described in this section. 4-6 community reports will be published per year and provided in conjunction with the SMESEC dissemination.

6 Conclusions

In first period we mainly developed tools to interact with SMEs such as questionnaires and Cyber Security Coaching tool (e.g. CYSEC tool). We start interacting with SMEs at various events and we initiated many contacts with European and National SMEs associations. Such associations are now waiting for SMESEC to present its initial solutions and many interactions with SMEs through on-line communication, webinars and workshops are planned for the 2nd period.

Training platform was developed and some initial trainings including template to provide were provided. We plan to organise training session from beginning 2nd period.

Initial feedback from SMEs understanding of cybersecurity items was provided in 1st period but more we interact we SMEs more we expect getting more detailed feedbacks expected more intensive in the second period.

7 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

Annex

ANNEX A

Author: Abbas AHMAD

Company: Easy Global Market

Contact: abbas.ahmad@eglobalmark.com

Training Title: Cross-site Scripting (XSS) & SQL injections by practice

Difficulty Level: Medium/Hard

Small Description: The objective of the Training is to learn about the security problems of web applications, taking on the role of a web security engineer.

Category: Cybersecurity

Key Words: XSS, SQL, Injection, XAMPP, security, web

PART 1: Objectives of the training

The objective of the Training is to learn about the security problems of web applications, taking on the role of a web security engineer. Several sub-objectives are expected:

- Practice exploiting security vulnerabilities in a legal environment: **DVWA**
  - Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.
- Understand the risks of a company deploying an unsecure application
- Beyond the role of web security engineer, learn methods and means of countermeasures to secure a web application:
  - As a system engineer, understand the importance of proper database access setup
  - As a development engineer, understand the importance of good development practices
  - As a customer / user account manager, understand the importance of good user profile management

Requirement for the Training

- Internet access
- Local Web Server to deploy DVWA (installation steps included)

PART 2: Initialization of the training

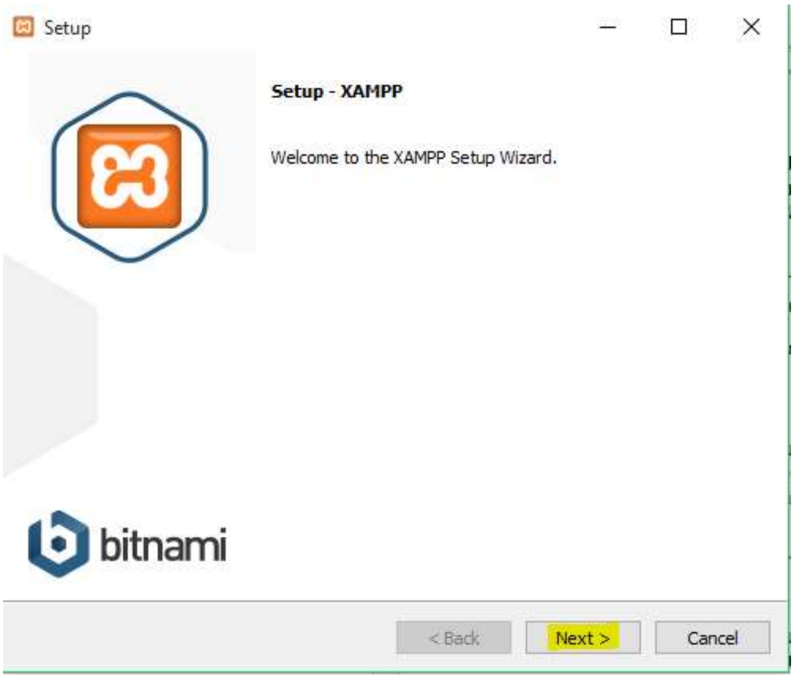
We provide here the procedure to follow to install a local server (xampp) on windows.

If you are under linux, you can follow this tutorial: http://www.howtoforge.com/installing- apache2-

with-php5-and-mysql-support-on-ubuntu-11.04-lamp

To start the Training, you need to

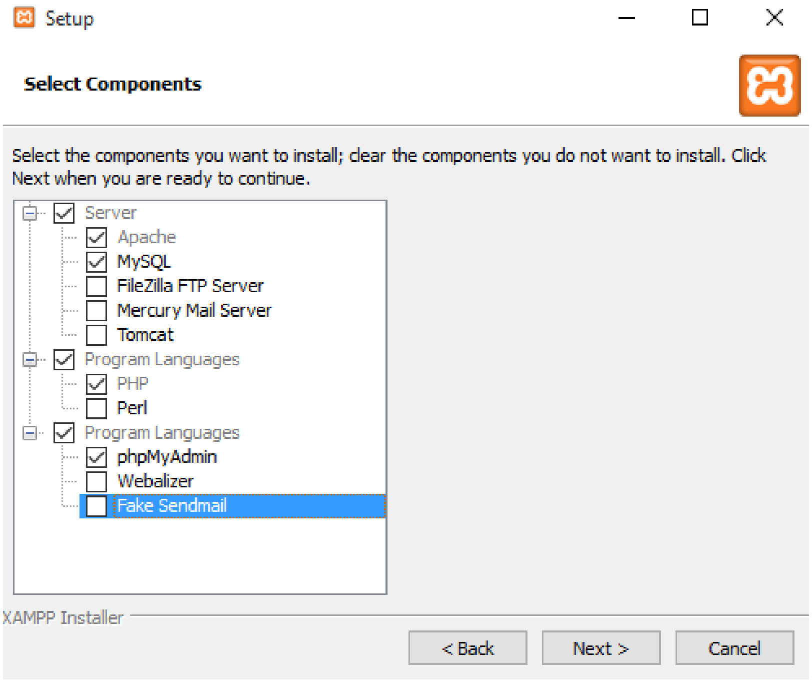
1. Install a local Apache/PHP/SQL server:
    - Access the Xampp website: http://www.apachefriends.org/en/xampp-windows.html
    - Download the latest version
    - Run the installation as follows:



Setup - XAMPP

Welcome to the XAMPP Setup Wizard.

Select only the software you need (Apache, MySQL, PHP and phpMyAdmin)

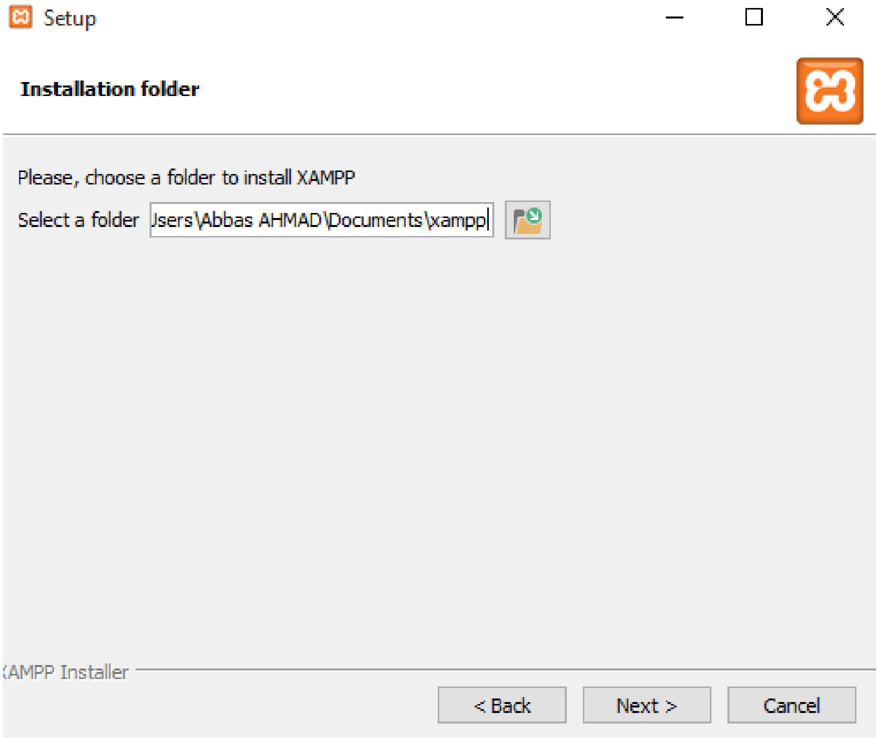


Select Components

Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

- ☑ Server
    - ☑ Apache
    - ☑ MySQL
    - ☐ FileZilla FTP Server
    - ☐ Mercury Mail Server
    - ☐ Tomcat
- ☑ Program Languages
    - ☑ PHP
    - ☐ Perl
- ☑ Program Languages
    - ☑ phpMyAdmin
    - ☐ Webalizer
    - ☐ Fake Sendmail

Install XAMPP in a folder where you have write permissions, your documents folder or on Desktop for example.



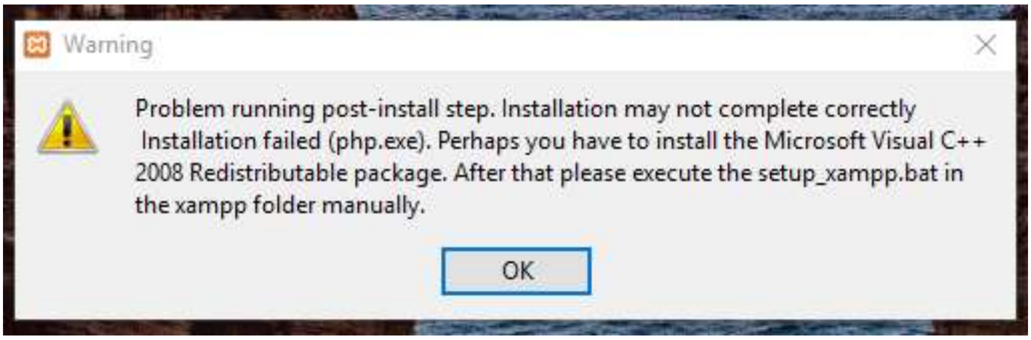
Setup

Installation folder

Please, choose a folder to install XAMPP

Select a folder Jsers\Abbas AHMAD\Documents\xampp

While installing you may encounter a Warning stating you need to install Microsoft Visual C++ 2008 Redistributable package



Warning

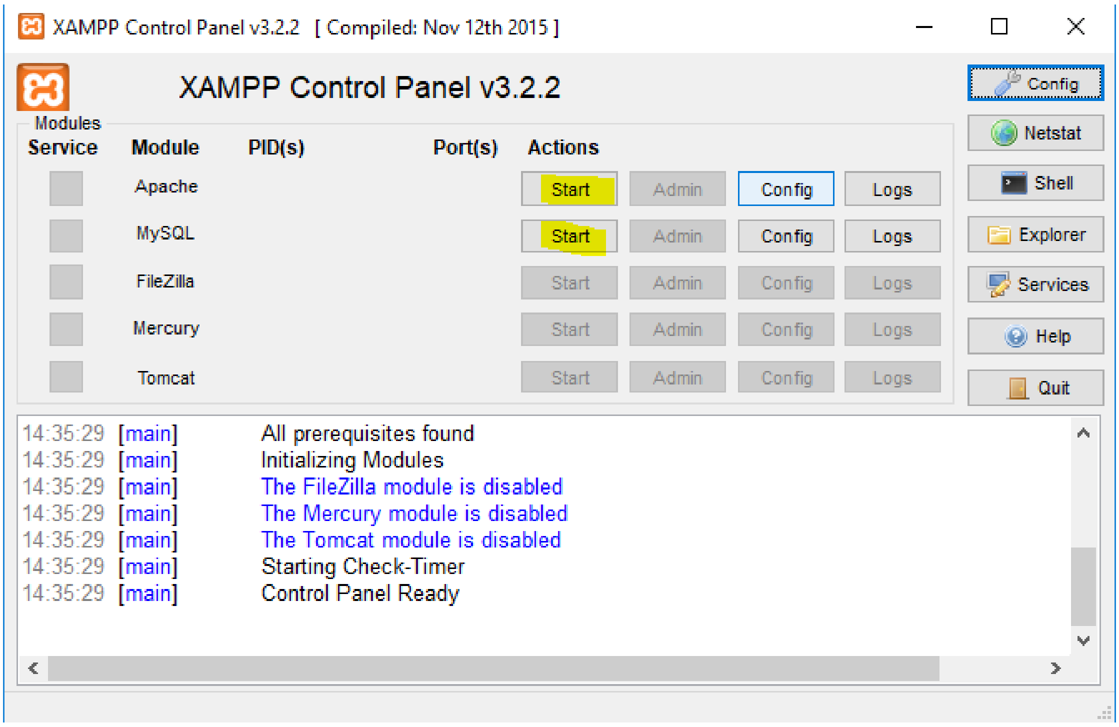
Problem running post-install step. Installation may not complete correctly
Installation failed (php.exe). Perhaps you have to install the Microsoft Visual C++ 2008 Redistributable package. After that please execute the setup_xampp.bat in the xampp folder manually.

You can find this package here:

https://www.microsoft.com/en-us/download/details.aspx?id=15336

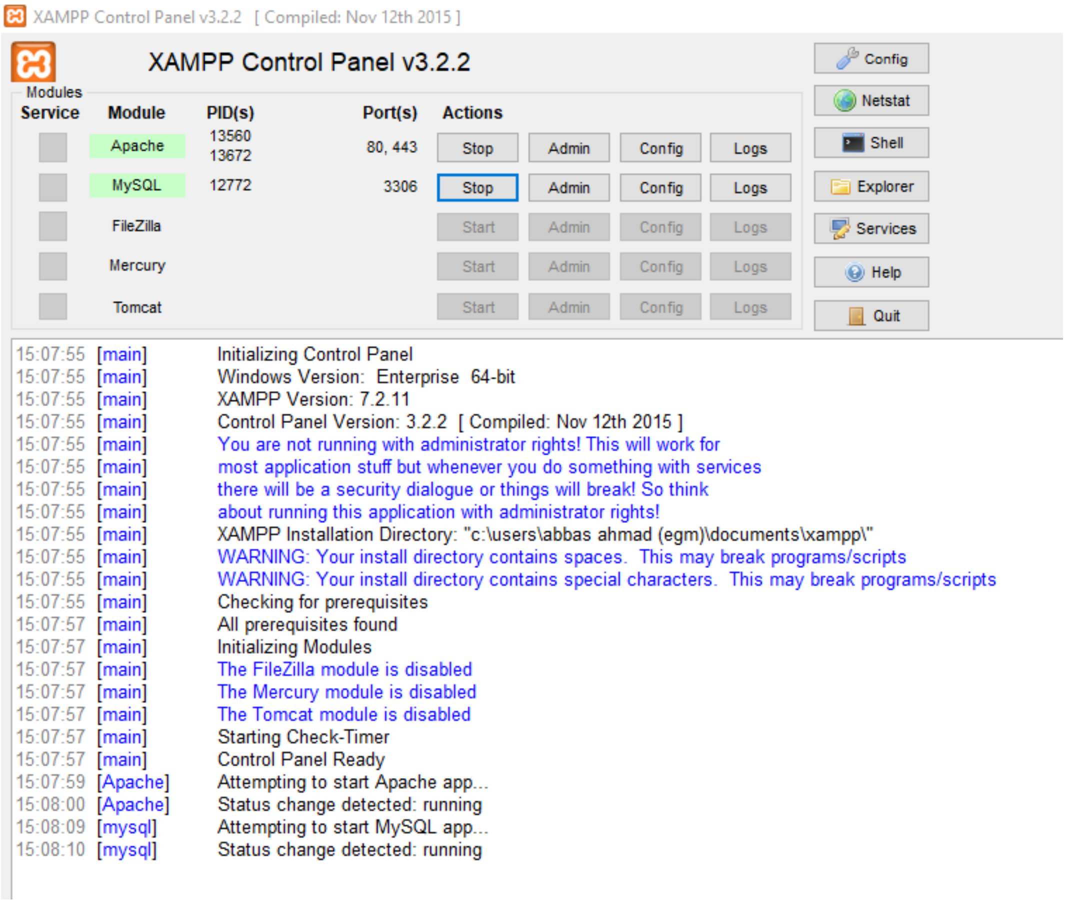
Then re-launch the installation process.

Once installed, launch XAMPP and start the "Apache" and "MySQL" modules.



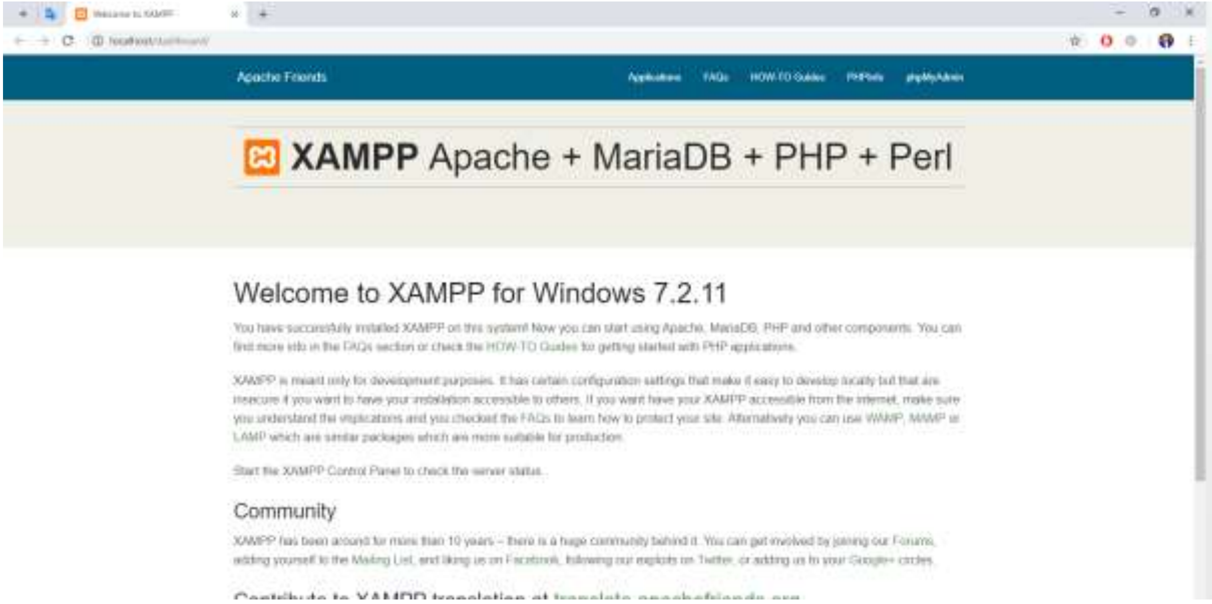
```
14:35:29  [main]        All prerequisites found
14:35:29  [main]        Initializing Modules
14:35:29  [main]        The FileZilla module is disabled
14:35:29  [main]        The Mercury module is disabled
14:35:29  [main]        The Tomcat module is disabled
14:35:29  [main]        Starting Check-Timer
14:35:29  [main]        Control Panel Ready
```

You should have XAMPP in the following state (ensuring that Apache and MySQL have started correctly):



```
15:07:55  [main]      Initializing Control Panel
15:07:55  [main]      Windows Version:  Enterprise  64-bit
15:07:55  [main]      XAMPP Version: 7.2.11
15:07:55  [main]      Control Panel Version: 3.2.2  [ Compiled: Nov 12th 2015 ]
15:07:55  [main]      You are not running with administrator rights! This will work for
15:07:55  [main]      most application stuff but whenever you do something with services
15:07:55  [main]      there will be a security dialogue or things will break! So think
15:07:55  [main]      about running this application with administrator rights!
15:07:55  [main]      XAMPP Installation Directory: "c:\users\abbas ahmad (egm)\documents\xampp\"
15:07:55  [main]      WARNING: Your install directory contains spaces.  This may break programs/scripts
15:07:55  [main]      WARNING: Your install directory contains special characters.  This may break programs/scripts
15:07:55  [main]      Checking for prerequisites
15:07:57  [main]      All prerequisites found
15:07:57  [main]      Initializing Modules
15:07:57  [main]      The FileZilla module is disabled
15:07:57  [main]      The Mercury module is disabled
15:07:57  [main]      The Tomcat module is disabled
15:07:57  [main]      Starting Check-Timer
15:07:57  [main]      Control Panel Ready
15:07:59  [Apache]    Attempting to start Apache app...
15:08:00  [Apache]    Status change detected: running
15:08:09  [mysql]     Attempting to start MySQL app...
15:08:10  [mysql]     Status change detected: running
```

Open a browser and access the page http://localhost/ . If the installation is OK, you should see the page below.



XAMPP Apache + MariaDB + PHP + Perl

Welcome to XAMPP for Windows 7.2.11

You have successfully installed XAMPP on this system! Now you can start using Apache, MariaDB, PHP and other components. You can find more info in the FAQs section or check the HOW-TO Guides for getting started with PHP applications.

XAMPP is meant only for development purposes. It has certain configuration settings that make it easy to develop locally but that are insecure if you want to have your installation accessible to others. If you want have your XAMPP accessible from the internet, make sure you understand the implications and you checked the FAQs to learn how to protect your site. Alternatively you can use WAMP, MAMP or LAMP which are similar packages which are more suitable for production.

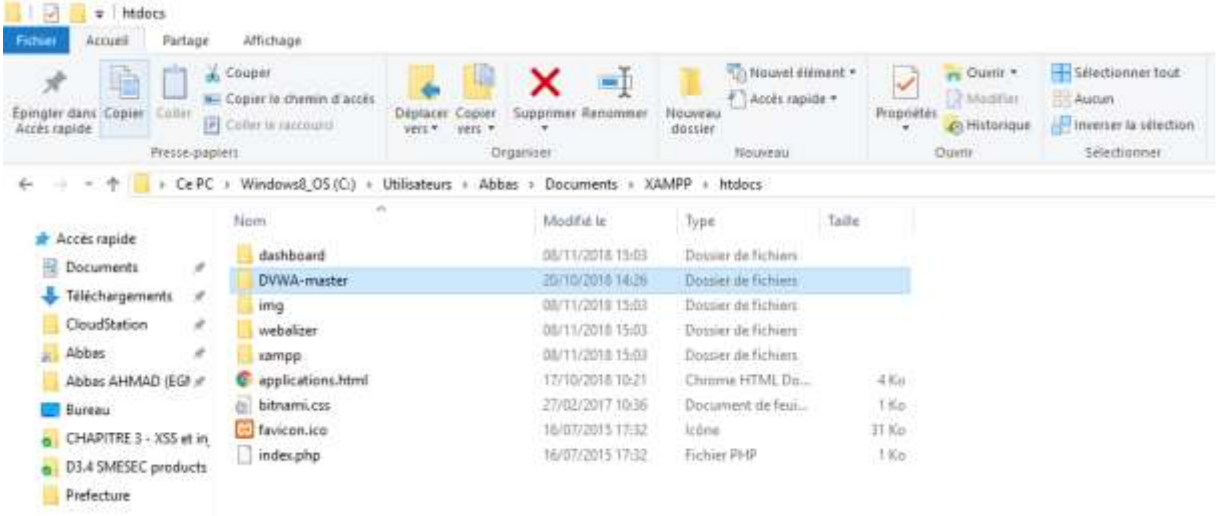
Start the XAMPP Control Panel to check the server status.

Community

XAMPP has been around for more than 10 years – there is a huge community behind it. You can get involved by joining our Forums, adding yourself to the Mailing List, and liking us on Facebook, following our exploits on Twitter, or adding us to your Google+ circles.

Contribute to XAMPP translation at translate.apachefriends.org

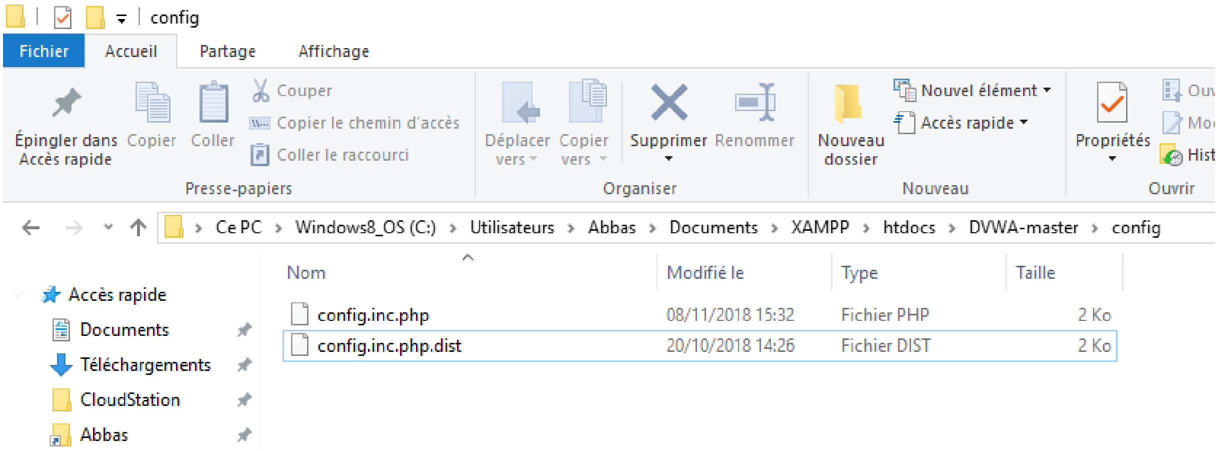
2. Retrieve the DVWA web application at http://www.dvwa.co.uk
   - Deploy the DVWA application on the local XAMPP by unzipping the downloaded archive in '{YourPath} /xampp/ htdocs'



Ce PC › Windows8_OS (C:) › Utilisateurs › Abbas › Documents › XAMPP › htdocs

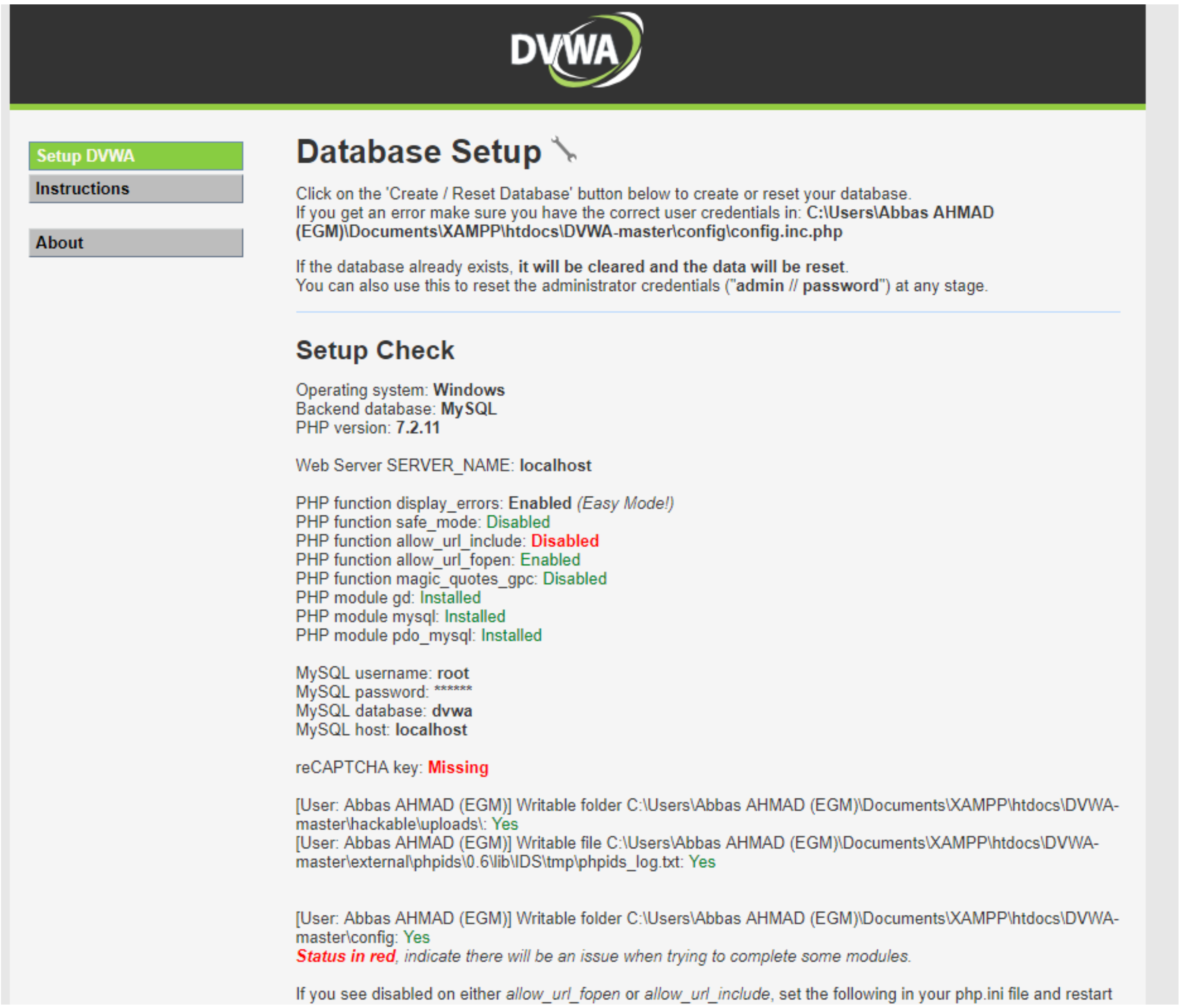
Nom	Modifié le	Type	Taille
dashboard	08/11/2018 13:03	Dossier de fichiers	
DVWA-master	20/10/2018 14:26	Dossier de fichiers	
img	08/11/2018 15:03	Dossier de fichiers	
webalizer	08/11/2018 15:03	Dossier de fichiers	
xampp	08/11/2018 15:03	Dossier de fichiers	
applications.html	17/10/2018 10:21	Chrome HTML Do...	4 Ko
bitnami.css	27/02/2017 10:36	Document de feui...	1 Ko
favicon.ico	16/07/2015 17:32	Icône	31 Ko
index.php	16/07/2015 17:32	Fichier PHP	1 Ko

Go to the Install folder, open the config folder within and copy paste the “config.inc.php.dist” into config.inc.php.



Nom	Modifié le	Type	Taille
config.inc.php	08/11/2018 15:32	Fichier PHP	2 Ko
config.inc.php.dist	20/10/2018 14:26	Fichier DIST	2 Ko

Open in your browser the following address: http://localhost/DVWA-master



Database Setup

Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in: **C:\Users\Abbas AHMAD (EGM)\Documents\XAMPP\htdocs\DVWA-master\config\config.inc.php**

If the database already exists, **it will be cleared and the data will be reset**.
You can also use this to reset the administrator credentials ("**admin** // **password**") at any stage.

Setup Check

Operating system: **Windows**
Backend database: **MySQL**
PHP version: **7.2.11**

Web Server SERVER_NAME: **localhost**

PHP function display_errors: **Enabled** *(Easy Mode!)*
PHP function safe_mode: Disabled
PHP function allow_url_include: **Disabled**
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
PHP module gd: Installed
PHP module mysql: Installed
PHP module pdo_mysql: Installed

MySQL username: **root**
MySQL password: ******
MySQL database: **dvwa**
MySQL host: **localhost**

reCAPTCHA key: **Missing**

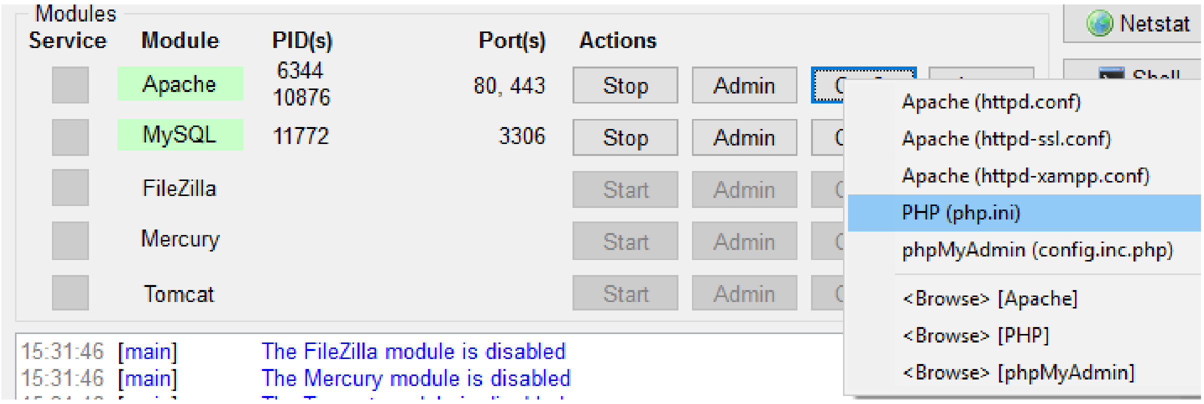
[User: Abbas AHMAD (EGM)] Writable folder C:\Users\Abbas AHMAD (EGM)\Documents\XAMPP\htdocs\DVWA-master\hackable\uploads\: Yes
[User: Abbas AHMAD (EGM)] Writable file C:\Users\Abbas AHMAD (EGM)\Documents\XAMPP\htdocs\DVWA-master\external\phpids\0.6\lib\IDS\tmp\phpids_log.txt: Yes

[User: Abbas AHMAD (EGM)] Writable folder C:\Users\Abbas AHMAD (EGM)\Documents\XAMPP\htdocs\DVWA-master\config: Yes
Status in red, *indicate there will be an issue when trying to complete some modules.*

If you see disabled on either *allow_url_fopen* or *allow_url_include*, set the following in your php.ini file and restart

You notice that the PHP function "allow_url_include" is by default disabled. We need to activate it.

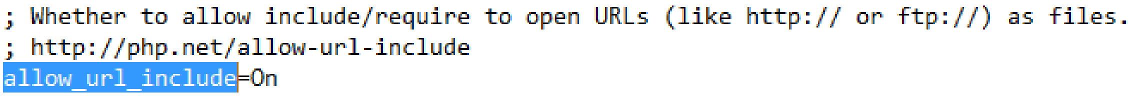
In the XAMPP application, access the PHP configuration file:



Service	Module	PID(s)	Port(s)	Actions	
	Apache	6344 10876	80, 443	Stop	Admin
	MySQL	11772	3306	Stop	Admin
	FileZilla			Start	Admin
	Mercury			Start	Admin
	Tomcat			Start	Admin

```
15:31:46  [main]        The FileZilla module is disabled
15:31:46  [main]        The Mercury module is disabled
```

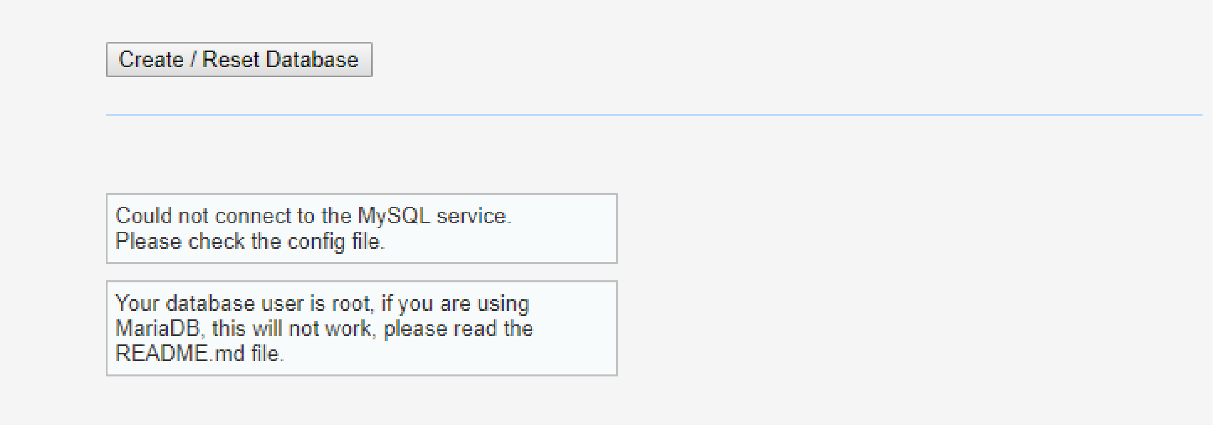
Look for the line "allow_url_include" and change its value to "On":



```
; Whether to allow include/require to open URLs (like http:// or ftp://) as files.
; http://php.net/allow-url-include
allow_url_include=On
```

Once the file has been successfully modified, press the "Create / Reset Database" button on the webpage.

If it shows you an error as in the following picture:

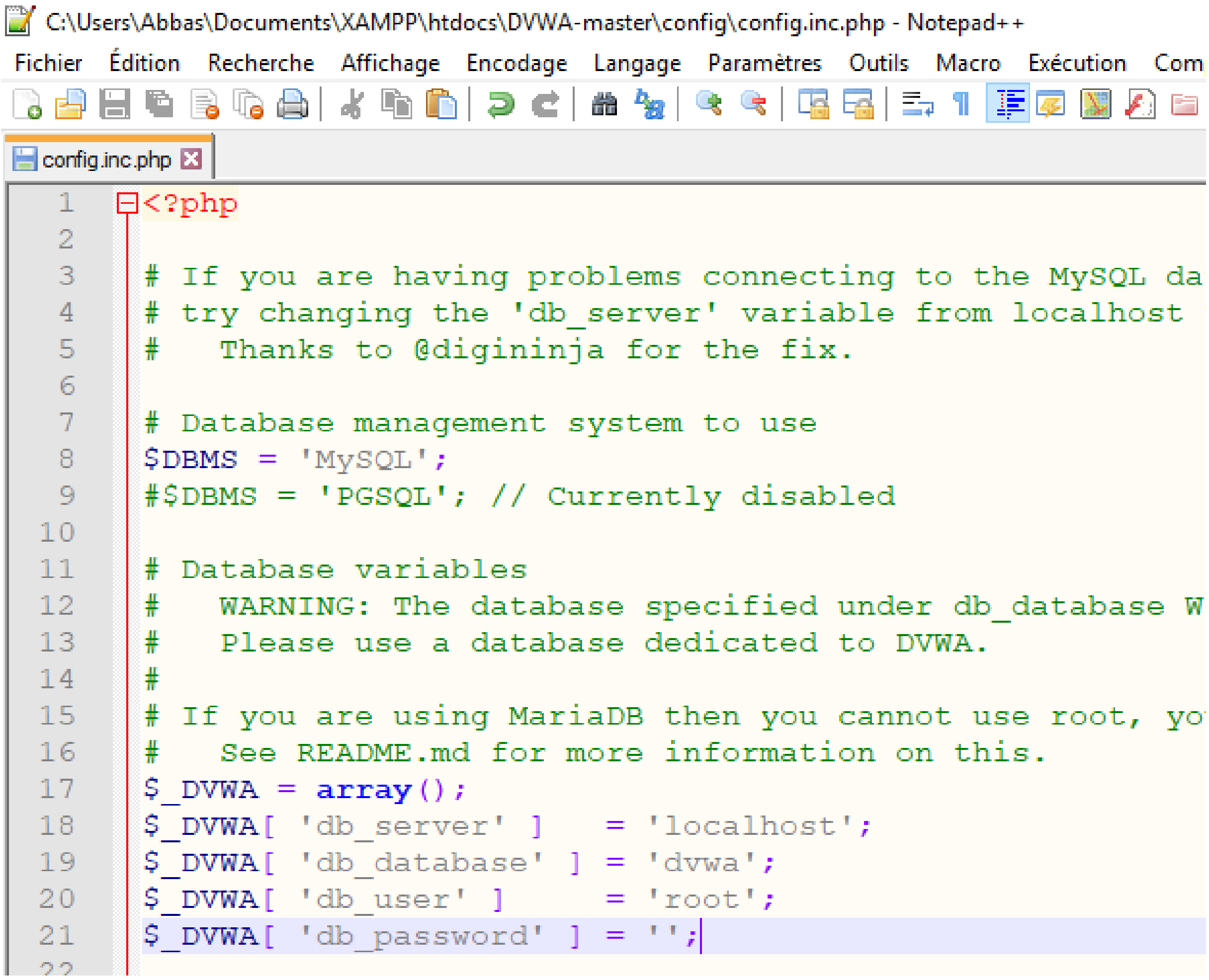


Could not connect to the MySQL service.
Please check the config file.

Your database user is root, if you are using MariaDB, this will not work, please read the README.md file.

You have to change the configuration of DVWA-master, access your DVWA-master deployment folder: '{YourPath} /xampp /htdocs/DVWA-master' then locate the file config.inc.php in the folder "config ".

By default during the installation of MySQL, it creates a user "root" without password. It is therefore necessary to locate the line "$ _DVWA ['db_password'] = 'p@ssword'; In the config file and delete the value. You can edit the file using your favorite text editor.

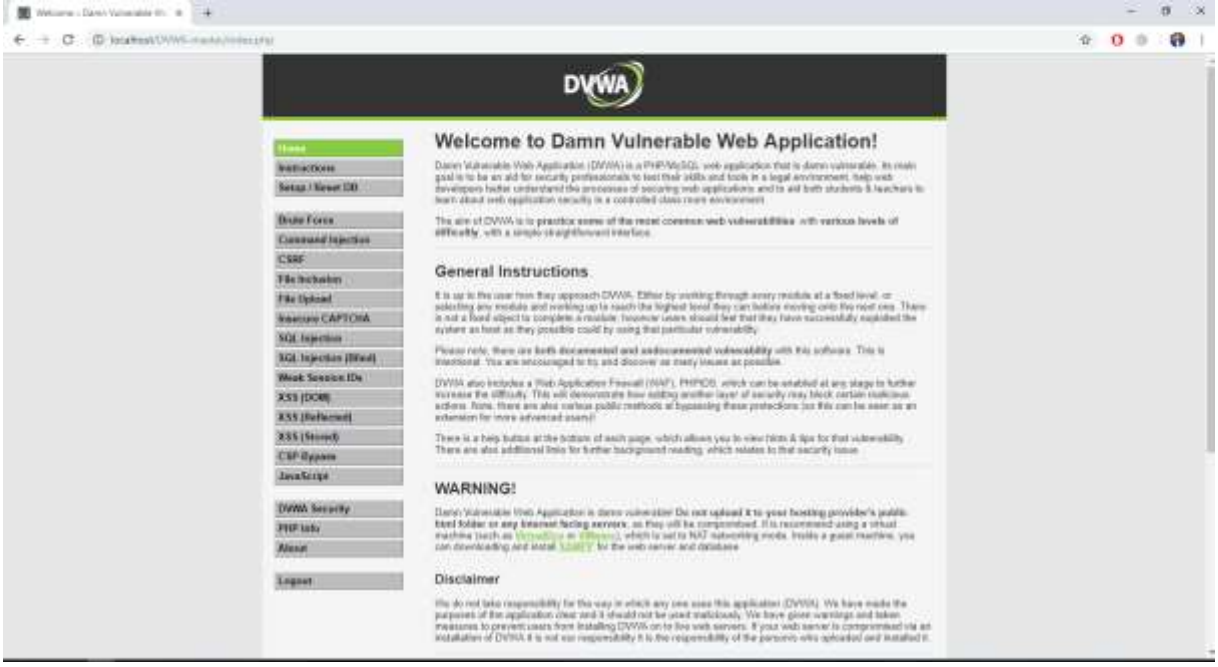

C:\Users\Abbas\Documents\XAMPP\htdocs\DVWA-master\config\config.inc.php - Notepad++
Fichier Édition Recherche Affichage Encodage Langage Paramètres Outils Macro Exécution Com
config.inc.php

```
<?php

# If you are having problems connecting to the MySQL da
# try changing the 'db_server' variable from localhost
#   Thanks to @digininja for the fix.

# Database management system to use
$DBMS = 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# Database variables
#   WARNING: The database specified under db_database W
#   Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, yo
#   See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ]   = 'localhost';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ]     = 'root';
$_DVWA[ 'db_password' ] = '';
```

Once the modification are done, restart the "Apache" and "MySQL" modules by stopping and restarting them: "Stop" -> "Start".

Go back to the page: http://localhost/DVWA-master and press the "Create / Reset Database" button again.

You will have the login page that appears, log in using "**admin**" for Username and "**password**" for Password:



Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerabilities**, with **various levels of difficultly**, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerability** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections (so this can be seen as an extension for more advanced users)!

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

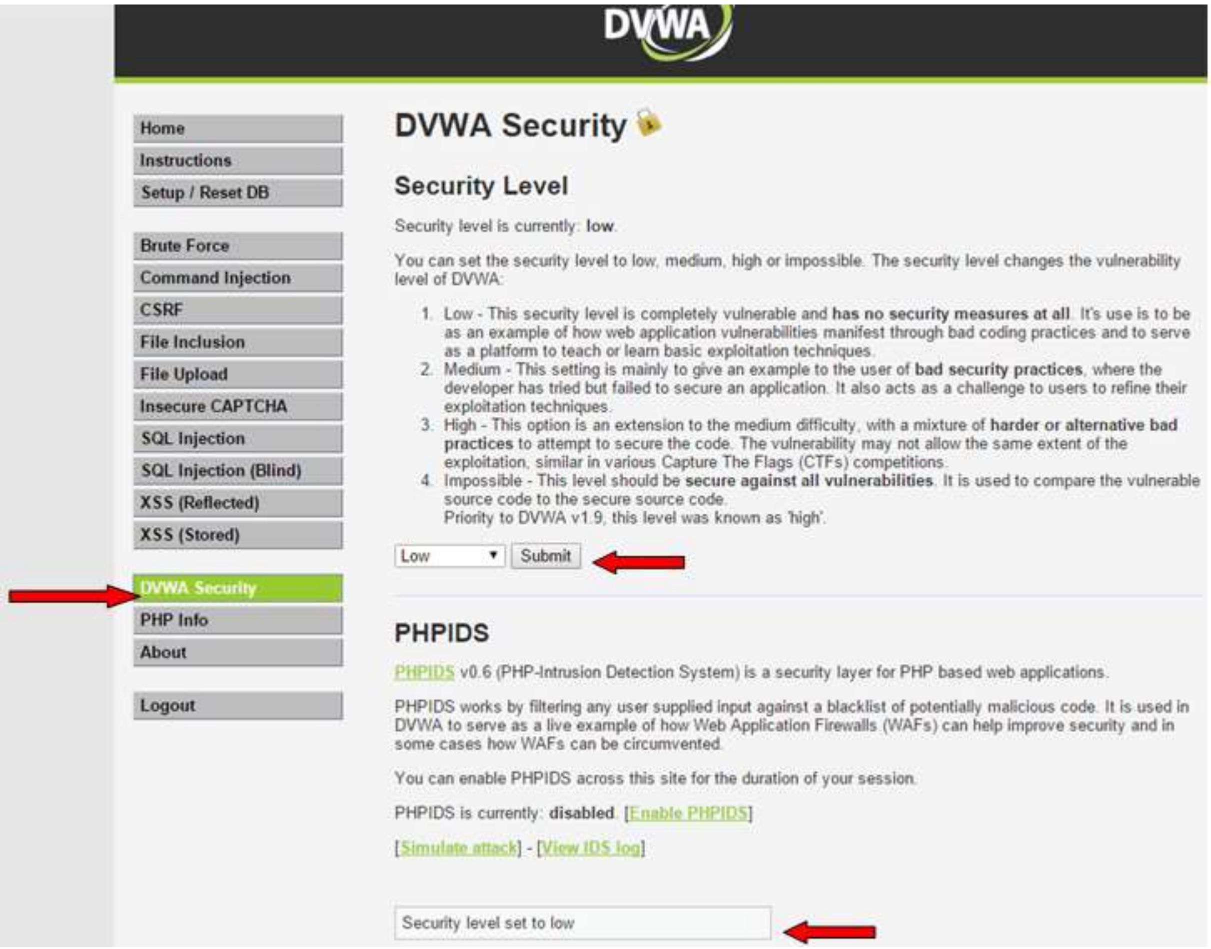
WARNING!

Damn Vulnerable Web Application is damn vulnerable! **Do not upload it to your hosting provider's public html folder or any Internet facing servers**, as they will be compromised. It is recommend using a virtual machine (such as VirtualBox or VMware), which is set to NAT networking mode. Inside a guest machine, you can downloading and install XAMPP for the web server and database.

Disclaimer

We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

Unless explicit indications, we will use the 'Low' security level of DVWA:



DVWA Security

Security Level

Security level is currently: **low**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
   Priority to DVWA v1.9, this level was known as 'high'.

Low ▾ Submit

PHPIDS

PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently: **disabled**. [Enable PHPIDS]

[Simulate attack] - [View IDS log]

Security level set to low

PART 3 - SQL injection What is a SQL Injection?

SQL injection (also known as SQL fishing) is a technique often used to attack data driven applications. This is done by including portions of SQL statements in an entry field in an attempt to get the website to pass a newly formed rogue SQL command to the database (e.g., dump the database contents to the attacker). SQL injection is a code injection technique that exploits a security vulnerability in an application's software.

The vulnerability happens when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

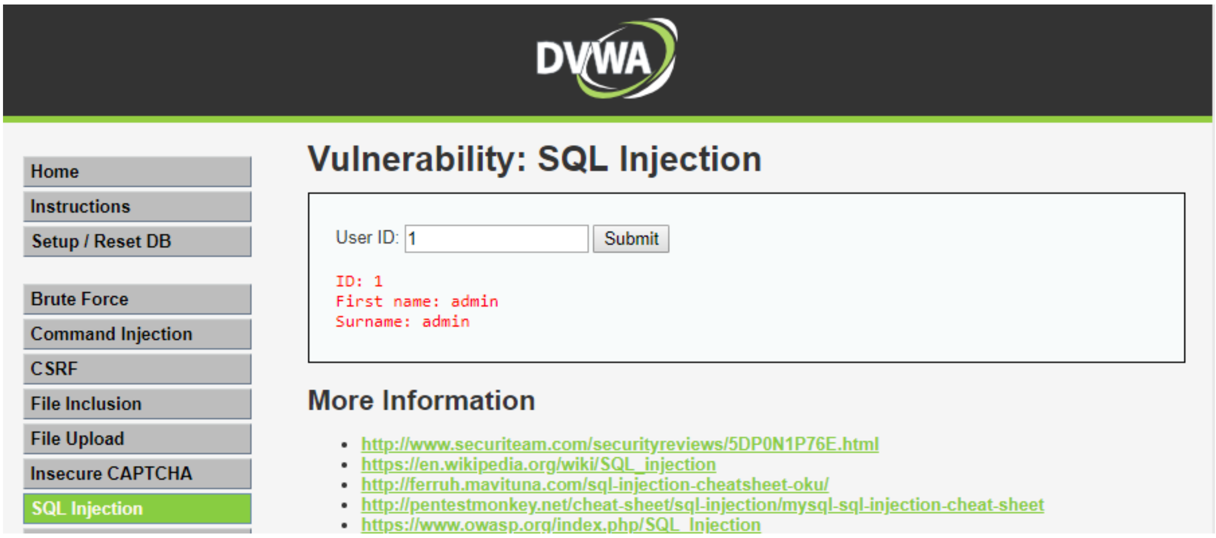
PART 4 - What is SQL Injection Harvesting?

SQL Injection Harvesting is where a malicious user supplies SQL statements to render sensitive data such as usernames, passwords, database tables, and more.

Basic Injection

Select "SQL Injection" from the left navigation menu.

- **Instructions**:
  1. Input "1" into the text box.
  2. Click Submit.
  3. Note, webpage/code is supposed to print ID, First name, and Surname to the screen.
- **Notes(FYI)**:
  1. Below is the PHP select statement that we will be exploiting, specifically $id.
  2. <CODE> $getid = "SELECT first_name, last_name FROM users WHERE user_id = '$id'"; </CODE>



Vulnerability: SQL Injection

User ID: 1

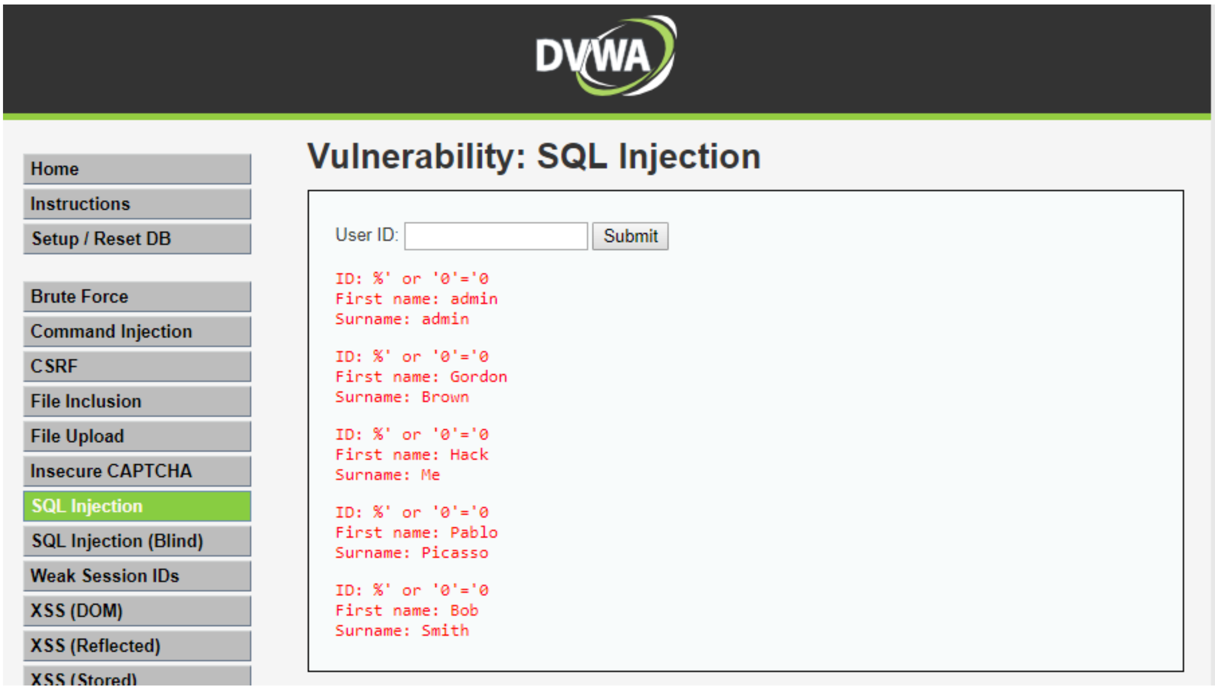
```
ID: 1
First name: admin
Surname: admin
```

More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_Injection

Always True Scenario

- **Instructions:**
  1. Input the below text into the User ID Textbox (See Picture).
     - %' or '0'='0
  2. Click Submit
- **Notes(FYI):**
  - In this scenario, we are saying display all record that are **false** and all records that are **true**.
    - %' - Will probably not be equal to anything, and will be false.
    - '0'='0' - Is equal to true, because 0 will always equal 0.
  - Database Statement
    - mysql> SELECT first_name, last_name FROM users WHERE user_id = '’%’ or ‘0’ =’0’;



Vulnerability: SQL Injection

```
ID: %' or '0'='0
First name: admin
Surname: admin

ID: %' or '0'='0
First name: Gordon
Surname: Brown

ID: %' or '0'='0
First name: Hack
Surname: Me

ID: %' or '0'='0
First name: Pablo
Surname: Picasso

ID: %' or '0'='0
First name: Bob
Surname: Smith
```