Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

SMESEC

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

D5.4 SMESEC Security Framework Assessment report

Document Identification			
Status	Final	**Due Date**	05/06/2020
Version	1.0	**Submission Date**	11/06/2020

Related WP	WP4, WP5	**Document Reference**	D5.4
Related Deliverable(s)	D5.3, D5.5	**Dissemination Level (*)**	PU
Lead Organization	IBM	**Lead Author**	Omri Soceanu (IBM)
Contributors	See list of contributors	**Reviewers**	Jose Francisco Ruiz (ATOS)
			Francisco Hernandez (WoS)

Keywords:
Trial, evaluation, testing, demonstrator, cybersecurity

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.

Document Information

List of Contributors	
Name	Partner
Francisco Hernández-Ramírez	Worldsensing
Olmo Rayón	Worldsensing
Maite García	Worldsensing
	EGM
	UU
Samuel Fricker	FHNW

Document History			
Version	Date	Change editors	Changes
0.1	22/04/2020	O. Soceanu	First draft
0.2	06/05/2020	O. Soceanu	Cost Analysis added and Survey Results updated
0.3	27/05/2020	O. Soceanu	Consolidating comments by EGM, WoS, UU
0.4	03/06/2020	O. Soceanu	Consolidating text by FHNW and adding WoS results
0.9	11/06/2020	O. Soceanu	After review
1.0	11/06/2020	ATOS	Quality review and submission to EC

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Omri Soceanu (IBM)	11/06/2020
Technical manager	-	-
Quality manager	Rosana Valle (ATOS)	11/06/2020
Project Manager	Jose Francisco Ruíz (ATOS)	11/06/2020

Table of Contents

List of Tables

List of Figures

List of Acronyms

Abbreviation / acronym	Description
ADC	Application Delivery Controller
API	Application Programming Interface
HTTP	Hypertext Transfer Protocol
IDS	Intrusion Detection System
OVH	Cloud Provider
OWASP	Open Web Application Security Project
SIEM	Security Information and Event Manager
SME	Small and Medium-sized Enterprises
T	Task
TaaS	Testing as a Service
TCO	Total Cost of Ownership
UX	User Experience
WP	Workpackage
ZAP	Zed Attack Proxy

Executive Summary

This deliverable belongs to WP5 *Refinement, Evaluation, Demonstration and Security Assessment of the SMESEC Platform in operational environment* whose ultimate objective is the unambiguous validation that the SMESEC security framework provides the required functionality specified at the beginning of the project by the use case partners and using the pilots as the main testbeds with the different versions of the SMESEC Framework developed in the project.

Using the results of surveys gathered from the open call of SMESEC and also open questionnaires completed by SMEs this document evaluates the performance of the SMESEC Framework and compares it to the requirements that were specified at the beginning of the project and described in D3.1 and D3.2. A socio-economic analysis is provided, and conclusions are drawn. As an initial conclusion extracted from the analysis the document shows that the SMESEC Framework meets all requirements of the use cases while, at the same time, lets some room for improvement in terms of ease of installation and configuration of the tools.

On the other hand, the deliverable also contains additional information of the pilots' status at M36 as an ad-hoc input which aims to provide how the SMESEC Framework is seen by the pilots' partners beyond the mere technical perspective. This last input wants to provide a clear overview of the gains provided by the new technology to the business and the day-to-day activity of the involved SMEs.

1 Introduction

1.1 Purpose of the document

The objective of WP5 "Refinement, Evaluation, Demonstration and Security Assessment of the SMESEC platform in operational environment" is: a) to evaluate if the new security framework developed within the preceding months provides the expected functionality in four representative application domains (e-voting, smart city, industrial services and smart grid) and b) to evaluate the results of the project in an open call.

This document makes up the core part of the deliverable D5.4 "SMESEC security framework assessment report", building upon the trail results collected in T5.3 as well as the collected results from the open call activities in T5.5. This helped us evaluate the SMESEC Framework in real-world environments. The document, therefore, provides a qualitative and quantitative assessment of the performance gains introduced by SMESEC in each SME pilot environment as well as the SMESEC Framework as a whole.

In this document we shall:

i) Qualitatively and quantitatively assess the performance gains of the deployed solution;
ii) Evaluate both the performance of the individual system modules and the integrated system;
iii) Analyse trial results against requirements of the project (e.g. technical, financial, etc.) and performance indicators;
iv) Extract lessons learned and recommendations;
v) Cost analysis. Based on the proposed case study for the four SME pilot domains a TCO analysis can be performed in order to evaluate the expected savings of the deployed solution. Particular scenarios will be defined, considering the automation level of the security assessment model and the usability of the solution (acceptance by the end-user community, cost differences and benefits between applications domains and optimal location and configuration of the security framework and components).

1.2 Relation to other project work

As explained above, this document provides an assessment and draws conclusions of the results collected in T5.3 as well as the collected results from the open call activities in T5.5.

The work described here will have an impact in the following work packages:

- WP3: the feedback of the testing will be used to finally refine the SMESEC Framework.
- WP6: the results of this deliverable will support the exploitation and dissemination activities.

1.3 Structure of the document

The document is structured around the following sections:

Chapter 1 is a general introduction and it presents the underlying rationale of the deliverable.

Chapter 2 Provides a qualitative and quantitative assessment of the performance gains of the deployed SMESEC Framework. It evaluates both the performance of the individual system modules and the integrated system.

Chapter 3 Analyzes trial results against technical requirements and performance indicators.

Chapter 4 Describes lessons learned and provides recommendations.

Chapter 5 Cost analysis: Based on the proposed case study for the four SME pilot domains, a TCO analysis can be performed in order to evaluate the expected savings of the deployed solution. Particular scenarios will be defined, considering the automation level of the security assessment model and the usability of the solution (acceptance by the end-user community, cost differences and benefits between applications domains and optimal location and configuration of the security framework and components).

Chapter 6 summarizes the overall conclusion of the document, identifying what has been achieved and the next steps to take the SMESEC to the next level.

2 Performance Evaluation

To assess the performance gains of the deployed SMESEC Framework we have used both results of tests reported in D5.3, results of the surveys of the SMEs of the open call and a public survey. For the public survey the SMESEC consortium has created a questionnaire to understand the exposure of SMEs to cyber threats and awareness of these SMEs and how to address them.
For the open call, the assessment of the SMEs was done using questionnaires tailored per SME type after they had the chance to work and test the SMESEC Framework.

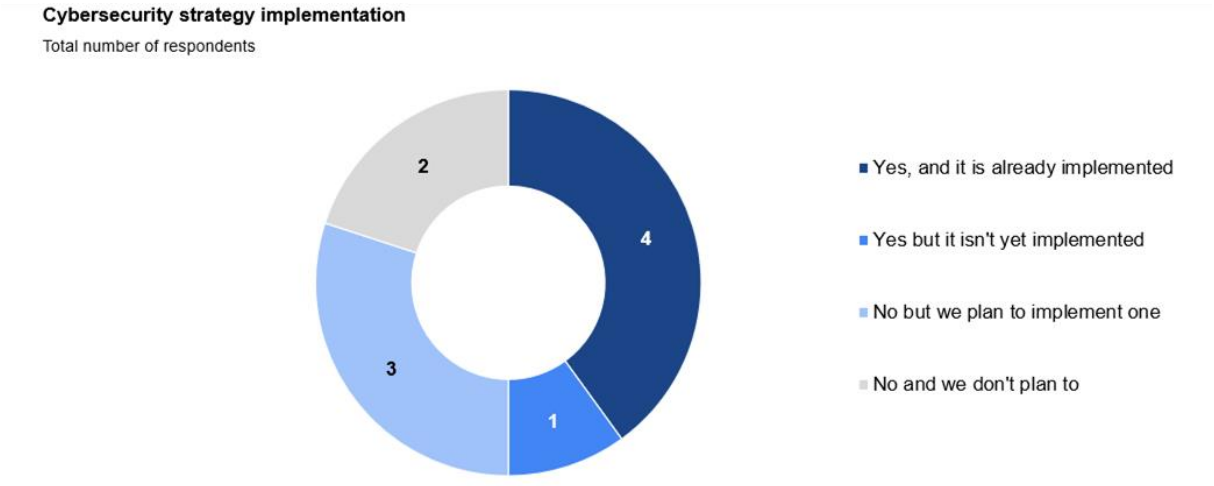
2.1 Cyber-Security Challenges, Priorities and Experience

Before diving into the responses of the surveyed parties regarding their experience with the SMESEC Framework, we will first discuss the challenges the different SMEs face regarding cybersecurity, their priorities and their experience with different cyber-attacks.

Nineteen SMEs responded to the survey. For most companies' respondents were from top positions within the organization. About 40% were CEOs and approximately 30% were CTOs or technical managers. Scales are detailed in the title of each figure, most on a range of 1-5. All respondents but one answered that they were responsible for the cybersecurity of their respective company. Nevertheless, less than half said they received training in the field of cybersecurity.

As can be seen in Figure 1, almost half of the respondents have already implemented a cybersecurity strategy but just as many are yet to implement one.

Figure 1 Cybersecurity Strategy Implementation

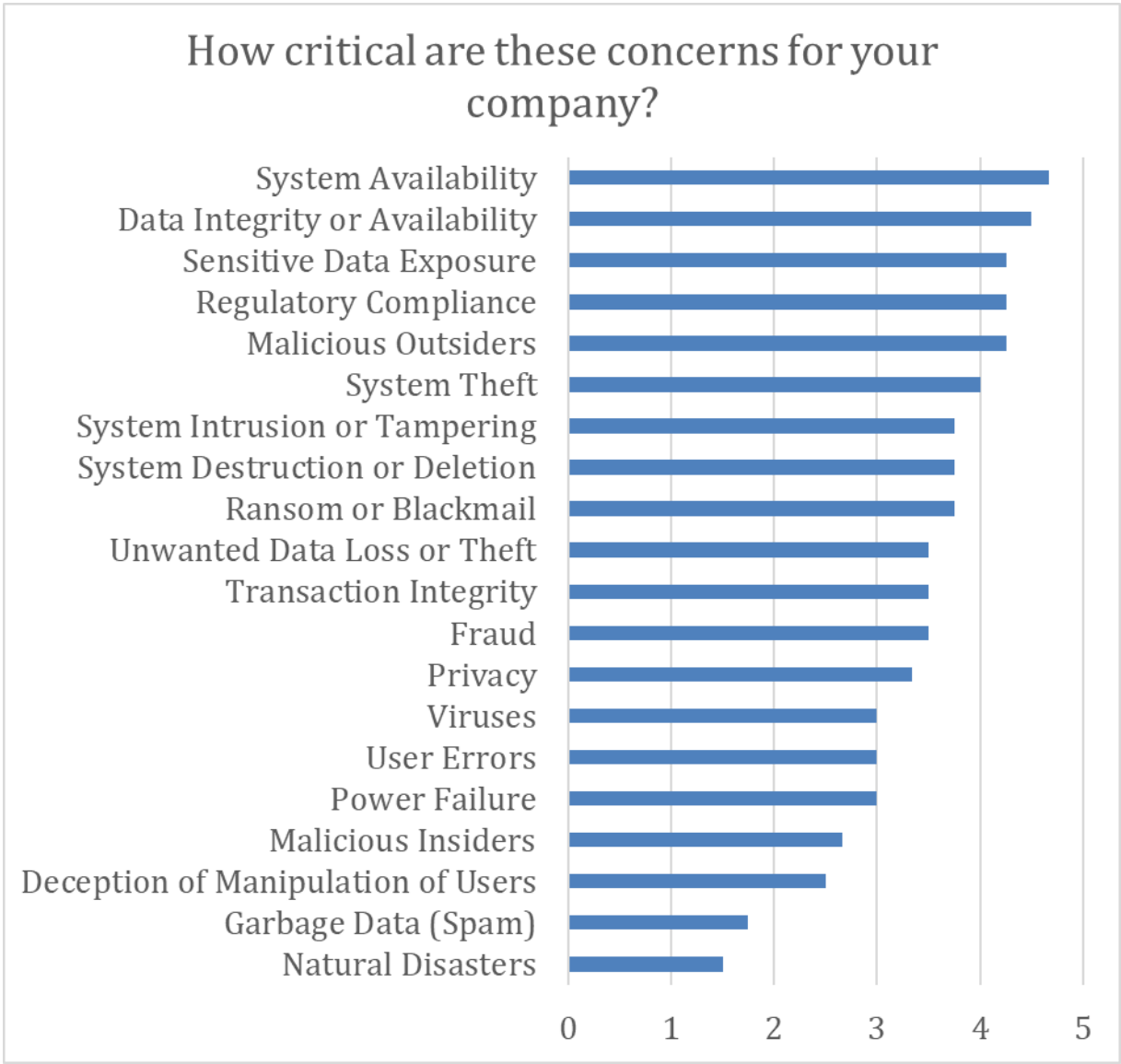


Concerns

Survey participants were asked, "How critical are these concerns for your company?" regarding different threats (both Malicious Cyber-Security Threats, Physical and Non-Malicious Maintenance issues) Below are the results for both the public questionnaire and SMEs of the open call.

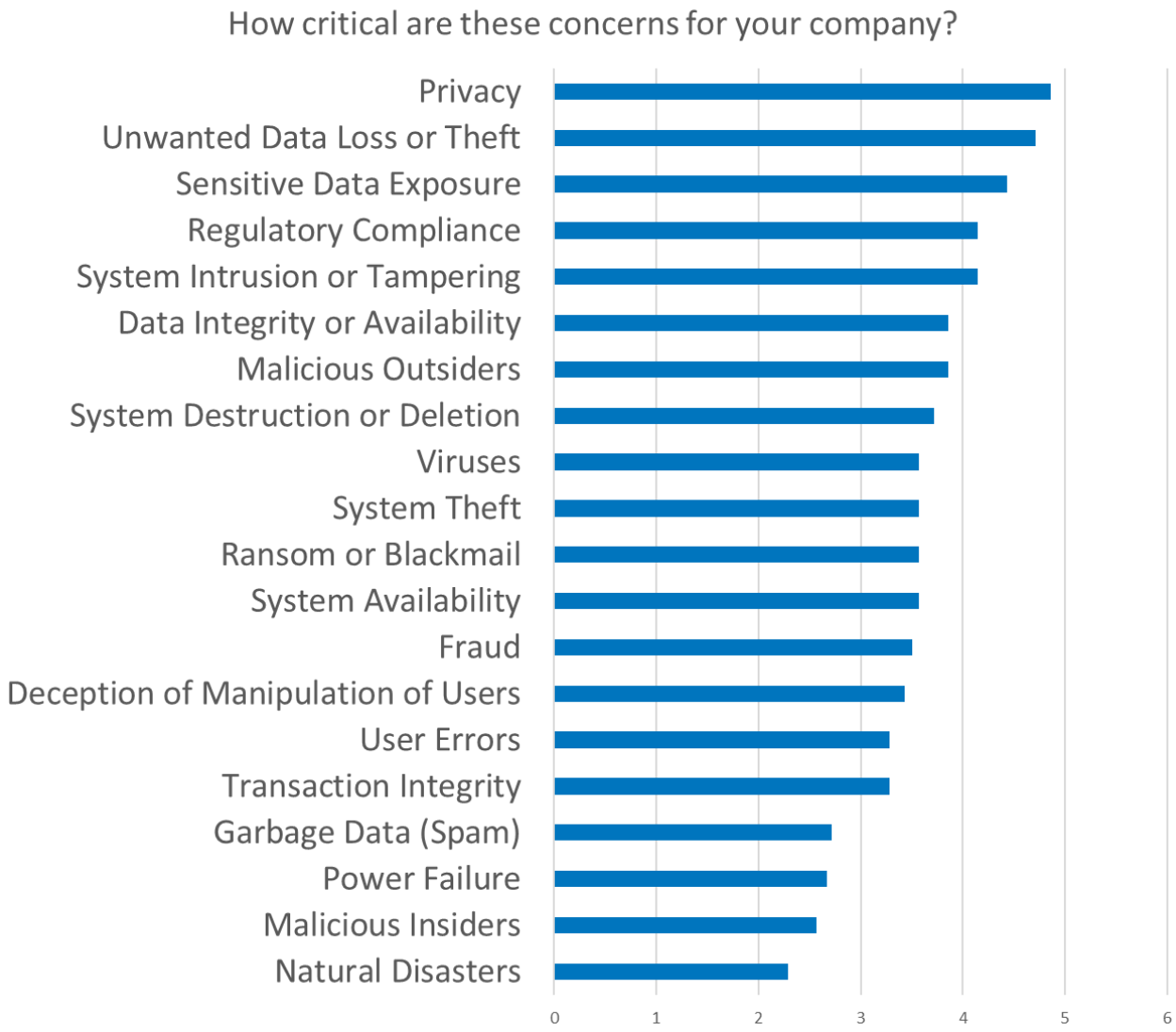
Public questionnaire results (X – axis represents mean of ranking in a scale of 1-5):

Figure 2 How Critical are these concerns for your company – Public



Open Call SMEs questionnaire results (X – axis represents mean of ranking in a scale of 1-5):

Figure 3 How Critical are these concerns for your company - Open Call SMEs

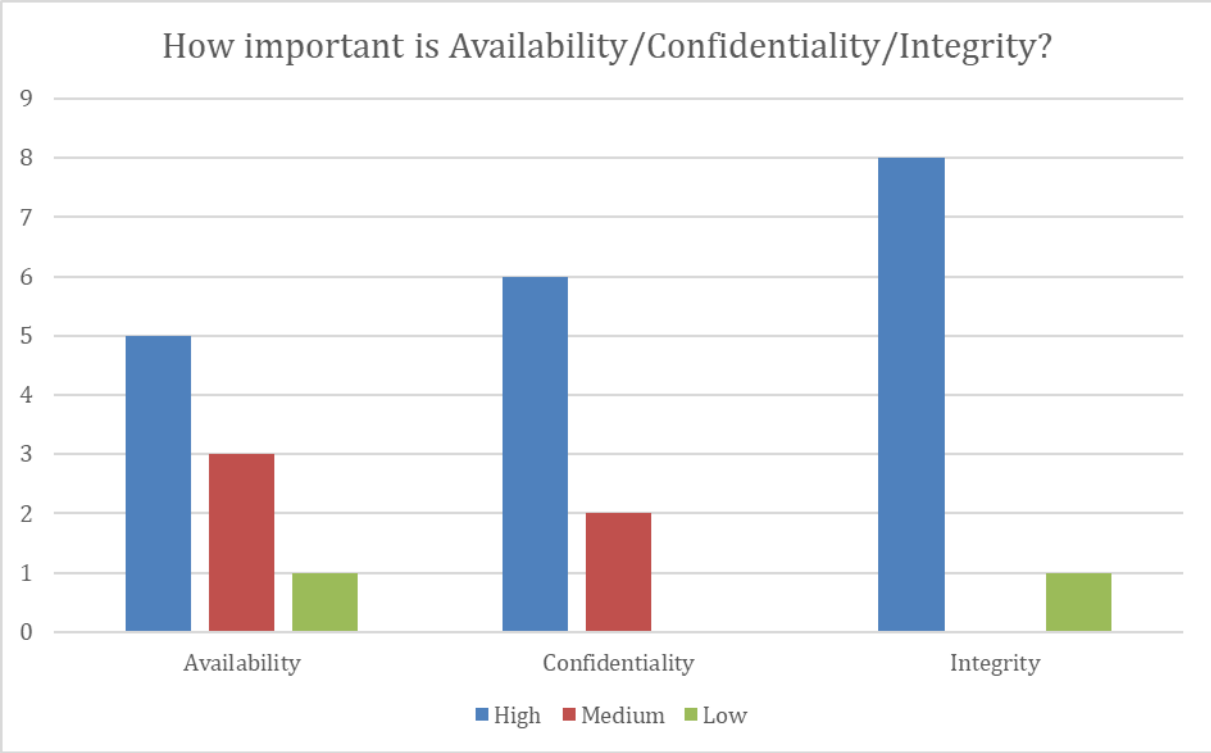


Availability vs. Confidentiality vs. Integrity

Survey participants were asked, "How important is Availability/Confidentiality/Integrity?" Below are the results for both the public questionnaire and SMEs of the open call.

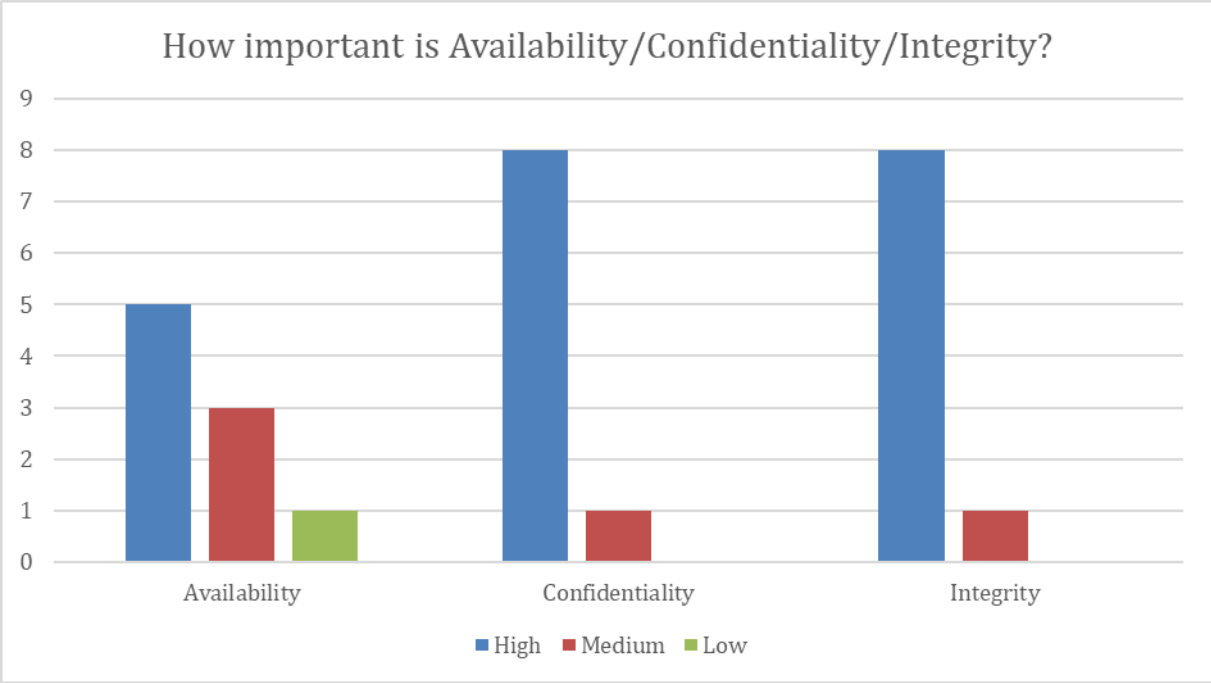
Public questionnaire results (Y – axis represents mean of ranking in a scale of 1-10):

Figure 4 How important is Availability/Confidentiality/Integrity? - Public



Open Call SMEs questionnaire results (Y – axis represents mean of ranking in a scale of 1-10):

Figure 5 How important is Availability/Confidentiality/Integrity? - Open Call SMEs



Note that again, we can see that Data Confidentiality is much more of a concern to the Open Call SMEs. At this point, we can hypothesize that the surveying companies that joined the Open Call of SMESEC

have an inherent bias and that companies that are more ignorant of confidentiality issues might not see the value and would not join the Open Call. This is also backed by the fact that about 60% of the public survey respondents didn't have training in cyber security compared to 40% of the Open Call SMEs.

Experience with Cyber-Attacks

Survey participants were asked, "What cyber-attacks or data breaches did your company experience in the past 12 months?"
We separated this question into three categories:

- Severe attacks (threat to your operations)
- Moderate attacks (requiring dedicated attention)
- Mild attacks (without significant impact)

Below are the results for both the Public questionnaire and Open Call SMEs.

Public questionnaire results (Y – axis represents number of respondents that answered accordingly):

Figure 6 What cyber-attacks or data breaches did your company experience in the past 12 months? - Severe Attacks – Public

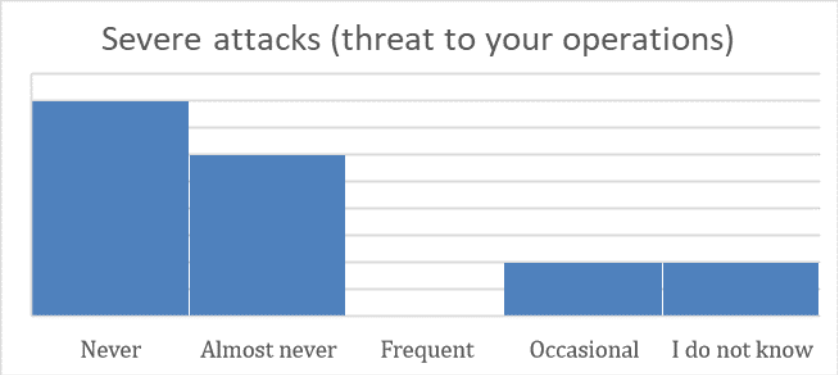


Figure 7 What cyber-attacks or data breaches did your company experience in the past 12 months? - Moderate Attacks – *Public*

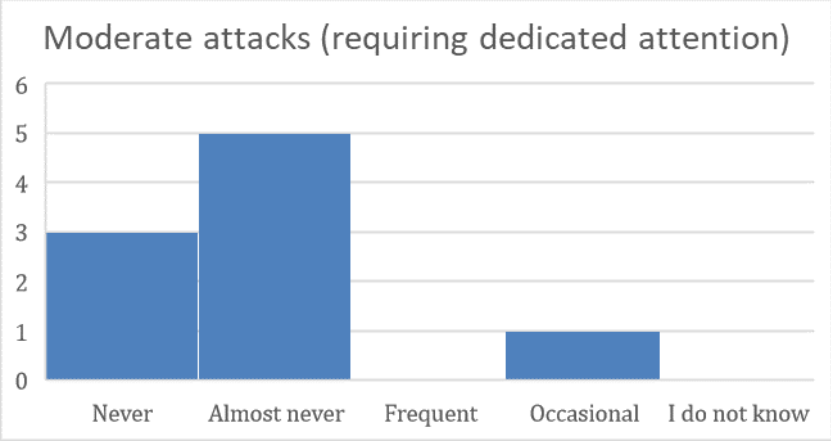
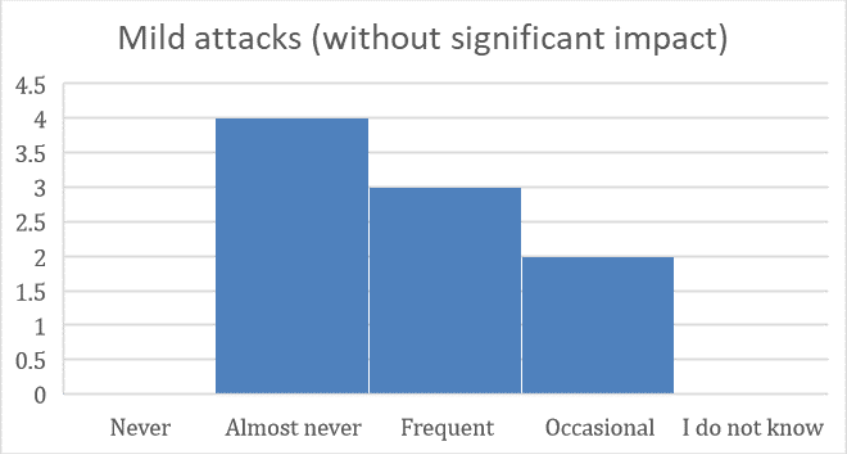


Figure 8 What cyber-attacks or data breaches did your company experience in the past 12 months? - Mild Attacks – Public



Open Call SMEs questionnaire results (Y – axis represents number of respondents that answered accordingly):

Figure 9 What cyber-attacks or data breaches did your company experience in the past 12 months? - Severe Attacks - Open Call SMEs

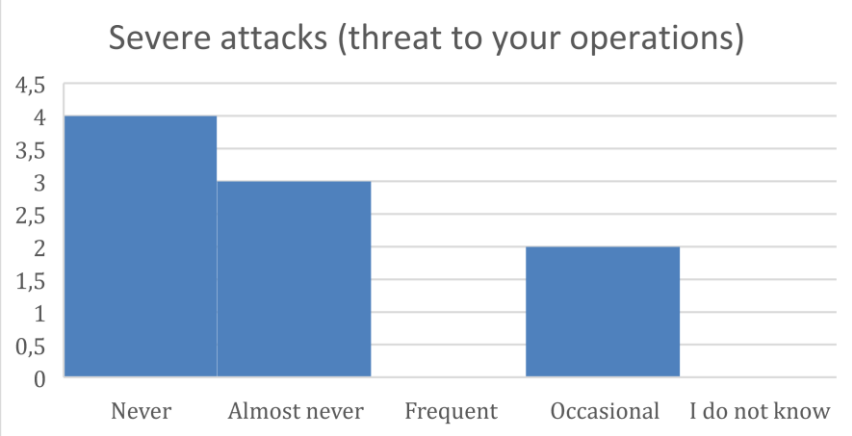


Figure 10 What cyber-attacks or data breaches did your company experience in the past 12 months? - Moderate Attacks - Open Call SMEs

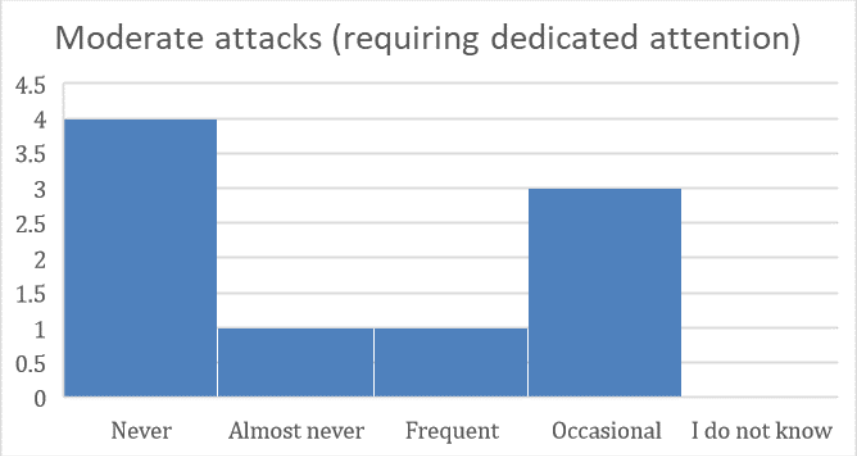
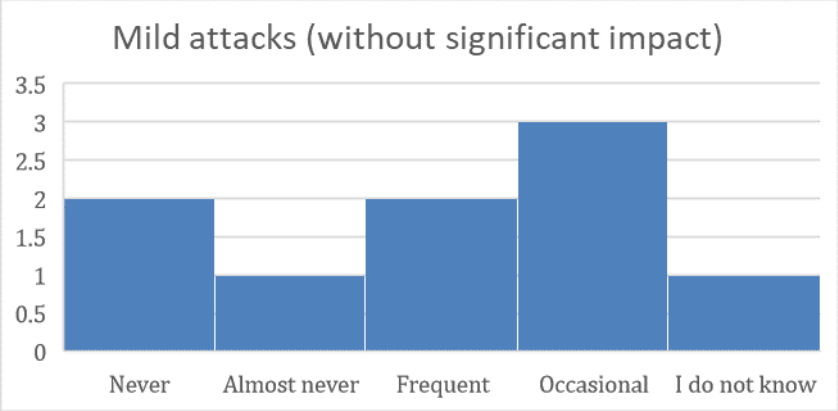


Figure 11 What cyber-attacks or data breaches did your company experience in the past 12 months? - Mild Attacks - Open Call SMEs



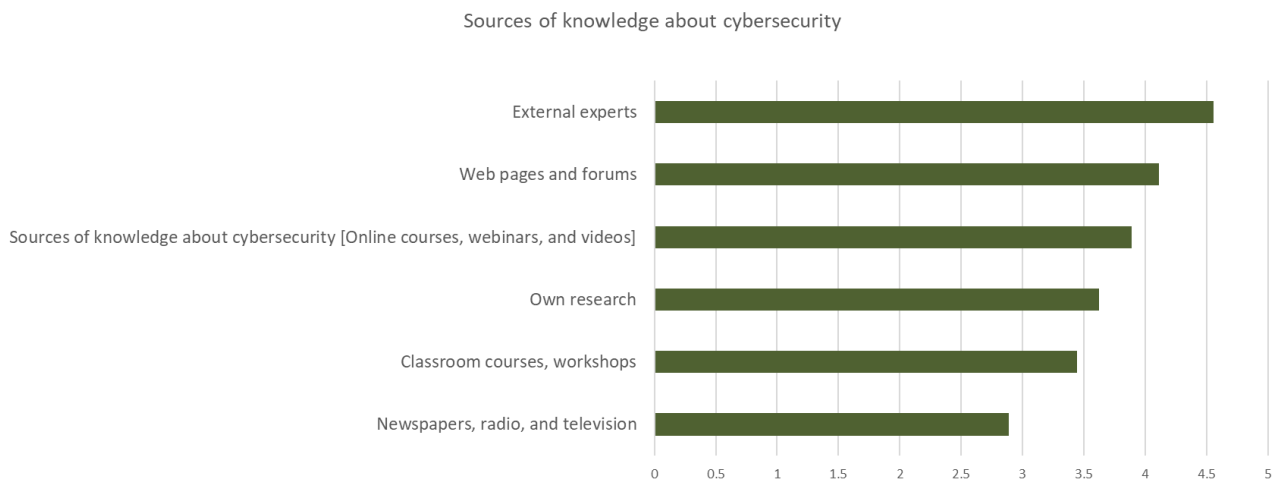
Two major insights can be drawn from these charts. The first insight concerns the "I don't know" answers. One of the biggest challenges of cybersecurity is the limited awareness to cyber-attacks. Even with all the cybersecurity tools money can buy, one can never have complete certainty that their company is not under attack. However, since mild attacks are generally quite frequent, ranging from port scanning to generic phishing attempts, lack of awareness that at least at some level they are occurring demonstrates the absence of even the most basic security tools. This is true to both the "I do not know", "Never" and "Almost never answers". The second insight is that there are companies that have testified to having "Occasional" moderate and even severe cyberattacks. This result is quite alarming for these companies. By their own account, a threat to operations is a day-to-day reality.

Sources of Knowledge about Cyber-Security

Survey participants were asked, "What are your Sources of Knowledge about Cyber-Security?"
Below are the results for both the public questionnaire and SMEs of the open call.

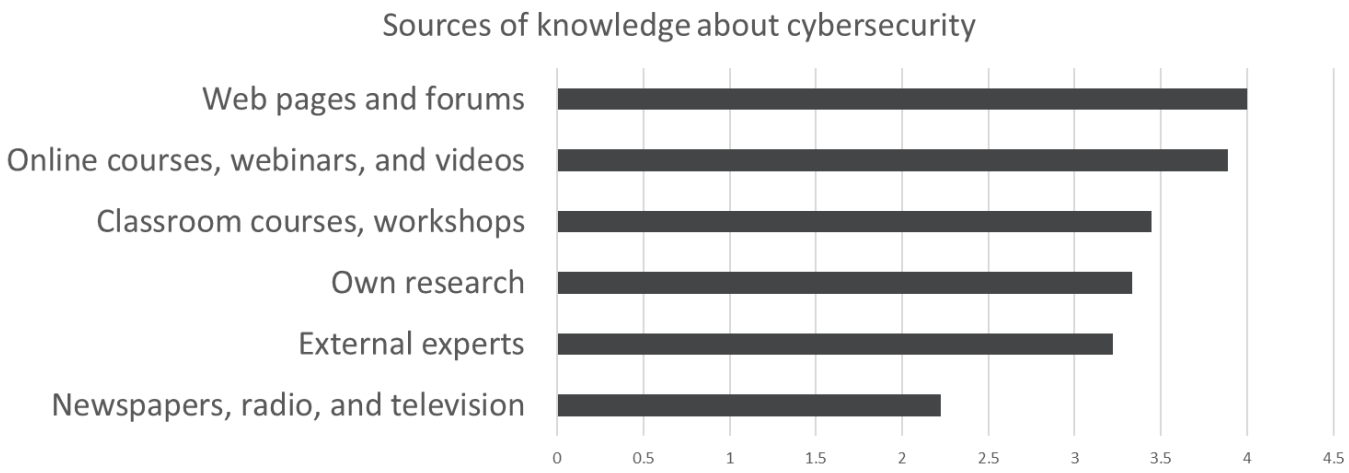
Public questionnaire results (X – axis represents mean of ranking in a scale of 1-5):

Figure 12 Sources of Knowledge about Cyber-Security – Public



Results of the questionnaire of the SMEs of the open call (X – axis represents mean of ranking in a scale of 1- 5):

Figure 13 Sources of Knowledge about Cyber-Security – Open Call SMEs



Note that the public respondents rely much more on external experts then their Open Call SMEs counter parts.

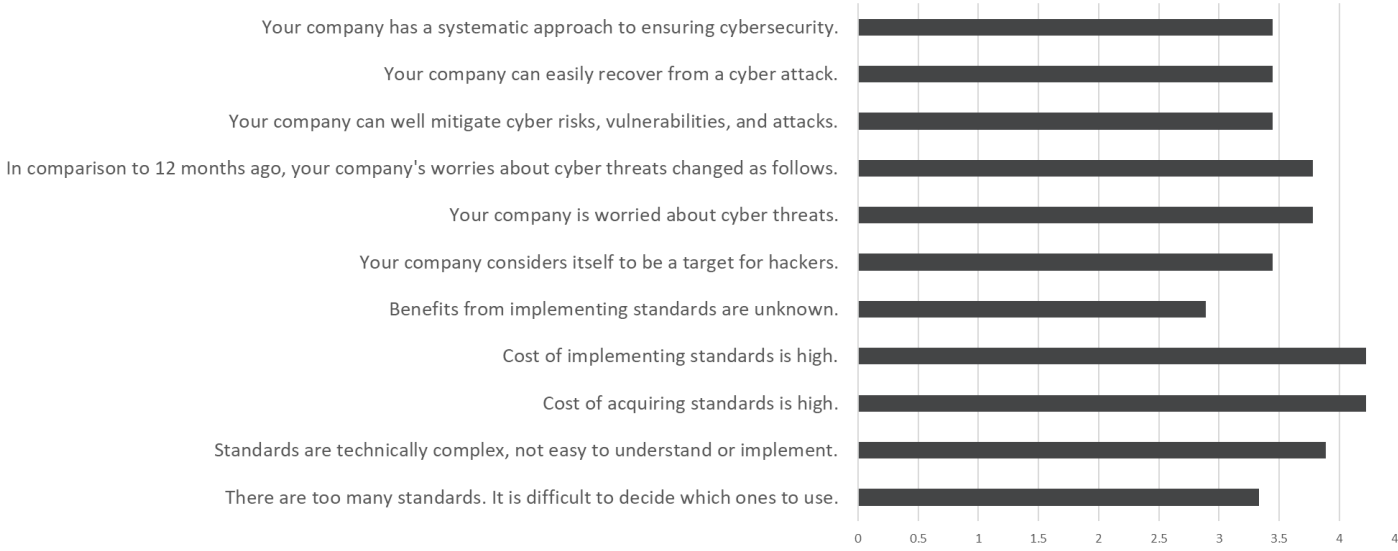
Cyber-Security Challenges

Survey participants were asked an array of questions to gage the attitude and challenges of the different companies towards cybersecurity.

Below are the results for both the public questionnaire and Open Call SMEs.

Public questionnaire results (X – axis represents mean of ranking in a scale of 1- 5):

Figure 14 Cyber-Security Challenges – Public



Open Call SMEs questionnaire results (X – axis represents mean of ranking in a scale of 1- 5):

Figure 15 Cyber-Security Challenges - Open Call SMEs-

It seems from the answers to the survey that there is a lack of understanding as to why it is important to follow standards and what they are required. Combined with the general feeling that adhering to these standards is quite costly, one can assume that standards might not be fully followed by the companies. At the same time, companies are quite worried about cyber threats and believe they are the target of hackers.

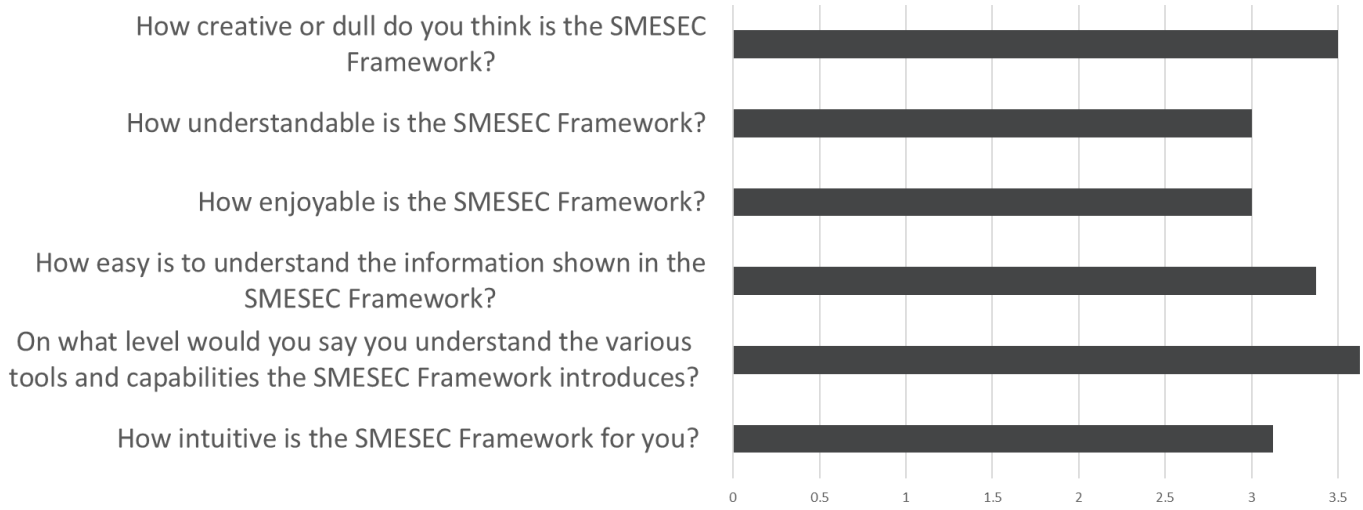
2.2 SMESEC Framework Experience

Next we assessed the general user experience working with the SMESEC Framework among the Open Call SMEs.

Understandability

Below are a series of questions that were posed to the survey participants (X – axis represents mean of ranking in a scale of 1- 5):

Figure 16 SMESEC Security Framework User Experience



Participants were asked: "What is the cumulative number of hours you spent on learning using the SMESEC Framework as a Framework?" The average amount of hours was **54 hours**. However, the standard deviation was quite high – 41, meaning that the answers vary from a few hours to several weeks.

For the question: "What is the cumulative number of hours you spent on learning using the relevant tools that the SMESEC Framework provides?" The average amount of hours was **86 hours**. However, like in the previous question, the standard deviation was quite high - 81.

Participants were also asked "Is the information shown in the main interface the one expected and is it useful?" about **88% of participants answered 'Yes'**. For the question: "Is it understandable the objective (information shown) in each of the tabs?" **All participants answered 'Yes'**

To the question: "Do you think the SMESEC Framework is easy or difficult to learn?" only **55%** said it was easy.

In conclusion, survey results show a moderate attitude towards the Frameworks understandability.

Usability

In order to assess usability, the following questions were asked:

- Do you think the SMESEC Framework provides valuable information? **100%** answered 'Yes'.
- Would you describe the user interface of the SMESEC Framework as boring or exciting? **75%** answered 'exciting'.
- Do you think the SMESEC Framework is fast or slow for providing information? **77%** answered 'fast'.
- Would you describe the SMESEC Framework as supportive or obstructive? **88%** answered 'supportive'.
- Is it easy or complicated to use? **63%** answered 'easy'.
- Do you think it is pleasing to the eye or unlikable? **88%** answered 'pleasing'.
- Due to the information it provides is it motivating or demotivating? **88%** answered 'motivating'.
- Does it meet your expectations? **75%** answered 'Yes'.
- Would you describe it as efficient or inefficient? **77%** answered 'efficient'.
- The information provided is clear or confusing? **88%** answered 'clear'.
- Do you think the SMESEC Framework is practical or impractical? **75%** answered 'practical'.
- Do you think the information of the SMESEC Framework is organized or cluttered? **75%** answered 'organized'.
- Are the functionalities of the SMESEC Framework friendly or unfriendly? **88%** answered 'friendly'.
- Do you think the SMESEC Framework is conservative or innovative? **71%** answered 'conservative'.
- On what level would you say that the SMESEC Framework meets your requirements? The average score was - 3.3

The above results show a general positive attitude towards the SMESEC Framework usability as a whole. Specifically, the information that is presented is valuable and clear. This result, in the context of the lack of understanding of cybersecurity standards, is especially important.

Functionality

In order to assess whether the SMESEC Framework as a whole met the needs of the participants, the following questions were asked:

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

  Here answers were quite diverse, ranging from firewall capabilities, SMS/Email alerts, and support of external tools.

- Which tool(s) that currently are not part of the SMESEC Framework, if any, would you want to see in the SMESEC Framework in the future?

Like in the previous question answers were quite diverse, again mentioning firewalls as well as tools such as penetration tools and cloud management of Windows Networks.

- How could we improve the SMESEC Framework to better meet your needs?

Most respondents pointed to the process of installation and integration of the components into small company infrastructure. They have described what can also be seen in the integration and installation section, that the difficulty of configuration setup is too complex for a SMEs and requires some IT expertise not always available in non-tech companies.

In general, it seems that users want more capabilities such as firewall tools while asking for a better installation experience.

Integration and Installation

In order to assess the ease of installing and integrating the SMESEC Framework the following questions were asked:

- Did you have to do any adjustments to your products/deployment methods in order to be able to integrate with the SMESEC Framework, or any of its tool? **30%** Reported that they needed to make adjustments.
- Is any of the clients/agents affecting the performance of your system? **33%** reported it affected the performance of their system
- Is any of the clients/agents non-compatible with your system? **66%** reported non-compatibility issues.
- Was any of the agents/clients identified as a possible threat/warning in your system? **Only 1** participant reported reports of a possible threat.
- How satisfied are you with the overall process for installing/configuring? Average satisfaction with the installation process was **1.8.**

The above results show that there is yet much room for improvement with the installation process.

2.3 Evaluation of individual system modules

For each of the system modules, we've asked the participants of the open call to rate the level of complexity to install, configure and use the component. Below are the question and results:

XL-SIEM

- How complex is to install the agent of the XL-SIEM? Average complexity with the installation process was **4.2**
- How complex is to configure the agent of the XL-SIEM in your system? Average complexity with the configuration process was **3.6**

- How complex is to uninstall/remove the agent of the XL-SIEM from your system?
  Average complexity with the removal process was **2.4**
- What do you think is the level of expertise required for managing (e.g. install, configure, etc.) it?
  Average level of expertise was **3**
- How useful were the instructions (e.g. documentation, videos) for installing/configuring the XL-SIEM?
  Average usefulness score was **2.8**
- Did you have to prepare your system before installing the clients/agents? **80%** reported '**Yes**'
- How much time (in hours) did you need for installing and configuring? On average **30.25 Hours**
- Did you have to update/install additional software for installing a component? **100%** reported '**No**'

It seems that installation and configuration were too complex for the average SME installation and configuration were quite difficult, while usage didn't require high technical skills.

Honeypot

- How complex is to install the agent of the Honeypot?
  Average complexity with the installation process was **4**
- How complex is to configure the agent of the Honeypot in your system?
  Average complexity with the configuration process was **4**
- How complex is to uninstall/remove the agent of the Honeypot from your system?
  Average complexity with the removal process was **2.7**
- What do you think is the level of expertise required for managing (e.g. install, configure, etc.) it?
  Average level of expertise was **3**
- How useful were the instructions (e.g. documentation, videos) for installing/configuring the Honeypot?
  Average usefulness score was **3**
- Did you have to prepare your system before installing the clients/agents? **1** Participant answered '**Yes**'
- How much time (in hours) did you need for installing and configuring? **13.3 Hours**
- Did you have to update/install additional software for installing a component? **100%** reported '**No**'
  If yes, what software and for what solution?

It seems that installation and configuration were too complex for the average SME installation and configuration were quite difficult, while usage didn't require high technical skills.

BitDefender

- How complex is to install the agent of the BitDefender?
  Average complexity with the installation process was **2**
- How complex is to configure the agent of the BitDefender in your system?
  Average complexity with the configuration process was **2.7**
- How complex is to uninstall/remove the agent of the BitDefender from your system?
  Average complexity with the removal process was **1.7**
- What do you think is the level of expertise required for managing (e.g. install, configure, etc.) it?
  Average level of expertise was **3**
- How useful were the instructions (e.g. documentation, videos) for installing/configuring the BitDefender?
  Average usefulness score was **3**
- Did you have to prepare your system before installing the clients/agents? **1** Participant answered '**Yes**'
- How much time (in hours) did you need for installing and configuring? **4 Hours**
- Did you have to update/install additional software for installing a component? **100%** reported '**No**'
  If yes, what software and for what solution?

It seems that BitDefender had a high usability score with low complexity scores for installation, configuration and level of expertise for use.

NetScaler

Only a single participant used NetScaler, here are the company's answers:

- How complex is to install the agent of the NetScaler?
  Complexity with the installation process was **5**
- How complex is to configure the agent of the NetScaler in your system?
  Complexity with the configuration process was **5**
- How complex is to uninstall/remove the agent of the NetScaler from your system?
  Complexity with the removal process was **5**
- What do you think is the level of expertise required for managing (e.g. install, configure, etc.) it? **Very High**
- How useful were the instructions (e.g. documentation, videos) for installing/configuring the NetScaler?
  Usefulness score was **1**
- Did you have to prepare your system before installing the clients/agents? **Yes**
- How much time (in hours) did you need for installing and configuring? **8 hours**
- Did you have to update/install additional software for installing a component?
  If yes, what software and for what solution? **Yes, netscaler VM**

It seems that NetScaler had a very low usability score with high complexity scores for installation, configuration and high level of expertise required for use.

CYSEC

CYSEC was used by all four SMESEC use case SMEs. During the piloting feedback was provided by this use cases. These problems were analysed and resolved. We focus here on the resolution of reported software quality problems. Impact evaluation of the content provided by CYSEC is reported in D3.6 for the SMESEC use case SMEs and in D5.5 for the SMESEC open call SMEs.

During early validation of CYSEC, the SMESEC use case SMEs reported problems related to login, availability, and stability of the CYSEC tool. These problems appeared when CYSEC was accessed by the human end-user through the web interface of the SMESEC Hub. Root-cause analysis indicated that the problems were due to the use of OAUTH that was inconsistent between CYSEC and the SMESEC Hub and lack of availability monitoring of the CYSEC SaaS.

Resolution 1: FHNW and ATOS agreed to the support of OAUTH Bearer-Tokens for authentication and authorisation. Interoperability tests were performed and confirmed viability of the solution.

Resolution 2: FHNW has setup continuous monitoring of the CYSEC cloud instance and established procedures to ensure >95% uptime.

A second area of reported problems concerned loss of data recorded by the end-user during the work with the CYSEC coaches and instability of the progress KPI over long term. Root-cause analysis showed that the problems were due to evolutionary updates of the CYSEC tool and coaches provided by FHNW to account for lessons-learned in the piloting of CYSEC. No data was lost. Instead, loss was perceived due to changes in questions, recommendation rules, and formulas for calculating the KPIs.

Resolution 3: FHNW has stabilised the questions, recommendation rules, and KPI formulas in the open-sourced major version of CYSEC released at the end of May 2020. The stability will avoid the reported perceived losses of data.

A third area of reported problems were related to the deployment and installation of the on-premises version of CYSEC (as opposed to the standard SaaS version integrated into the SMESEC framework). Root-cause analysis showed that the problems were due to the quality of documentation.

Resolution 4: FHNW has improved the documentation as part of open sourcing the CYSEC release of May 2020.

3 Analysis of Requirements Against Results

Functional Requirements

The functional requirements identified In D3.1 for SMESEC Framework were broken into two main categories: threat defence and security management.

The threat defense includes the following functional requirements:

- Protect the SME infrastructure from adversary's attacks.
- Detect adversary's attacks on the SME infrastructure.
- Monitor the SME infrastructure.
- Alert when an attack on the SME infrastructure is detected.
- Respond to adversary's attacks on the SME infrastructure.
- Discover vulnerability in the SME infrastructure.

The security management requirements include:

- Provide assessment of security level.
- Provide suggestions for improving security level.
- Provide evaluation of security risk and consequences.
- Provide assessment of criticality.

Objective qualitive results described in D5.3 and D5.5 show that the SMESEC Framework meets all functional requirements with high marks, providing both comprehensive threat defense, as well as, good security management.

Non-Functional Requirements

The non-functional requirements identified for the SMESEC Framework fall into the following categories:

- Modularity of Deployment – The SMESEC Framework must allow modular deployment of SMESEC security solutions at the SME's system.
- Modularity of Development – The SMESEC Framework must allow modular development of SMESEC tools.
- Confidentiality – The SMESEC Framework must allow governance of SME data and allow SME to decide the level of confidentiality of the data collected by the SMESEC Framework and tools.
- Usability – The SMESEC Framework should meet high usability standards and offer a unified interface for all tools included in the SMESEC Framework.
- Scalability – The SMESEC Framework must allow load scalability, multi-tenancy, and easy expansion of the framework.

For all 'binary' non-functional requirements, the final SMESEC framework completely meets the requirements as described in past deliverables. Regarding Usability, since the requirement is more subjectively measured, we will rely upon the Survey cited in this report. As discussed earlier most components received a high usability scores and generally positive reviews. Nevertheless, installation and configuration were pain points for most users and for most components. This is also true to the

SMESEC Framework as a whole. In the tables below, one can observe the coverage of business and platform requirements, as well as, detection capabilities of the different tools in the SMESEC platform.

Table 1: Requirements vs. Fulfilment – business and platform requirements

Business-and Platform requirements	Required	Was the requirement met?									
		XL-SIEM	GravityZone	Citrix ADC	EWIS Honeypot	CY SEC	TaaS	Anti ROP	Angel Eye	Expli SAT	Cloud-IDS
Availability	✓				V		V	V	V	V	
Usability	✓		V								V
Privacy	✓	V			V		V				
Cost	✓										
Alerting	✓						V				
Scalability	✓		V		V	V	V	V	V	V	V
System integrity	✓			V		V		V	V	V	V
Confiden-tiality	✓	V	V		V		V				V
Non-repudiation	✓	V		V	V	V	V				
Authen-tication	✓	V			V		V	V	V	V	V

Table 2: Requirements vs. Fulfilment - detection capabilities

Protection capabilities	Required	Was the Requirement met?									
		XL-SIEM	Gravity Zone	Citrix ADC	EWIS Honeypot	CYSEC	TaaS	Anti ROP	Angel Eye	Expli SAT	Cloud - IDS
Web application servers	✓	V			V	V	V	V	V	V	
Database servers	✓	V			V	V	V	V	V	V	
Network traffic	✓		V		V	V	V	V	V	V	
Web servers	✓	V			V	V	V	V	V	V	
Email servers	✓	V			V	V	V	V	V	V	
DDoS	✓		V		V	V	V	V	V	V	
Access abuse	✓		V			V					
Software misuse	✓	V		V		V					
Zero-day attacks	✓			V	V	V	V				V
Code injection	✓	V	V	V	V	V	V				V
Man-in-the-Middle attacks	✓	V	V	V	V	V	V				V

4 Conclusion of the analysis of SMEs

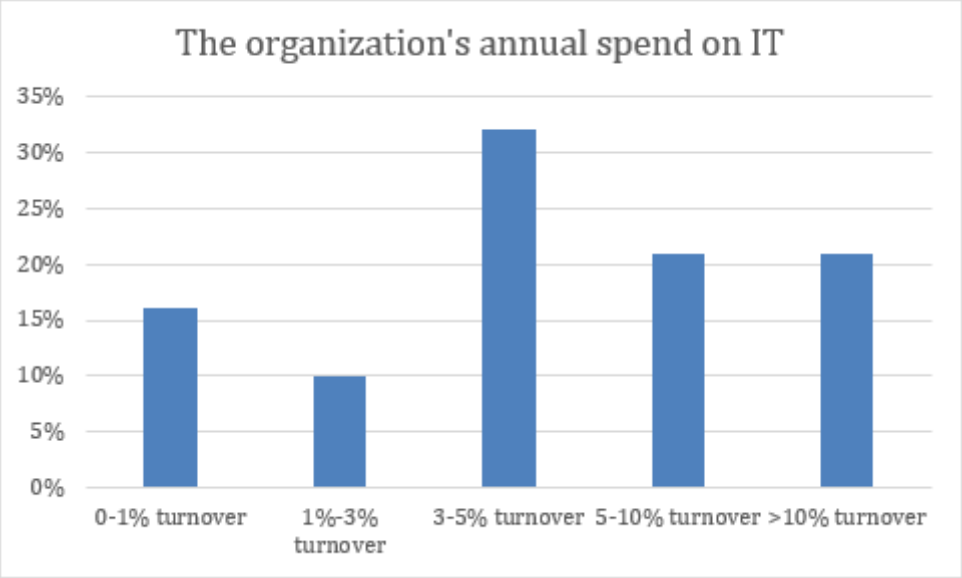
Cyberattacks are a top concern for many SMEs. Nevertheless, due to their size they often lack skilled personnel that are able to effectively handle some of the challenges of building and maintaining an effective cybersecurity defence. This is evident throughout the survey responses. Hence, beyond its effectiveness and functional requirements, the requirement of usability holds an especially significant role. Without it, no matter what the success rate in mitigating threats is, the tool will never be used.

Usability is measured at different points in the software lifecycle. From installation, through configuration to actual operational use and finally removal. From the quantitative tests in D5.3 and D5.5 and the subjective survey responses, it seems that the SMESEC Framework gets high marks for functional and non-functional requirements. As for usability, once installed and configured users tend to be able to handle the operation well and with ease. However, the installation and configuration process is still a pain point that is yet to be solved. We would recommend relying on external experts for the initial installation and configuration in cases where the local team is unable to handle the complexity level. In addition, we recommend, in future work, to improve the usability in order to allow SMEs to perform the whole process independently of outside assistance.

5 Cost Analysis

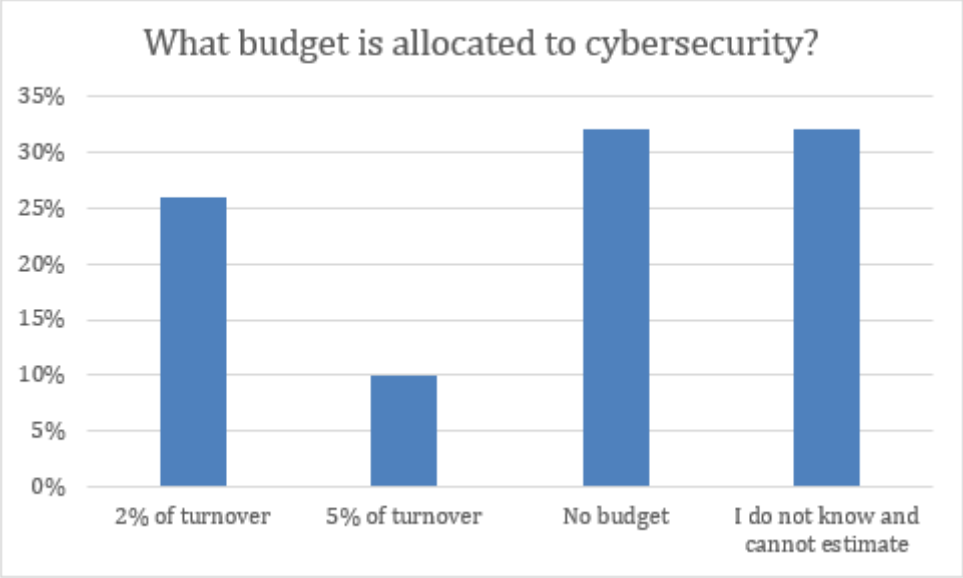
As evident from the results in sub-section 2.1, cybercecurity is on the minds of most CEOs in our survey. It is therefore interesting to see how much they are willing to allocate for it. First, we asked respondents about the percentage of their turnover allocated to their IT needs in general.

Figure 17 How much of your company's turnover is allocated to IT?



We then asked respondents "How much of your company's turnover is allocated to cybersecurity"

Figure 18 How much of your company's turnover is allocated to cybersecurity?



Viewing the amounts allocated to cybersecurity in light of the amounts allocated annually to IT, one can conclude that the notion that Cybersecurity is a top IT priority is not reflected in the budgetary numbers. With over 30% of respondents not even allocating money for it.

It should be noted that 60-70% of companies do not have a budget (or don't know) allocated to cybersecurity although 70% of them invest more than 3% of their turnover (if one considers SMEs turnover of 2 million, it is over 60,000€ a year) in IT. Our primarily target customer (SMEs with no education around Cybersecurity) do have in mind some idea of the cybersecurity costs and they may be hesitant to invest in it due to the prices offered by the consortium. But they are willing to enhance the awareness in their organizations and this can be the entry point to also introduce additional functionalities of the framework.

When asked about the price of a comprehensive cybersecurity solution, "Which is the price, you as an SME, consider affordable?" the mean response was about 2800 Euros per year. Although the mean turnover of the companies that were surveyed was about 2 Million Euros, this number is still relatively low and doesn't coincide with the weight the respondents gave to cybersecurity. It does however provide, in our opinion, a more honest metric to the level of prioritization cybersecurity gets, and the quality of the solution that can be provided accordingly.

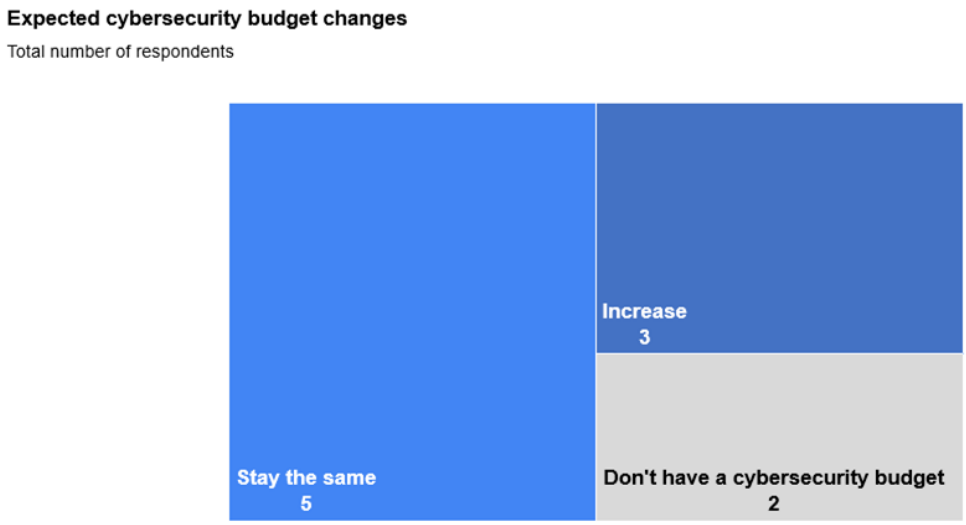
We also asked: "In case of budget restrictions, is there any component you will consider a MUST and pay for it individually? (without paying for the whole framework)". Here answers varied quite a bit -

Ransomware protection, SIEM, End-point protections, Cloud and Transport level security and storage, Detection and Alerting component, Antivirus, Hosting/Mail Services, Intrusion detection and prevention, Firewall, Protection against hackers, Online Backup and intelligent virus protection. As well as two "None" answers. This shows that the 'MUST' component is very individualistic and is quite different from company to company.

This information has been used as an additional input to benchmark the original approach of the consortium to its pricing structure. This price shows the intentions of the end users regarding the use of specific tools and not the whole SMESEC framework. This question was aimed to gather information around one of the key pillars of SMESEC project, a budget friendly framework for SMEs.

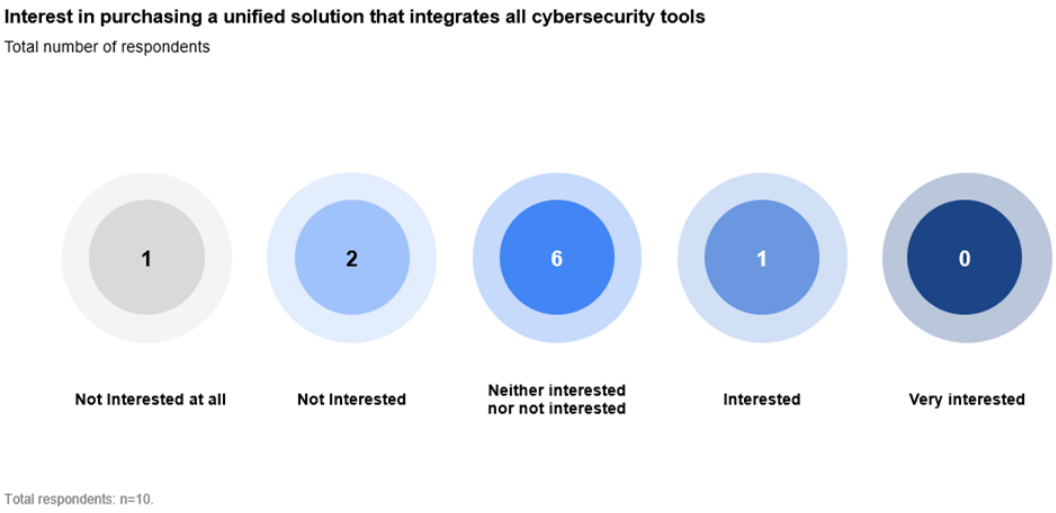
Although as described in D6.5 in the pricing structure, the lower trench of SMESEC Framework was on the limit of 7500€ (non-contemplated in the budget allocation of a high % of SMEs), this SMESEC basic package includes a wide range of tolls that could exceed the SMEs coverage intentions. A tailor-made approach to each customer needs can accommodate both budget limitation and the needed cybersecurity approach to their organizations. This is also evident in Figure 19 answers suggest that cybersecurity budgets are expected to remain the same or increase in most surveyed SMEs, with no planned decrease.

Figure 19 Expected Cybersecurity budget changes



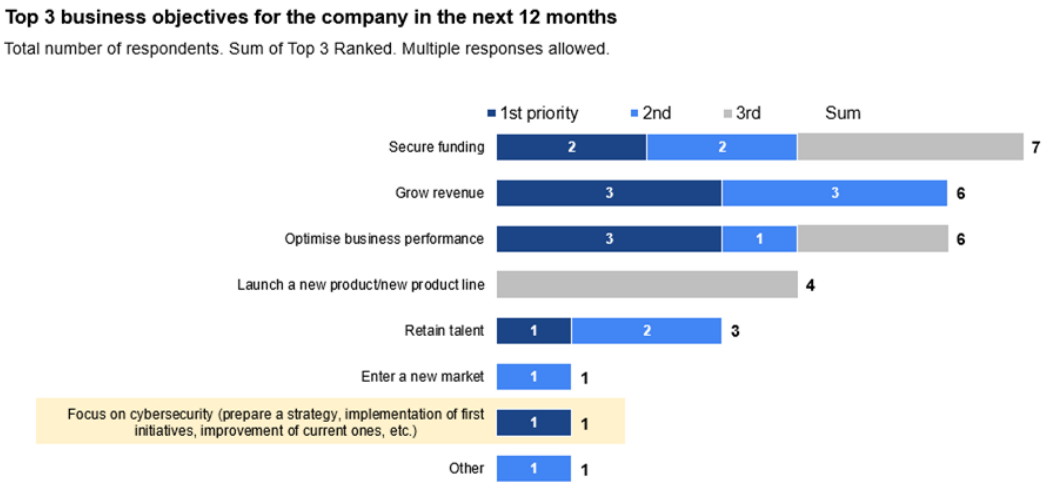
In Figure 20 One can see there is weak outright interest in purchasing a unified solution for integrating all cybersecurity tools, but a substantial number of latent interests by undecided respondents.

Figure 20 Interest in purchasing unified solution for integrating all cybersecurity tools



Another evidence for the place cybersecurity has in the SME leaders' mind can be seen in Figure 21. When asked to list the top 3 business objectives for the company in the next 12 months, focus on cybersecurity was mentioned by only one respondent.

Figure 21 Top business objectives for the company



6 Conclusions

Building upon the trail results collected in T5.3 as well as the collected results from the open call activities in T5.5, we conducted an evaluation of the SMESEC security framework in the real-world environment. We provided a qualitative and quantitative assessment of the performance gains introduced by the SMESEC security framework in each SME pilot environment, as well as the complete framework as a whole we have qualitatively and quantitatively assessed the performance gains of the SMESEC Framework, evaluated both, the performance of the individual system modules, and the integrated system, analysed trial results against WP3 requirements and extracted lessons learned and recommendations.

Cybersecurity is a top concern among SME leaders. Its affects go far beyond breach of confidential information and data infringement. With availability and data integrity also at risk, one would expect a hefty portion (or at least some) of the IT budget to be allocated to cyber defence. Consequently, when gathering requirements for the SMESEC framework a vast and thorough list of capabilities emerged. However, when surveyed about the price SMEs are willing to pay and currently allocating to cybersecurity, a different attitude towards security was evident. Perhaps this attitude is a result of lack of knowledge (as also evident by responses to different survey questions, especially regarding the amount of cyber training and knowledge), perhaps while respondents claim cybersecurity is a top concern it is in fact not that high in the priority list. No matter the reason, these results emphasize the importance of training. Proper cybersecurity education should be the first step before offering a technological solution, so that SME leaders can be better informed and would be able to better asses risk and value. At the same time, one should strive to lower costs and offer a modular solution that can accommodate smaller budgets.

We have concluded that the SMESEC Framework meets functional and non-functional requirements and provides an effective and necessary solution to a core challenge to many SMEs. As per our economic analysis SMESEC framework price is higher than the mean price of the survey answers, although there is also a group of potential customers with even higher budget SMESEC approach has to leverage the awareness and training tangible needs express in the survey by the SMEs to make a first contact and show all the benefits that such platform can provide. Due to its lower scores for ease of installation and configuration, we recommend that future work will focus on improving these parts of the solution.

7 Feedback from the pilot partners at M36

As stated in the executive summary, this brief section is introduced in the deliverable D5.4 to provide a feedback from the pilots on the gains that the SMESEC Framework delivers to their day-to-day activity.

The different inputs have been gathered in a free format so that they can freely express their feelings at M36 about the proposed solution.

7.1 Pilot 1: e-Voting

7.1.1 Introduction

This document aims to gather details with regards to the final integration of the different use cases and the solution providers as well as detailing how the initial goals have been accomplished by the synergies brought by such collaboration.

Firstly, there will be a brief summary of the final architecture and systems of the use case itself, detailing the current architecture and other technical details of the structure of the use case. Afterwards, there will be a general description of how the use of the framework has enabled further functionalities, also providing details of how the specific technology for each solution provider has contributed to the improvements on making the actual product more secure. These aspects will be in tight relation to the requests done at the beginning of the project in Section 6 of Deliverable 2.1.

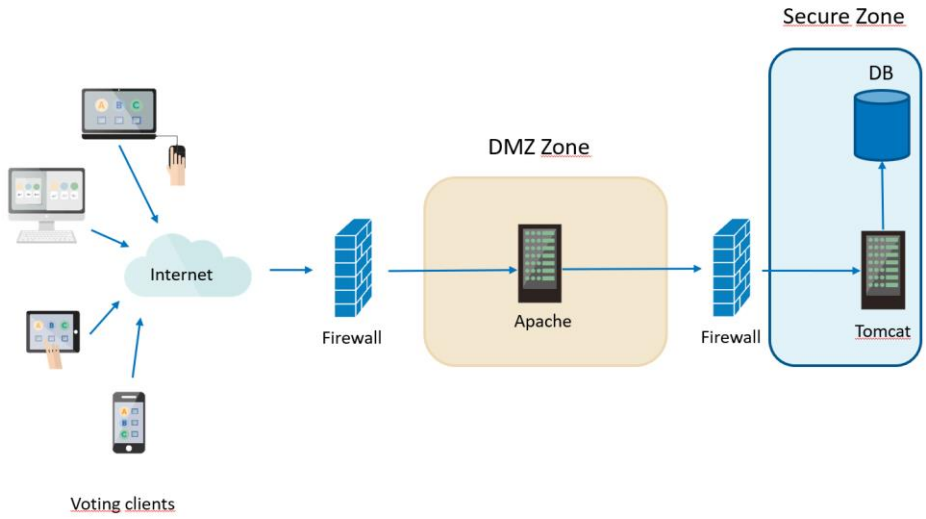
7.1.2 Improvements of the architecture of the use case

The online voting system deployed in the SMESEC project had a structure that is common in web services. The system was composed of three main components: a web server (Apache), an application server (Tomcat) and a database (DB).

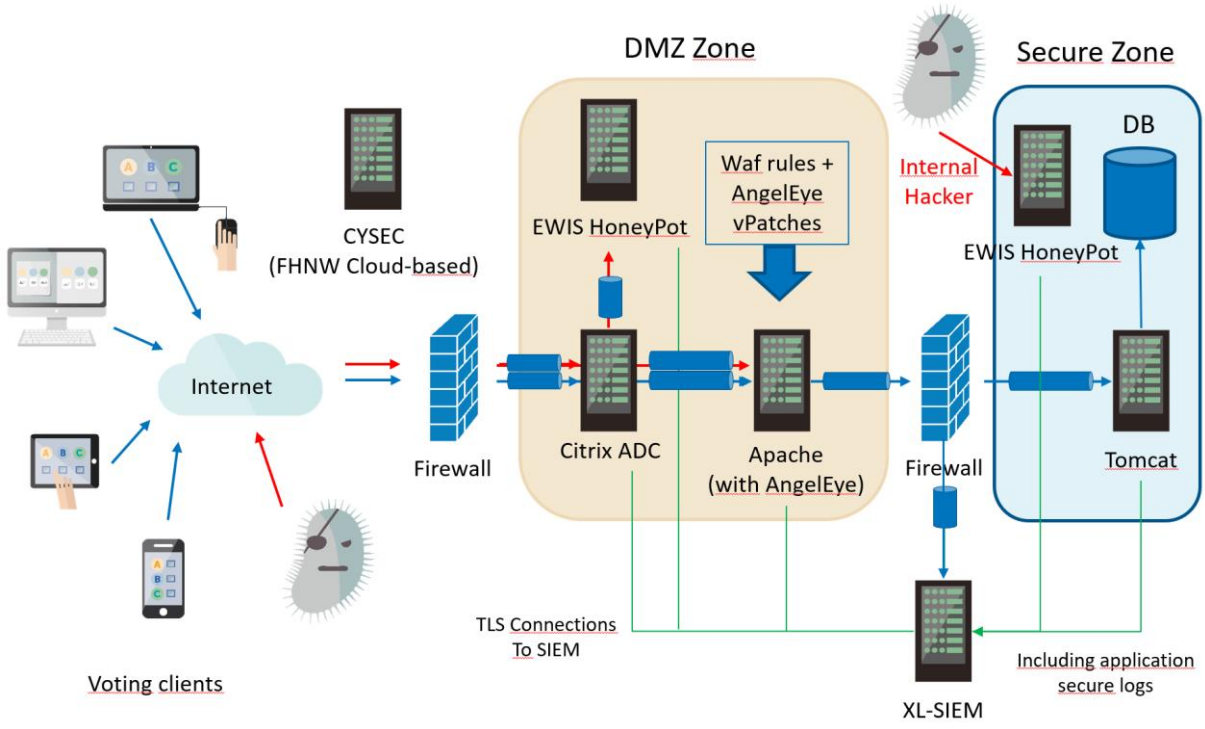
The web server was deployed in a DMZ network, which was accessible through Internet. The application server and the database were deployed in a Secure Zone network, which was not directly accessible through Internet. The voters connected to the system using a Javascript Voting Client that was locally executed in their computers.

The SMESEC framework and a subset of the tools were integrated in the online voting system use case. The tools integrated were Citrix ADC, two instances of the EWIS HoneyPot, XL-SIEM and AngelEye. Also, CYSEC was activated for our use-case, although it did not require any modification in the online voting system. The following graphic shows the integration of the different tools into the online voting system:

Before SMESEC



After SMESEC



Citrix ADC is used as an application firewall; thus, it was configured to be the first element that process the incoming connections that arrive from the Javascript Internet Voting Clients to the web server. The EWIS HoneyPot deployed in the DMZ Zone is used as a system to receive redirected connections

rejected by Citrix ADC, i.e. connections that Citrix ADC have determined that are not compliant with the voting REST API. The EWIS HoneyPot that is installed in the Secure Zone is a regular honeypot system used to attract attackers that are trespassing into this private network. The XL-SIEM agent, deployed in a dedicated subnet, listens for Syslog connections from the other components deployed, e.g. web server, web application server, etc. The syslog of these components is forwarded to this agent that, in turn, forwards it to the external XL-SIEM server. Angel-Eye is used as a periodically analyser of the HTTP requests received in order to detect potential zero-day attacks. And, finally, CYSEC is a tool that, despite not being deployed within our system, is accessible through the framework main pages and presents questions that are used to evaluate the security awareness of the users of it.

All the online voting system, as well as the tools of SMESEC integrated, were deployed in an EC2 environment of Amazon Web Services, although the same scenario is valid to be deployed in physical networks. From a perspective of the SMESEC Framework, the components selected can be used both in virtual and physical environments.

7.1.3 Enhanced functionalities

7.1.3.1 The SMESEC Framework

The SMESEC Framework front-end has largely enhanced the use case functionalities by offering a dashboard that allows to monitor in real-time the security of the e-voting system deployed. In case there is a problem an alarm is raised, and it can be studied in more detail in order to guarantee the security of the system. Also, in the other hand, the framework provides both security recommendations, given in the context of a security questionnaire available to the users, and trainings, which are offered to the users (some of them selected as mandatory).

7.1.3.2 The solutions

SMESEC has brought the possibility to complement the online voting system with a security framework that is adapted to the needs of SMEs. The following security benefits are obtained:

- Application level firewall: The connections to the Voting Portal, the most critical part of the service because it has to be online and available during all the election, are filtered at application level. Thus, in case an attacker tries to exploit this component with malformed requests to this service, the connection is redirected and send away from the server. This decreases the probability to compromise the Voting Portal. This is aligned with the initial requirement to protect the web application servers and the network traffic of the system.
- Intruders detection: If an intruder reaches the Secure Zone network, due to the actions exploring the network, we will receive alerts from the deployed HoneyPot included in the framework. This is useful to obtain an early detection of malicious activities within the system. This is also aligned with the requirement of protection the network traffic of the system.
- Events and alarms: The framework allows to gather and show events that are generated by the security tools of the framework and/or directly by the online voting system components. Also, these events can trigger alarms when some of them happen. This can help to detect suspicious activities in the system that may indicate an attack is carried on or that is being prepared. This

is aligned with the initial requirements about the protection of the different components of the system, ie. the web servers, web application servers and database.

- Detection of zero-day attack: The framework provides mechanisms to detect malicious requests against the web servers, which may lead to zero-day attacks, i.e. newly discovered attacks for which there is not fix available and the server is still unpatched. In our case we applied it to the Voting Portal in order to detect possible attacks that bypass the application level firewall. This was aligned with the initial requirement about the protection of the web application server, which would be the target of this type of attack.
- Security awareness: The framework provides online quizzes to evaluate the security of the company. In our particular case that we have a security team, this is not as necessary as other parts of the framework, but it can be useful to provide security self-assessment capabilities to our customers.

7.1.3.3 Testing

The testing of the system was done during the WP5 test campaign. The functionalities previously described were tested in the following manner:

- Application level firewall: a Scytl internal tool, ROTI, which simulates different parts of the voting process, was used to execute several security tests against the Voting Portal and ensure the system could not be compromised. The tests were adapted to test the application level firewall offered by Citrix ADC. They consisted of sending malformed requests of the main operations that are issued by the Voting Client to the Voting Portal. The tests passed if the requests were rejected as expected.
- Intruders detection: The honeypots were tested using synthetic attacks that were simulating Denial of Service attacks, SQL injection attacks and Brute-force attacks. After executing these tests the different dashboards of the system were checked in order to see that they were detected.
- Events and alarms: The SIEM included in SMESEC was tested both with a tool that was generating synthetic test messages, and using examining the events produced due to the execution of the previously described tests.
- Detection of zero-day attacks: This functionality was tested using the previously mentioned testing tool ROTI fed with synthetic data created with the same application used to generate the training data of the system. The testing tool was issuing manipulated requests, simulating the ones of the Voting Client, and these requests were registered by the Apache Web Server and latterly analyzed by the appropriate tool of the SMESEC framework. Comparing the result of the analysis with the type of data used to issue the requests, we could compute the efficiency of the detector.
- Security awareness: In this case we run the quiz ourselves and evaluated the types of questions received and the later feedback obtained.

7.1.4 Conclusions

The main goal to be achieved using SMESEC security framework is to increase the security at the infrastructure level, as it currently is at application level only if no other tools are used. However, with SMESEC, Scytl will be able to offer its e-Voting service combined with a robust security framework that will allow SMEs and public authorities to be aware of their security by themselves and to add

security measures in their election processes with a budget adapted to each case. This will enhance not only the level of security of its platform, with an additional security layer, but also its credibility with clients. Such approach will help these entities to carry out consultation processes even with limited budgets, and with the highest levels of security, availability, and transparency. For these reasons, SMESEC Framework helps to overcome entry barriers for online voting, from both a security and a cost point of view, allowing local authorities and small public entities to implement direct democracy practices and e-government.

In addition to all that, SMESEC framework becomes a tool to improve security training and awareness within the company.

7.2 Pilot 2: Smart City

Inside the context of SMESEC, University of Patras (UOP) was responsible for the smart city pilot. The pilot focused on securing the sense.city, a smart city platform developed for citizens that want to report to their municipality problems they may have in relation to their city infrastructures and operations.

One of the peculiarities of this pilot was the fact that, contrary to the rest of SMESEC pilots (IoT, eVoting, Smart Energy), sense.city was a free tool created by a University and not a market product offered by a company. Thus, the development team, which was mainly composed by research stuff and students, had mainly focused on the functionality and features and did not pay too much attention on other aspects like business and marketing plans, security aspects, compliance with local regulations etc.

With the release of sense.city's first version and its adoption by the municipality of Patras, UOP team realized that their solution had the opportunity to become an actual market product. But to achieve such a goal the team had to start working more professionally and adopt more business-oriented habits and practices. Such practices included market analyses, business plans, competitors' products evaluation as well as security enhancements, regulations compliance etc.

At the same time the SMESEC project was starting and sense.city was one of the pilots that would evaluate the proposed security tools and solutions. University of Patras viewed their participation in this project as an opportunity to address several security requirements of the sense.city platform and its infrastructure (UOP cloud facilities). The team wanted to use the SMESEC framework to ensure that their service is provided to municipalities without introducing significant risks to their systems or data.

Inside the project, UOP adopted various security tools to protect the sense.city service. However, apart from the technical tools, SMESEC heavily influenced the security awareness of the lab. People involved in the development of the platform, realized that it was not just security components that were missing. Several required processes and security practices were overlooked and were directly putting the platform at risk. Security partners from SMESEC consortium helped UOP identify their critical vulnerabilities

and based on their recommendations sense.city started implementing security plans, organized patch management, backup plans etc.

With better security in place, UOP begun the development of a new "more sensitive" feature based on which, people with special needs can register their location inside sense.city and public protection authorities can dynamically adjust their operational plans in case an emergency incident takes place nearby. This feature was a "game-changer" in the market for smart city applications, since it was not offered by other platforms with similar functionality like the sense.city. With this feature, sense.city attracted the interest of many Greek municipalities which in turn led to increased resource requirements and personnel costs.

To be able to support its new costs, the team decided, from the beginning of 2020, to start charging the sense.city service. Also, it begun re-evaluating its plans for creating a new company. With the help of SMESEC partners (ATOS and WoS), they created a business plan and a roadmap towards the launch of a self-sustainable spin-off. The business plan revealed that based on its current customers and costs, the company is not yet viable, but it can be within the next one or two years. For this reason, the team decide to postpone the creation of the company. We must note that all budget estimations used for the business plan were based under the assumption that sense.city's income comes only from its customers. A possible collaboration with funding schemes (angel funds, VCs etc.) would probably allow the creation of a company much sooner.

7.3 Pilot 3: Industrial Pilot

7.3.1 Introduction

This document aims to gather details with regards to the final integration of the different use cases and the solution providers as well as detailing how the initial goals have been accomplished by the synergies brought by such collaboration.

Firstly, there will be a summary of the final architecture and systems of the use case itself, detailing the current architecture and other technical details of the structure of the use case.

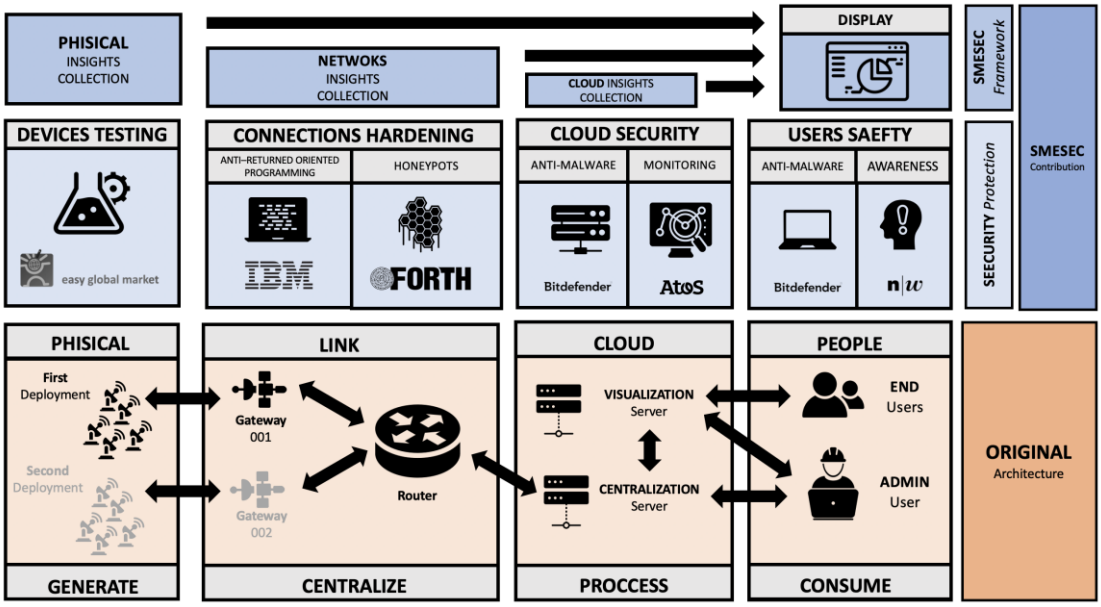
Afterwards, there will be a general description of how the use of the framework has enabled further functionalities, also providing details of how the specific technology for each solution provider has contributed to the improvements on making the actual product more secure. These aspects will be in tight relation to the requests done at the beginning of the project in Section 6 of Deliverable 2.1.

7.3.2 Improvements of the architecture of the use case

The commercial product Loadsensing was originally intended to provide advanced infrastructure monitoring capabilities to the clients by using IoT systems and other related-technologies. The architecture of this product was, however, initially designed with poor protection capabilities against standard cyberattacks (see Figure 01, original items highlighted in orange).

As a result of SMESEC implementation, Worldsensing has achieved a much more mature status to cope with cyber security issues, enabling identification, protection, monitoring and responding capabilities that before the project were not even conceivable. The new elements added along these three years (*Figure, new elements detailed in blue*) allow to address the functional requirements identified at the beginning of the project (see below).

General view of the integration of SMESEC elements with original Loadsensing elements

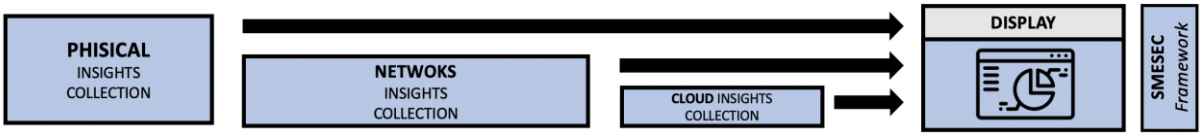


7.3.3 Enhanced functionalities

7.3.3.1 The SMESEC Framework

The industrial pilot developed in the frame of the project activity covers from physical sensors deployed in a football stadium to cloud systems. Therefore, any solution aiming to secure such an end-to-end infrastructure had to aggregate heterogeneous data in a simple and harmonious way: one of the main requirements to the SMESEC framework from the very beginning.

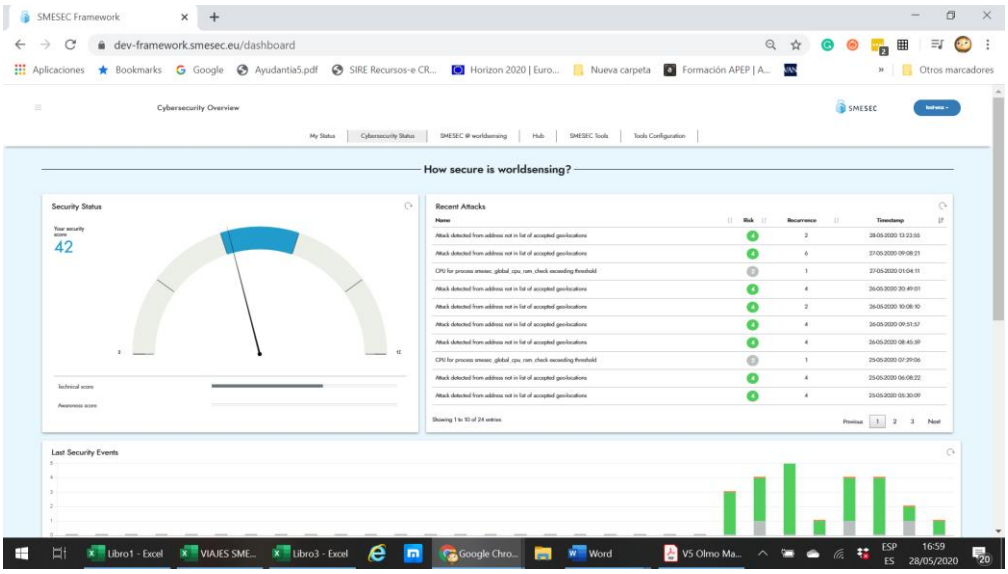
SMESEC Framework functionalities for Worldsensing pilot (industrial pilot)



Once the SMESEC framework is up and running, it can be asserted that it is more than the sum of its parts, providing unique aggregation capabilities in a simplified way. In fact, the usability of the solution is remarkable and very intuitive. This allows use even for non-cybersecurity experts, who can gain a rapid insight of the pilot status and all the existing threads in a real time approach. Last but not least, the

implementation of business rules and the possibility to launch alert messages through SMS or email is a very attractive functionality for micro companies, in which the lack of human resources often makes necessary multi-tasking of their employees (alerting).

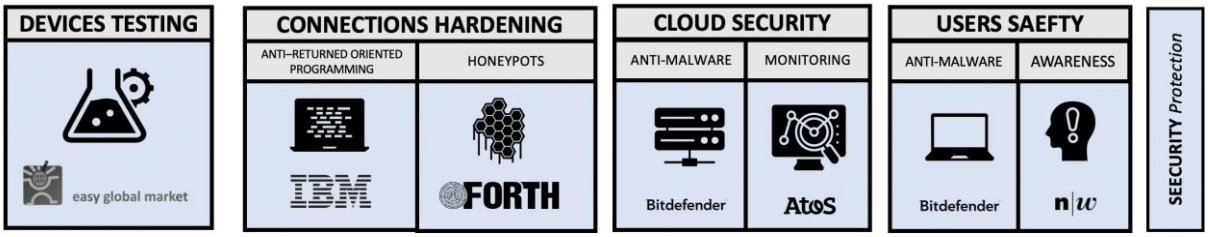
SMESEC framework view: the status of the pilot is shown in a user-friendly approach



7.3.3.2 The solutions

Without any pretensions to being exhaustive and avoid duplicities with previous deliverables, it should be stressed that the selected security solutions allow covering the end-to-end architecture of the pilot, even covering the human factor. Now, the solutions work in an orchestrated way and the feasibility to operate in larger Loadsensing deployments has been validated (scalability). On the other hand, it has been proved that each solution actively protects against specific attacks (see deliverable D5.3).

Solutions integration schema within the Industrial Pilot

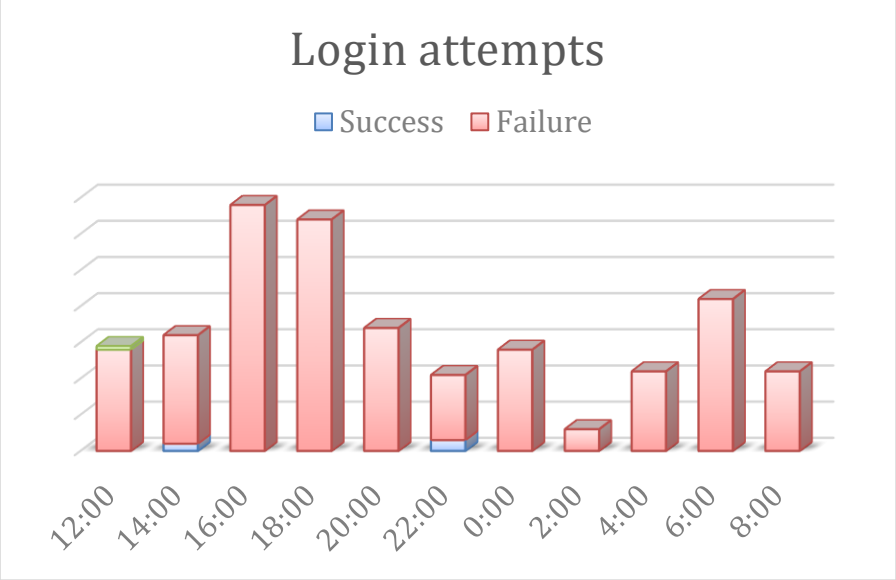


7.3.3.3 Testing

The functional tests carried out at pilot level (see D5.1, D5.2 & D5.3) have successfully validated the performances of the SMESEC framework instance deployed by Worldsensing.

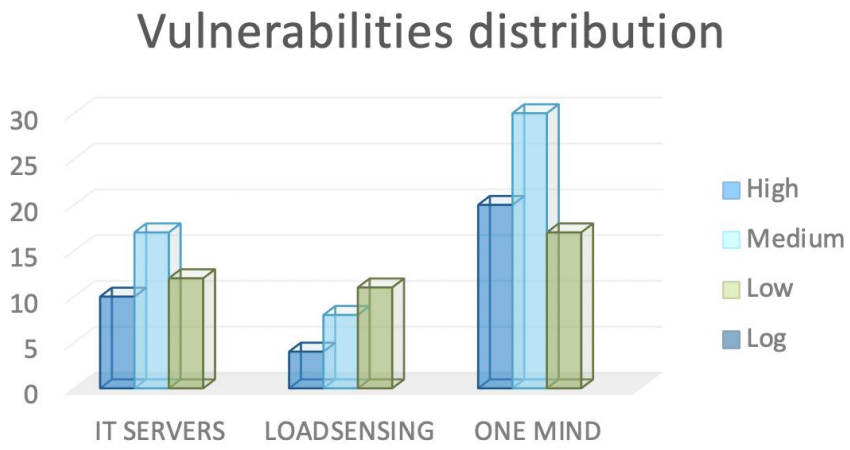
Beyond this preliminary but necessary work, the solution has been, above all, tested in a real-mode approach during some months, providing an unprecedent opportunity to observe cybersecurity risks and threats that before SMESEC were unknown inside Worldsensing. For instance, the figure below shows the fraudulent login attempts in the pilot cloud systems that were detected in one single day.

Login attempts in the pilot cloud machines



This information combined with the improved cybersecurity awareness within the company has allowed readdressing the development priorities without Worldsensing, starting from a vulnerability discovery exercise of our infrastructures and products (Figure below)

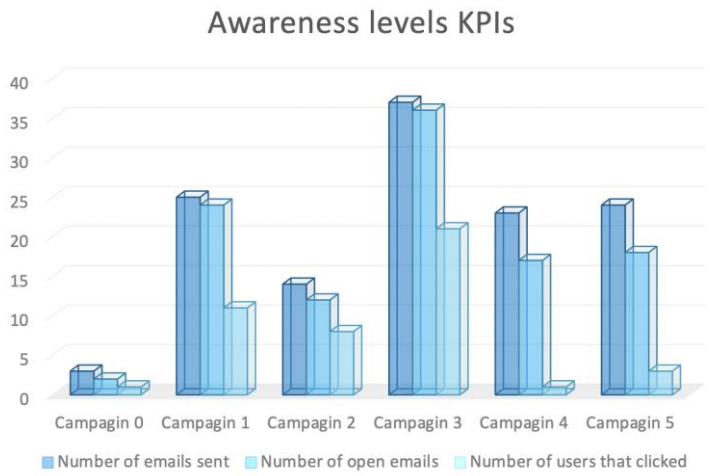
Vulnerabilities distributions by criticality level found in Worldsensing assets and products



If looked from the human angle, the increase in cybersecurity awareness has been huge: the project has enabled the company to have a security manager who generated an internal culture in Worldsensing by

using many of the trainings provided by the SMESEC Framework. Not only, but also through different phishing campaigns there was a clear improvement in the level of information that the users had upon scams and cyber-attacks via email. This step forward at company level is demonstrated with the ISO27001 label granted two years ago.

Aggregated results of phishing campaigns completed during the SMESEC period among Worldsensing's employees



Having said that, the following table summarizes how the initial requirements from Worldsensing are met by the final version of the SMESEC framework.

Business objectives		
Availability	X	Technology of XL-SIEM and SMESEC Hub will work together preventing any service disruption by monitoring and early alerting about attacks.
Usability	X	The solution can be easily used without previous knowledge. Training tools are provided to cover knowledge weaknesses
Privacy	X	Data protection is now ensured by the usage of the framework that preserves privacy by its layered approach within the client's infrastructure.
Cost	-	-
Alerting	X	The SMESEC Hub allows the configuration of dynamic and flexible alarms (web, SMS, email)
Platform objectives		
System integrity	X	The security level of the solution has been validated by the red team analysis
Non-repudiation	X	The log automated system will allow for any forensic or audit investigation to gather all the needed proof of events.
Authentication	X	Authentication through Keycloack has been implemented.

Scalability	X	The solution will be easily scalable by the creation of configuration files that will automatically deploy the different parts of the security framework.
Protection objectives		
Web application servers	X	Bit Defender endpoint management will provide protection against all malware threat on the servers.
DDoS	X	Forth honeypots systems enable early intruders' detection as well as providing denial of service attempts alerts.
Access abuse	X	Role based access control will prevent from any unauthorized access to the technology.
Software missuse	X	Rule based access control will prevent from any malicious usage of the technology.
Zero-days attacks	X	Detection technology by XL-SIEM will alert if any unusual behaviour comes out in the systems.
Code injections	X	IBM anti-ROP technologies will alter the source code in such way that it will be impossible to modify the original usage of the systems.
MiTM attacks	X	End to end encryption will protect against message interception and any confidentiality, integrity or availability attack that might arise.

7.3.4 Conclusions

SMESEC project has been an incredible opportunity to enhance the overall security maturity in Worldsensing, from many different points of view, included the human dimension. From the company assets protection perspective, and considering the technology made available by the solutions providers, the cybersecurity enhancements have been outstanding. The different systems have now extra protection layers that are enabling more reliable systems and technology at company level.

A lot of work has been done in the area of enhancing also the product, and Loadsensing, the product that was used for the pilot within the project has clearly evolved from its initial status towards a much stable and reliable product with less vulnerabilities and chances to be exploited.

Last but not least, having this security mindset has enabled the company to reach clients that were not possible to do so in the past due to the higher demanding requirements that we are able to deliver now (like real time monitoring and event management).

7.4 Pilot 4: Smart Grid

7.4.1 Introduction

This document aims to gather details with regards to the final integration of the different use cases and the solution providers as well as detailing how the initial goals have been accomplished by the synergies brought by such collaboration.

Firstly, there will be a brief summary of the final architecture and systems of the use case itself, detailing the current architecture and other technical details of the structure of the use case. Afterwards, there will be a general description of how the use of the framework has enabled further functionalities, also providing details of how the specific technology for each solution provider has contributed to the improvements on making the actual product more secure. These aspects will be in tight relation to the requests done at the beginning of the project in Section 6 of Deliverable 2.1.

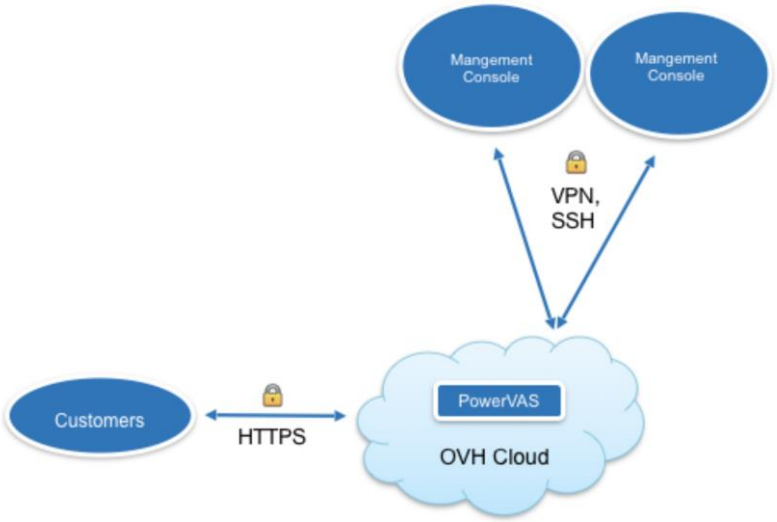
7.4.2 Improvements of GridPocket architecture thanks to SMESEC

Gridpocket as a company that offers software as a service in energy sector always paid attention to cybersecurity in order to keep its clients' data safe. Before starting the project, our architecture was different than the present one. Thanks to the SMESEC project, we learned and applied many things while realizing that our architecture could be significantly improved.

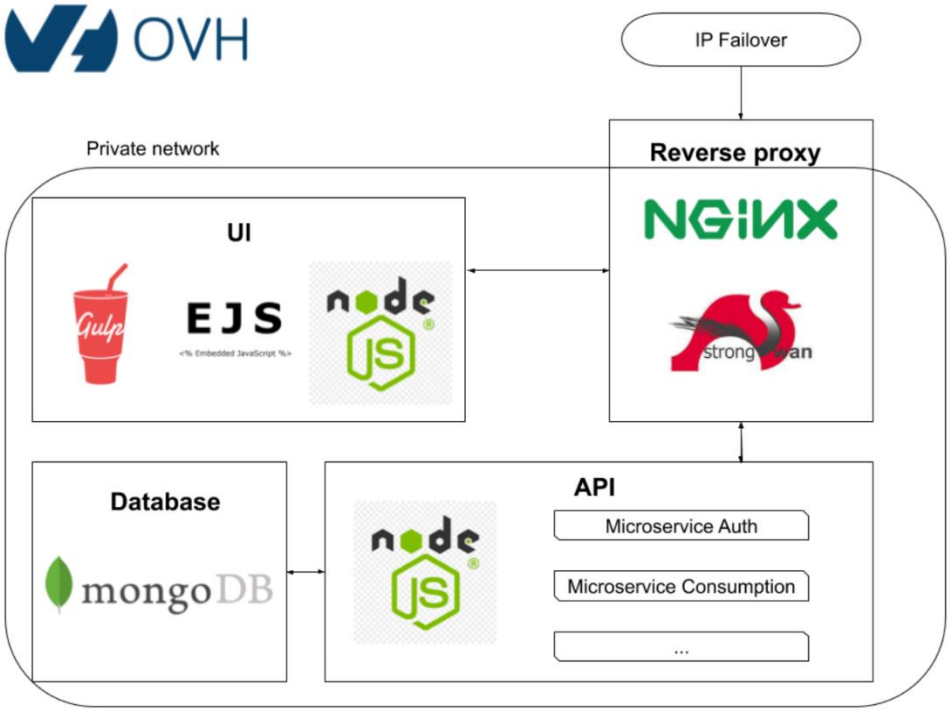
7.4.2.1 Architecture before the project

Before joining the project, our architecture was quite simple (see Figures below). Our clients connected to the server located in the cloud using an encrypted HTTPS connection and we connected to the server using a VPN (Virtual Private Network) and a SSH protocol. On our cloud server, every connection was going through the reverse proxy, then data was displayed using UI modules and API requests. Our technologies were mainly protected against injection of malicious code (on the front and backend sides). In addition, we organized basic cybersecurity training for our employees.

GridPocket general architecture at the beginning of the project



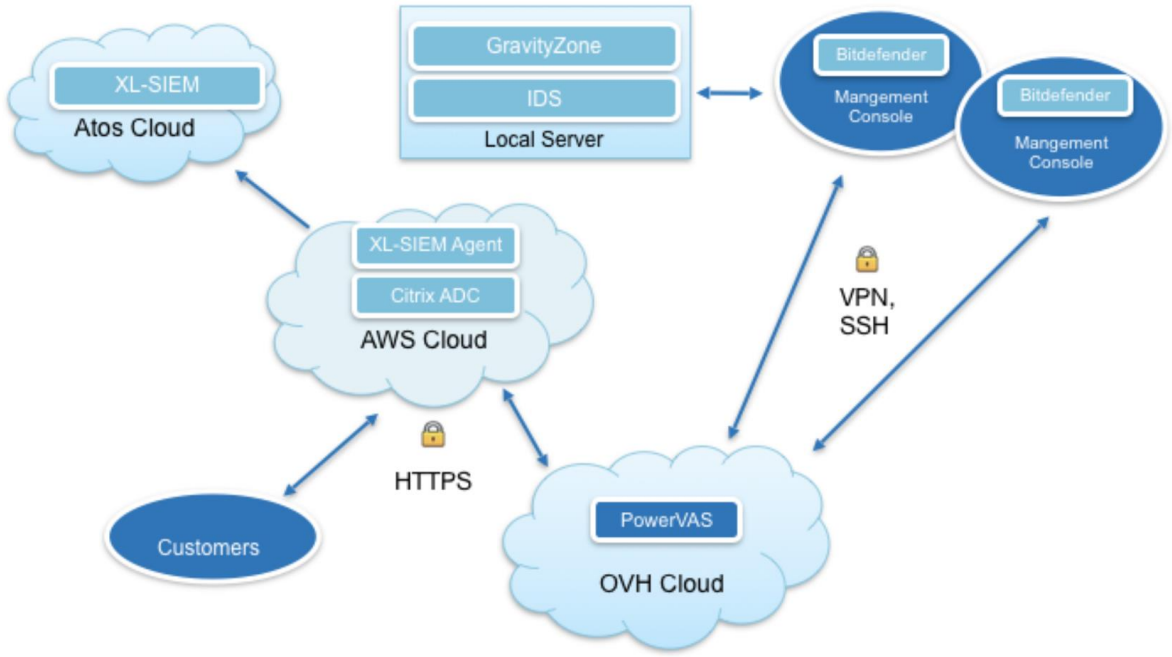
Gridpocket server architecture before SMESEC



7.4.2.2 Architecture after the project

During the SMESEC project, we expanded our architecture by adding another local machine with IDS (Intrusion Detection System) and Gravityzone both installed. Thanks to this, we have expanded our architecture with tools to detect and block potentially dangerous traffic. We also installed Bitdefender on other local machines previously used. In addition, we added another cloud from another provider (AWS) where Citrix ADC and XL-SIEM agent have been installed and configured. Agent XL-SIEM communicated with the cloud of Atos, on which XL-SIEM was located. It contributed to the fact that we have strengthened the security of our network and obtained the option of displaying cybersecurity data in one place (XL-SIEM website). This new architecture is described in Figure below.

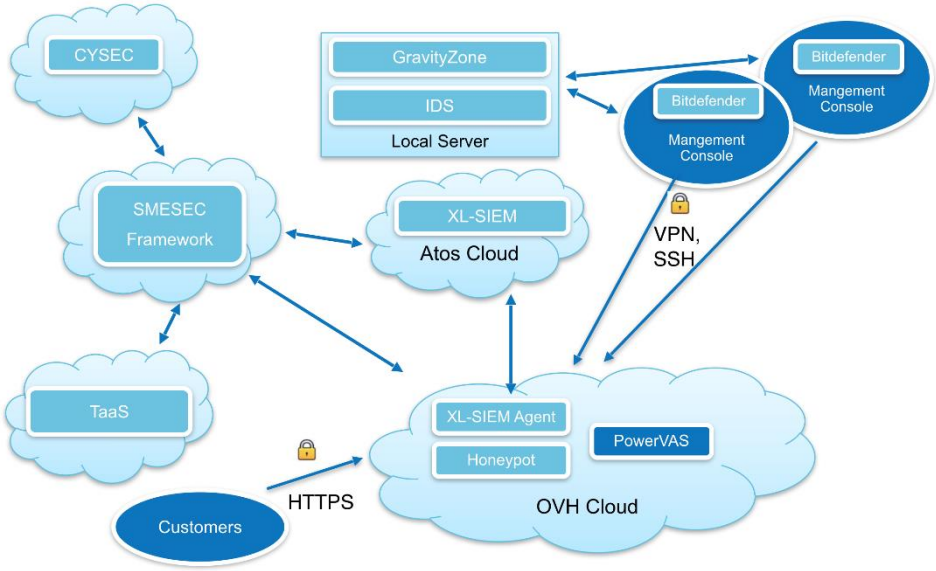
Gridpocket general architecture during the SMESEC project



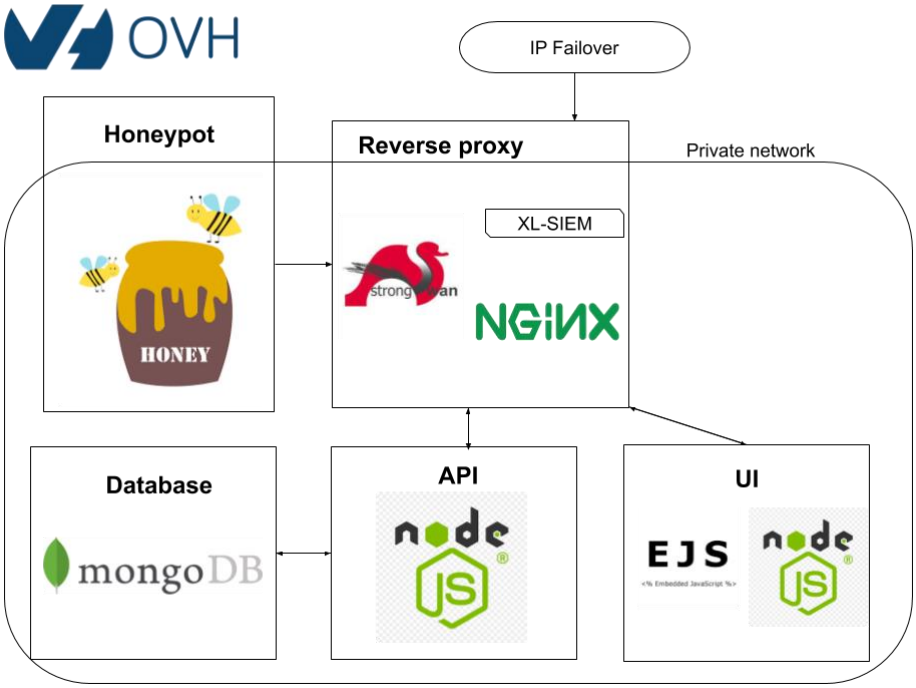
In the last phase of the project, we decided to move the XL-SIEM agent and Citrix ADC from the AWS cloud to the OVH cloud, where our server was located. This was mainly due to economic aspects (OVH cloud is much cheaper to maintain) and ergonomic (we preferred to have everything in one cloud to manage it easier). In addition, we also installed Honeypot next to the reverse proxy, and all potential attacks are targeted there. Unfortunately, after a very long time of fighting, it turned out that Citrix ADC could not be configured on the above cloud. As a consequence, only our agent XL-SIEM and Honeypot remained on our OVH cloud.

In addition, we started using the TaaS tool to test our API and started using the trainings and quizzes found in the CYSEC tool, which meant that our employees could expand their knowledge of cybersecurity on their own. The complete architecture is described in Figures below.

Gridpocket general architecture at the end of SMESEC project



Gridpocket server architecture at the end of SMESEC project



7.4.3 Enhanced functionalities

7.4.3.1 The SMESEC Framework

Improving our level of security was possible thanks to the acquisition of a lot of knowledge in the field of cybersecurity. The use of coaches through Cysec was extremely useful to get this level of knowledge. The help of the developers of individual tools was also very useful to increase our security level. Configuration and installation of the different tools was the first step of the work. The SMESEC framework web application was very user-friendly to supervise events occurring in individual tools and following their different status. We believe that one of the strengths of the Framework was that it could be managed even by a person who does not have much experience with cybersecurity through its main interface.

In our case, the SMESEC framework was useful because different people could easily control the security status of our solutions by only checking the dashboard of the solution. This was a great gain of time not to control the cyber security status of all the different tools individually.

7.4.3.2 The solutions

As we mentioned before, the SMESEC project has greatly helped GridPocket cybersecurity. Until now, we have mentioned it in a quite general way. Here, we list exactly what are the aspects that have been developped or strengthened during the project:

- **General security maintenance - GravityZone** - Our machines were protected from potential risks (malware, spyware, firewall for our PC's)
- **Protection in case of breach into company network - Honeypot** - If any attacker manages to get into our network, and such an attack is detected, all its movement will be redirected to a virtual sandbox, where he will lose a lot of time and may refuse further attacks. Thanks to this, we can gather more information about the attacker and use it in the future to improve our security.
- **Testing our API security - TaaS** - We can test our API if there are safe to use and if there are no security holes in them that could be used against us
- **Network communication security - IDS** - We can detect if there is any intruder and block him, so that our network remains secure
- **Having events about security breaks - XL-SIEM** - Thanks to it, we don't have to keep an eye on logs from individual tools, and we'll find every information about any attack attempts in one place, thanks to which we can operate more efficiently
- **Broadening knowledge about cyber security and employee training - CYSEC** - A tool that is not the only one designed to protect us physically against attacks but allows us to develop knowledge in the field of cybersecurity, to learn new solutions and possibilities of protection in the network. It is well suited to test employees' knowledge and show them that cyber security is really important nowadays for the smooth functioning of a company

7.4.3.3 Testing

To make sure that our system or network was secure, we had to test the SMESEC protection in practice. To do so, we tested the security of GridPocket PowerVAS platform with SMESEC in many different ways. One of them was to realize some testings prepared by the suppliers of the individual tools. All of the installed SMESEC tools were tested. All tools worked as they should for the different use cases. We

had problems during the testing for some of the tools, but with the help of suppliers of these tools we managed to deal with them.
Below is a brief description of the different encountered problems and how they were fixed (if possible):

CYTRIX ADC:
Initially our Citrix ADC was located in AWS cloud. It was not an optimal solution for us, and we moved it to OVH cloud, where is our main solution for customers - PowerVAS. Unfortunately, OVH cloud is not compatible with Citrix ADC. We managed to install Cytrix ADC there, but it wasn't fully configured, because of the inability to configure it on this cloud. Tests included Cytrix ADC couldn't be completed in our case. Based on the technical analysis and exchanges with SMESEC team, we have decided not to pursue further research and experimentation with this tool.

Bitdefender Gravityzone:
All tests except one went without any obstacles. We had identified, however a certain number of technical issues with running **IT_02_5_GravityZone.** Our scans were not detected. The problem was that the computer machine we scanned had an OSX operating system where port scans are not detected by Bitdefender Gravityzone. After some time and consultation with Bitdefender, we were able to perform the test on a MS Windows OS machine and the test was carried out, but only once. Once again it was impossible to complete the tests. There was probably a problem with the cache or the blocking of the possibility of the next scan in MS Windows or Gravityzone, so we had to find another workstation with MS Windows, on which the test was already documented.

XL-SIEM:
Initially, during a long period of time the dashboard of XL-SIEM did not detect our tests and showed incomplete information from other tools. However, after consulting with the team from Atos and one of the tool's updates, this problem was solved. Following all update and configuration procedures it was possible run all required tests without any further compilcations.

TaaS:
Before running the API test (IT_05_2_TaaS) we had an issue after migrating our API into the tool. GridPocket team requested support from EGM, as a result it has managed to do a number of changes in the API tests, so all tests were completed.

IDS:
We didn't have any problems running tests of this tool. Network scan and DDoS attacks have been correctly detected, and information about this has been sent to XL-SIEM.

Honeypot:
While performing one of the tests, we discovered that one of the Honeypot tools was not working. We contacted FORTH and the problem was solved, so we could do the test without any problems. DDoS attack, database and brute force attacks have been correctly detected and information about that had been successfully forwarded to XL-SIEM.

In addition to testing individual tools, we also tested the content of training courses and educational quizzes found in CYSEC. Several of our employees performed tests and quizzes and positively assessed their substantive content.

7.4.4 Conclusions

In summary, the SMESEC project significantly increased the level of security in GridPocket company, and additionally influenced the employees' perception on many aspects of cyber security. Thanks to the use of SMESEC tools, we have significantly increased the level of security of our industrial platforms and personal stored data. The security of our customers was increased, which is a great added-value for the company. We are confident to be substantially less exposed to many of the most common attacks lurking on SMEs on the web (DDoS, ports scanning, malware etc.). We also believe that the SMESEC framework, which collects information from all tools and allows them to be easily processed, is what is needed in the cybersecurity SME market today. It allows to significantly reduce the time devoted to taking care of safety and supervising individual tools for this purpose, which is extremely important for companies that primarily need this time to develop their own solutions. In addition, our employees have developed their knowledge of network threats and how to be protected against them. We acquired this knowledge during the installation and configuration of individual tools, we also received huge support and many advices from other project members who are one of the most important players on the cybersecurity market. And we also took courses specially prepared for the needs of SMEs, thanks to which we found a compendium of knowledge in one place and we could easily expand our knowledge.

For the future of the project, we are proud to have participated to different improvements implemented during the project. The first improvement was the ability to check the operation of the Forth and Bitdefender tools, so there is no need to connect to the server on which they are installed and check it manually. The next element was an alarm, when an attempt to connect to an IP server not being using a VPN that has rights to such a connection is detected. Thanks to this solution, we would also not have to manually check if such an event took place.

The last thing that is very important and may not be able to be done in the future is the ability to configure the Citrix ADC tool on the OVH cloud. We are aware that this is a fairly complex process, because the OVH cloud settings do not allow it and it is not the fault of the tool provider, and the OVH cloud infrastructure, as well as the cloud as popular as its competitors (Amazon, Google or Microsoft).

More generally, it is clear that SMESEC addresses the most important needs of integrated security solutions for SMEs. Our use case has demonstrated many benefits of such an approach and at the same time indicated directions for further improvements, both for each of the tool, as well as a deeper integration and 'productization' of the SMESEC framework.

8 References

[1] **Deliverable:** SMESEC. *D.5.1.– Trial scenario definitions and evaluation methodology specification.* 2019

[2] **Deliverable:** SMESEC. *D.5.2.– System readiness for validation activities* 2019

[3] **Deliverable:** SMESEC. *D.5.3.– Prototype Demonstration: Field Trial Results*

[END OF THE DOCUMENT]