



SMESEC

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

D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)

Document Identification			
Status	Final	Due Date	31/05/2019
Version	1.0	Submission Date	18/06/2019

Related WP	WP6	Document Reference	D6.3
Related Deliverable(s)		Dissemination Level (*)	PU
Lead Organization	UU	Lead Author	Bilge Y. Ozkan
Contributors	ATOS FHNW EGM	Reviewers	Ovidiu Mihăilă, BD Noemi Folch, ScytI

Keywords:
Dissemination, market analysis, cybersecurity, standardisation, SMEs

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

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

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

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

Document Information

List of Contributors	
Name	Partner
Marco Spruit, Bilge Y. Ozkan	UU
Alberto Miranda	ATOS
Samuel Fricker, Alireza Shojaifar	FHNW
Philippe Cousin	EGM

Document History			
Version	Date	Change editors	Changes
0.1	21/03/2019	UU	High level table of contents
0.2	29/03/2019	UU, FHNW, ATOS	Table of contents
0.3	17/04/2019	ATOS, UU	Exploitation and Standardisation content merged.
0.4	13/05/2019	ATOS, UU	Exploitation content updated.
0.5	17/05/2019	ATOS	Exploitation content updated.
0.6	20/05/2019	FHNW	Dissemination content updated.
0.7	21/05/2019	UU	Dissemination part integrated with the document. Proof reading done.
0.8	21/05/2019	EGM	Executive summary and conclusion included.
0.8.1	22/05/2019	FHNW	Dissemination part update.
0.9	22/05/2019	UU	Final draft version ready for review
0.93	05/06/2019	FHNW	Finalisation of the dissemination, incl. KPI reflecting status of end of May.
0.94	11/06/2019	ATOS	Updates for the first peer review
0.96	11/06/2019	ATOS	Updates for the second peer review
0.97	12/06/2019	UU	Final updates and checks for the peer reviews
1.0	18/06/2019	ATOS	Quality control and submission to EC

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	2 of 142
Reference:	D6.3	Dissemination:	PU	Version:	1.0
				Status:	Final

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Marco Spruit, Bilge Y. Ozkan (UU)	18/06/2019
Technical manager	Christos Tselios (Citrix)	18/06/2019
Quality manager	Rosana Valle (ATOS)	18/06/2019
Project Manager	Jose Francisco Ruiz (ATOS)	18/06/2019

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	3 of 142		
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

Table of Contents

Document Information	2
Table of Contents	4
List of Tables.....	6
List of Figures	7
List of Acronyms.....	8
Executive Summary	10
1 Introduction.....	11
1.1 Purpose of the document.....	11
1.2 Relation to other project work.....	11
1.3 Structure of the document	11
2 Exploitation Activities	12
2.1 Exploitation Strategy.....	12
2.1.1 Joint Exploitation Plan	12
2.1.2 Individual Exploitation.....	15
2.2 Business Plan.....	22
2.2.1 Summary	22
2.2.2 Market Monitoring	22
2.2.3 Business Model	35
3 Dissemination Activities	58
3.1 Dissemination Strategy, incl. Updates.....	58
3.1.1 Updated target audiences and approach to reaching SMEs:.....	59
3.1.2 Strategy and Roadmap.....	61
3.1.3 Updates to Target Audiences and Messages	62
3.2 Updates to the Dissemination Tools.....	63
3.2.1 Webpage.....	64
3.2.2 Flyer/Leaflet	68
3.2.3 Presentation slides	71
3.3 Communication of the Open Call.....	77
3.3.1 Advertisement of the Open Call.....	78
3.3.1 Online Campaigns	81

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	4 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

3.3.2	Campaign Monitoring	83
3.3.1	Discussion	84
3.4	Dissemination Report	85
3.4.1	Blog with External Events	85
3.4.2	Blog with News	94
3.4.3	Social Media Posts using Twitter, Facebook, LinkedIn, and YouTube	101
3.4.4	Publications	103
3.4.5	SMESEC Workshop	105
3.4.6	KPI.....	105
3.5	Conclusions	107
4	Standardization Activities	109
4.1	Collaboration and Liaison with European Standardization Bodies	110
4.1.1	Investigating European Initiatives and Their Publications on Standardization	110
4.1.2	Identifying WGs and Committees for Cybersecurity and SMEs.....	112
4.1.3	Cybersecurity Standards Workshop and a Survey to Identify Needs and Gaps	113
4.1.4	Establishing Liaisons with the SDOs to Identify the Opportunities for Contribution.....	116
4.1.5	Providing Input for the Needs and the Gaps.....	116
4.2	Studying Existing Cybersecurity Standards for Enhancing SMESEC	116
4.2.1	Shortlist Relevant Standardisation Bodies/Organisations for SMESEC	121
4.2.2	List of Standards Used by SMESEC Tools	122
4.2.3	Identified Opportunities to Contribute Standardisation.....	123
4.2.4	CySME Maturity Model and Standardisation	123
5	Conclusions	131
6	References	132
7	Annex	133
7.1	Annex I IPR Agreement	133
7.2	Annex II Commercial Agreement	138

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	5 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

List of Tables

<i>Table 1: Competitor's Analysis</i>	23
<i>Table 2: Framework Components Pricing Details</i>	36
<i>Table 3: SMESEC Functionalities and Additional Services</i>	42
<i>Table 4: Customer Segmentation Forecast</i>	42
<i>Table 5: Revenue Streams Year 1-Year 3</i>	44
<i>Table 6: Cost Structure Year 1-Year 3</i>	45
<i>Table 7: Loadsensing Go-to-market Strategy</i>	50
<i>Table 8: Customer Segmentation Forecast</i>	51
<i>Table 9: Revenue Streams Year 1-Year 3</i>	52
<i>Table 10: Cost Structure WoS Year 1-Year 3</i>	53
<i>Table 11: Business Model Indicator</i>	57
<i>Table 12: Identified SME associations and status of cooperation as of M24.</i>	60
<i>Table 13: Dissemination message (modifications in comparison to D6.2: SMESEC Framework and Open Call)</i>	62
<i>Table 14: Access and download statistics of the open call.</i>	83
<i>Table 15: Summary statistics for the campaigns on Twitter and Facebook.</i>	83
<i>Table 16: External Events with SMESEC Involvement</i>	85
<i>Table 17: Publications during the year 2.</i>	103
<i>Table 18: Visibility monitoring and related objectives.</i>	106
<i>Table 19: Social network followers by month (*: no final figure available at the time of writing).</i>	106
<i>Table 20: Scientific impact monitoring and related objectives (*: see comment below)</i>	107
<i>Table 21: Relevant standardisation bodies/organisations for SMESEC</i>	117
<i>Table 22: Longlist of Possible Standards related to SMESEC Tools</i>	118
<i>Table 23: Relevant Standardisation bodies/organisations for SMESEC (after the interviews)</i>	121
<i>Table 24: List of Standards used by SMESEC Tools</i>	122
<i>Table 25: CySME Cybersecurity Maturity Model Focus Areas</i>	124
<i>Table 26: The results of ECSO SoTA Search</i>	128
<i>Table 27: ETSI, CEN and CENELEC database search results</i>	129
<i>Table 28: Capability Identified in Different Standards</i>	129

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	6 of 142		
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

List of Figures

<i>Figure 1: Cyberbit – Cyber Security Platform Functionalities</i>	29
<i>Figure 2: GCA Toolboxes</i>	29
<i>Figure 3: Backstory Tool</i>	30
<i>Figure 4: Uppercase Tool</i>	30
<i>Figure 5: Virus Total Tool</i>	30
<i>Figure 6: Fortika Vision</i>	31
<i>Figure 7: Identification of SMESEC stakeholders</i>	34
<i>Figure 8: Business Model Generation Template</i>	35
<i>Figure 9: SMESEC Framework Business Model</i>	41
<i>Figure 10: SMESEC Functionalities</i>	42
<i>Figure 11: WoS Business Model Canvas</i>	49
<i>Figure 12: LoadSensing Customers and Distributors Worldwide</i>	51
<i>Figure 13: Overview of SMESEC dissemination approach</i>	59
<i>Figure 14: Overview of SMESEC dissemination objectives</i>	61
<i>Figure 15: Dissemination plan</i>	62
<i>Figure 16: SMESEC tools presentation on www.smesecu.eu.</i>	68
<i>Figure 17: Call for action.</i>	68
<i>Figure 18: Updated SMESEC Flyer</i>	70
<i>Figure 19: SMESEC General Presentation Slides</i>	77
<i>Figure 20: Open Call Page.</i>	81
<i>Figure 21: Twitter campaign 1.</i>	82
<i>Figure 22: Twitter campaign 2.</i>	82
<i>Figure 23: Facebook campaigns 1 and 2.</i>	83
<i>Figure 24: Snapshots of the SMESEC presence on social channels</i>	102
<i>Figure 25: Demography of Linked-In Followers – company sizes.</i>	103
<i>Figure 26: Two main activities for the standardisation task</i>	109
<i>Figure 27: Revised standardisation plan</i>	109
<i>Figure 28: Top-Down Approach Activities</i>	110
<i>Figure 29: Cybersecurity Standardisation Workshop</i>	114
<i>Figure 30: Bottom-up Approach Activities</i>	116
<i>Figure 31: Semi-structured Interview Protocol</i>	121
<i>Figure 32: CySME Maturity Model</i>	124
<i>Figure 33: CYSEC Tool (from deliverable D 2.3)</i>	126
<i>Figure 34: Relationships between the model components</i>	127
<i>Figure 35: Assessment - Improvement - Standardisation Mechanism</i>	127
<i>Figure 36: The process of selecting standards for the assessment questions</i>	128

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	7 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

List of Acronyms

Abbreviation / acronym	Description
AHPS	Atos High Performance Security
AI	Artificial Intelligence
API	Application Programming Interface
CAGR	Compound Annual Growth Rate
CAPEX	Capital Expenses
DDoS	Distributed Denial-of-Service
DoW	Description of Work
EC	European Commission
ECSO	European Cyber Security Organisation
EU	European Union
GCA	Global Cyber Alliance
GDPR	General Data Protection Regulation
GRC	Governance, Risk Management and Compliance
HTTP	Hypertext Transfer Protocol
HW	Hardware
ICT	Information and Communication Technology
IDS	Intrusion Detection Systems
IEC	International Electrotechnical Commission
IoT	Internet of Things
IPS	Intrusion Prevention Systems
ISO	International Organization for Standardization
IT	Information Technology
IPR	Intellectual Property Right
JV	Joint Venture
KPI	Key Performance Indicators
MBT	Model-Based Testing
OPEX	Operational Expenses
R&D	Research and Development

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	8 of 142				
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

R&I	Research and Innovation
ROI	Return on Investment
ROP	Return Oriented Programming
SBS	Small Business Standards
SDO	Standards Developing Organization
SIEM	Security Information and Event Management
SME	Small or medium-sized enterprise
SSL	Secure Sockets Layer
SoTA	State of the Art
SW	Software
SWG	Secure Web Gateway
TaaS	Test as a Service
TBC	To Be Confirmed
TBD	To Be Determined
TC	Technical Committee
UK	United Kingdom
URL	Uniform Resource Locator
USD	United States Dollar
UTM	Unified Threat Management
VPN	Virtual Private Network
WAF	Web Application Firewall
WG	Work Group
WP	Work Package

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	9 of 142		
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

Executive Summary

SMESEC intends to deliver a lightweight unified framework to ensure cybersecurity of SMEs, which are considered key players towards creating additional value for the technical ecosystem of the European Union. Both privacy and security are considered to be determining factors for massive IT deployments of new connected solutions as well as for the technical update of most of the currently existing industry sectors. Combining consortium member's solutions and benefiting from the experience of 4 use cases in Industrial Internet of Things, Smart Cities, Smart Grid, and eVoting, SMESEC aims at offering to SMEs an advanced cost-efficient and easily accessible solution, which will be operational almost instantly, without an extended security knowledge or a dedicated team.

In this context, the SMESEC consortium designed at M6 an overall strategy to maximize the project audience, prepare the final framework exploitation and efficiently contribute in the related standards. As a parallel activity, SMESEC improves the overall awareness of the SMEs in the cybersecurity domain through a carefully designed and meticulously executed plan, and this is fully synchronised and integrated into the Project's dissemination activities.

This deliverable describes the dissemination, exploitation and standardization activities carried out during the second period (M12 to M24) of SMESEC project, including a refinement of the exploitation roadmap and all communication and standardization actions set to enhance the project impacts already progressed during the last period but which have well progressed during this 2nd period.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	10 of 142		
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

1 Introduction

1.1 Purpose of the document

This document presents the overall second-year results of the SMESEC project in the areas of dissemination (Task 6.1), exploitation (Task 6.2) and standardization (Task 6.3). The information presented includes the contributions from all project partners.

1.2 Relation to other project work

The objective of this subsection is to describe how the present document relates to the DoA, the project roadmap, as well as to other existing deliverables.

1.3 Structure of the document

This document is structured in four major chapters:

Chapter 1 presents the introduction of the document.

Chapter 2 presents the summary of exploitation activities for the period M12-M24.

Chapter 3 presents the summary of dissemination activities for the period M12-M24.

Chapter 4 presents the summary of the standardization activities for the period M12-M24.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	11 of 142		
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

2 Exploitation Activities

In this section, we present the exploitation activities and the results of these activities during the second year of the project.

2.1 Exploitation Strategy

After a closer approach to the exploitation of the developments done by each partner (individual exploitation of the partner's developments by their own) during Year 1, main efforts carried out by the consortium during this project period Year 2 are related to a cooperative transfer to market of consortium developments.

The main topics addressed in this report, as detailed below in the subsection, include:

- Joint exploitation:
 - IPR.
 - Commercial agreement.
 - New legal entity.
- Individual exploitation:
 - Individual exploitation plans (update).

All those activities are still in the negotiation phase. An updated version would be delivered by M36 with the outcome of those discussions.

2.1.1 Joint Exploitation Plan

2.1.1.1 IPR

During this project period Year 2, consortium partners have been working for the generation of an IPR agreement whose sole purpose is to reflect the distribution of the Intellectual property rights by component. This distribution is represented by a % of ownership. The document is currently under discussion and a final version should be ready by the end of the project.

The rationale behind this agreement is to coordinate and agree the distribution of the intellectual property rights between each party and their claims upon the development and contribution they have carried out and expect to do till the end of the project, during the project live span in all components susceptible to have a commercialization and make a profit out of the transfer to the market of such functionalities.

This IPR agreement will be integrated in the commercial agreement as a base line. This commercial agreement is also described in this report and includes a tentative distribution of the compensation per partner in any commercial action that may occur in the future (if finally signed).

Partners have been requested to describe their contribution to the development of each of the SMESEC components:

- In case of one single partner, developing the component the IPR % would be 100%.
- In case two or more partner contribute to this development, that % should be distributed among all contributors after they reach an understanding of that distribution.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	12 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

The current version, still pending to be validated by the consortium partners, is attached to this document as Annex I IPR Agreement.

2.1.1.2 Commercial Agreement

A draft version of a commercial agreement has been designed and distributed among the consortium partners. This agreement includes the roles and responsibilities of each of the signing parts, as long as a compensation scheme based on a multi-angle approach to the activities and efforts carried out by each signing part.

This commercial agreement can be used as a template for any commercial opportunity that could appear in the future for the exploitation of the consortium developments. It also provides a major flexibility as it does not need to be signed by all partners, only the ones that would have the intention to participate in a common exploitation of the results (the range of partner to be included in it goes from bilateral to multilateral agreements).

The current version, still pending to be validated by the consortium partners, is attached to this document as Annex II Commercial Agreement.

2.1.1.3 New Legal Structure

As the last pillar in the discussion of the exploitation strategy conducted during this Year 2 period is the definition and discussion of the generation of legal structure.

Here exist three main options regarding the legal partnership structures:

New Legal Entity (Start Up): This option develops a new legal entity that will be in charge of the commercial SMESEC activities.

Main topics to be addressed by this new legal entity:

- Legal basis (type of entity);
- Legal base (country);
- Business model, business plan;
- Ownership model for the entity (who owns how many shares);
- Governance model (how partners control it).

Owners' IPR would be assigned to the company in return for shares (also, it can be a license in return for fees).

The company then operates as an independent entity and shares its benefits with the company owners. SMESEC project partners can participate in any of those two options:

1. As a shareholder in the company, with its shareholding being related to the ownership of assets assigned to the company.
2. As a participant in the new organization in a variety of activities: management, sales, development, marketing, consulting and delivery of infrastructure resources.

Joint Venture: A joint venture (JV) is a business agreement between two or more partners acting together and sharing resources in pursuit of a business or in relation to a specific project.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	13 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

The partners can contribute in different ways to the joint venture: via assets, investment or skills, sharing risks and benefits, and by taking different levels of responsibility. Revenue sharing and liability sharing would be described in the joint venture agreement. A JV agreement should describe the scope, the management, financial and strategic objectives, the decision-making process, responsibilities of each partner, how to avoid and resolve disputes, how to add or remove entities, partners' rights and obligations and how to share benefits and losses from the JV.

A lighter version of this format would be more similar to a collaborative project with no central office, and participants are assigned on a full/part time basis.

Supply Chain: A supply chain consists of several partners that contribute to delivering a component of product or service.

Main characteristic is that there is no central. In this model each partner would focus on its core competency. Each partner acts as supplier/customer to the following partner to build the supply chain.

An intermediate option is to sign **commercial collaboration agreements** between consortium partners (two or more), targeting specific customer segments (depending on the services offered).

Some partners are exploring different opportunities to collaborate with 3rd parties (external companies to the consortium) alongside with different opportunities to participate in public administration tenders.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	14 of 142		
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

2.1.2 Individual Exploitation

The present section provides the SMESEC partners' individual exploitation updates identified during Year 2. As it was mentioned in D6.2 [2], this document will be updated once the project partners identify any new individual exploitation opportunity for their organizations:

Individual Exploitation Plan of ATOS

1. Partner profile:

Atos is a global leader in digital transformation with 120,000 employees in 73 countries. European number one in cloud, cybersecurity and high-performance computing, the group provides end-to-end orchestrated hybrid cloud, big data, business applications and digital workplace solutions through its Digital Transformation Factory. It also provides transactional services through Worldline, the European leader in the payment industry.

Within Atos Research & Innovation (ARI), node of R&D at Atos in Spain, there exist a key technology transfer and business development team that works on transition from research results to Atos global portfolio and service lines.

2. Your motivation to participate in the project and commitment:

SIEMs are innovative solutions that perform a wide variety of actions in order to detect, correlate, normalize and evaluate information coming from different sources. Such powerful tools need to evolve in order to cope with current and future threats and attacks. The motivation of Atos in the project is to grow our portfolio by enhancing our XL-SIEM solution with detection, reaction and correlation capabilities focusing in the specific aspects of SMEs, which form more than 90% of companies of Europe

3. Means to achieve your objectives:

One of Atos crucial offerings are the Atos AHPS - SIEM and Real-time Risk Management which have successfully secured the Olympic Games since 2002. Also, the cybersecurity department experts involved in the project will help to achieve the project objectives.

4. Opportunity which appeared/appears:

Atos security operators encounter new types of, previously unknown, threats and vulnerabilities. This is further escalated by the rapid growth of technology and data availability. Those factors combined require the solution to be in continuous development in order to keep up with the evolving, complex environment. Also, due to the growing and large sophistication of cyber threats and the criticality of data, it is important for organizations to be aware of their status and perform an in-depth cybersecurity assessment in order to reduce risk levels and increase their cybersecurity maturity. SMESEC developments in cyber security solution focus in the SMEs domain fits in the ATOS Identity, Security and Risk Management commercial portfolio of solutions.

PROFILE AND MOTIVATION

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	15 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

5. **Exploitable assets and results:**

RAE: The RAE provides information of cyber risks from the technical and business point of view, with expectations of costs and impact in the business for the threats. Also, it supports static and real-time analysis, covering not only known vulnerabilities but also zero-day attacks, ADP, etc.

XL-SIEM: Our solution provides, among other characteristics, identification of new and complex attack patterns, high-level risk metrics and correlation rules, user and entity behaviour analytics, support for big data analysis, TLS certification for communication between the agents and SIEM, anonymization and encryption of data, and generation of heartbeats to monitor the status of the agents

6. **Rationale:**

Atos is particularly interested in the outcomes of the SMESEC project as it will bring the necessary improvements and further enhance the AHPS-SIEM offering. Currently the AHPS-SIEM is operated mostly by security engineers that monitor activities from a wide variety of devices and then raise alerts as needed.

Atos will test in XL-SIEM the enhancements provided by the outcomes of SMESEC project, which later on will be introduced in the next-generation SIEM of the company.

The networking generated during this project with SME's associations will extend Atos customer portfolio and this may have additional impacts in other areas of the company (Consulting, software factory, etc.).

7. **Your Value Proposition towards Joint Exploitation of SMESEC:**

Atos SMESEC components will complete the SMESEC framework offer with both components developed, XL-SIEM and RAE. The exploitation of the whole framework will extend the SMESEC offer beyond the individual exploitation of Atos, while XL-SIEM is a key element of the framework.

8. **Roadmap: the timeline plan you have for using those assets:**

Initial presentation of the assets to the Atos innovation board for validation in inclusion in the commercial portfolio.

The management of the Cybersecurity area have been participating in internal meeting with Research and Innovation to identify their current customers' needs and how SMESEC components could be integrated in their portfolio offering.

9. **Measurement:**

Number of commercial opportunities schedule with the company portfolio customers

10. **Positioning:**

Already described in D6.2 Annual report on exploitation, dissemination and standardization (Year 1) in the competitor's section

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	16 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

Individual Exploitation Plan of GridPocket

1. Partner profile:

GridPocket is an innovative software-as-a-service company focused on development of energy value-added services and platforms for the smart grid utilities. The solutions of GridPocket include applications for energy management, demand response control software, M2M and behavioural experts' systems for electricity, water, gas and heating utilities

2. Your motivation to participate in the project and commitment:

Our company seeks an opportunity to enhance security level of our product PowerVAS by leveraging technologies provided by our partners. Moreover, as a company with long R+D background, we strive for opportunity to take a part in a cutting-edge research project in the area of cybersecurity.

3. Means to achieve your objectives:

GridPocket has nine years of experience in the development of software, mostly intended for utilities market. Cybersecurity plays crucial role in developing solutions for our customers, therefore we participate in several research projects in fields related to it. Our team consists of professional and talented developers interested in cybersecurity. We are still improving the security of our inner infrastructure and our security specialist constantly watches over it and prevents any possible threats.

4. Opportunity which appeared/appears:

As already mentioned above, security plays crucial role in our market. This need arises both from necessity to protect our direct customers data, which is utilities companies, as well as the personal information of the end users. Any data leak could compromise our customer and lead to churn increase and financial loses. On the other hand, better data protection translates into higher reliability of our solutions and greater customers loyalty.

5. Exploitable assets and results:

As a part of Smart Grid Pilot program, we implement several technologies into our PowerVAS product. Those are specifically: Citrix Netscaler, Forti IDS and HoneyPot, EGM TaaS, Bitdefender Gravity Zone, Atos XL-SIEM. During this process, we are learning how to combine, integrate and manage all these tools together, to achieve complete security of our application. We are also building the cybersecurity threats awareness among our employees.

6. Rationale:

GridPocket plans to use listed in a previous point asset to improve the cybersecurity and reliance of our product, PowerVAS. This in turn will improve company's reliability and help us gain new customers. Regarding the later exploitation of those assets, limited resources of the company leave no scope for using them to protect company's other products. Decision in this matter will depend on the licenses and exploitation fees of tools, and the future needs of PowerVAS.

PROFILE AND MOTIVATION

WHAT AND WHY

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	17 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

7. Your Value Proposition towards Joint Exploitation of SMESEC:

GridPocket doesn't share any specific component with partners. Company's contribution to the project is implementation and testing the framework in real, production environment and sharing the information and feedback about it. What GridPocket expects from partners the most, is presenting the company as one of the partners which first implemented and validated the framework.

8. Roadmap: the timeline plan you have for using those assets:

- M18-M22: Finalize the integration of tools/framework in PowerVAS (link tools to XL-SIEM, install honeypots and be ready to test PowerVAS API with the TaaS tool.
- M23-M26: Plan training and testing sessions with GridPocket technical team. The training session will make the team aware of the integrated tools, and the testing sessions will help validate that every tool is operating properly. Feedbacks and comments will be provided to the SMESEC framework developers if required
- M27-M30: Work sessions will be scheduled with GridPocket clients to show them the results of the testing sessions. This to make them more confident about the protection of their personal data.

9. Measurement:

GridPocket plan is to run a series of tests examining correct behaviour of each component in situation of various cyber threats. Planned tests will include:

- IDS, WAF and Honeypots will be tested jointly with the same strategy: a penetration test will be conducted on the main endpoint.
- TaaS will be used to test the new authentication micro-service deployed in GridPocket called MS_AUTH. A set of test cases covering user login, logout and general user will be prepared for both normal and privileged user.
- Bitdefender tests are not precise yet, but probably some test virus signature will be deployed, to check whether it is detected
- XL-SIEM will be tested with penetration tests, to check if it's providing relevant alerts

10. Positioning:

As already mentioned above, GridPocket is not providing any specific asset to a project, so it's not possible to provide any comparison in this matter.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	18 of 142		
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

Individual Exploitation Plan of Scytl

1. **Partner profile:** Scytl is the worldwide leader in secure electronic voting, election management and election modernization solutions. Its solutions incorporate unique cryptographic protocols that ensure maximum security, transparency and auditability in all types of elections. Scytl's ground-breaking electoral security technology is protected by international patents and it enables organizations to electronically carry out all types of electoral processes in a completely secure and auditable manner, positioning the company as the global leader in this industry.
2. **Your motivation to participate in the project and commitment:** Within SMESEC, Scytl will be able to update its security solutions with more efficient mechanisms. The proposed real-life experimentations will evaluate the SMESEC framework for the e-voting use case. The identified most cost-effective cyber-security mechanisms will be integrated on the commercial offer of Scytl to provide more functionality and lines of protection for Scytl's clients.
3. **Means to achieve your objectives:** Because of its expertise, Scytl is the internationally recognized leader in secure election management and electronic voting solutions. Over the last 10 years Scytl has electronically managed over 100,000 electoral events across more than 20 countries, including the USA, Mexico, France, Norway, Switzerland, Austria, BiH and India. Founded in 2001 as a spin-off from a university research group, Scytl has a strong commitment to R&D. Its current patent portfolio is the largest in the industry and is composed of more than 40 international patents in security applied to election processes.

Scytl's solutions have been audited by independent organizations and by academic experts in the field of election administration that have consistently found its security and technology to be reliable and compliant with the highest security standards currently established. Scytl has capitalized on its 18 years of research experience to develop ground-breaking cryptographic protocols that secure the election registration, voting and results consolidation processes and are patent-protected. Scytl's technology and software are also protected by copyrights.

4. **Opportunity which appeared/appears:** the main goal is to increase the security at the infrastructure level, as it currently is at application level only. Scytl will be able to offer its e-Voting service combined with a robust security framework that will allow SMEs and public authorities to implement high-level security measures in their election processes without requiring a large budget. Such approach will help these entities to carry out secure consultation processes even with limited budgets.
5. **Exploitable assets and results:** Cost-effective cyber security mechanisms and training opportunities for SMEs. SMESEC will provide the security layer for hardening, monitoring, attack detection and prevention as well as a method to ensure the availability of the election process. The integration of both technologies will provide a joint solution that will allow entities with limited budget to implement secure online voting processes

WHAT AND PROFILE AND MOTIVATION WHY

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	19 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

with the highest levels of security, availability and transparency. Moreover, SMESEC will address the requirement for last minute code and service modifications to meet the peculiarities of each specific voting process.

6. **Your Value Proposition towards Joint Exploitation:** the delivery of the framework that can be integrated in the system based on our customers' needs. A use case will be provided by Scytl for testing purposes. The goal is to help local authorities and small public entities to improve and maintain the security controls of their ICT infrastructures with particular interest on last minute code and service modifications to meet the peculiarities of specific requirements.

**ROADMAP WITH
TIMELINE**

7. **Roadmap:** In M25 (TBC) the second prototype will be ready for the validation with the pilot.

8. **Measurement:** A plan to measure the impact of planned actions is still to be agreed and finalised.

9. **Positioning:** N/A

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	20 of 142		
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

Individual Exploitation Plan of FHNW

PROFILE AND MOTIVATION

1. Partner profile:

FHNW is a university of applied sciences with extensive experience ICT-related teaching and Swiss, European, and Global R&I projects.

2. Your motivation to participate in the project and commitment:

Research and development of a Cybersecurity Coach software (CYSEC).

3. Means to achieve your objectives:

Research and development team, personal network of Swiss SMEs and cybersecurity experts.

4. Opportunity which appeared/appears:

FHNW intends to exploit CYSEC by integrating it into a commercialization entity (startup or existing company). Further, project applications have been submitted to extend the CYSEC capabilities and adapt it to new domains.

5. Exploitable assets and results:

c.f. IPR Sheet.

6. Rationale:

Academically: research vehicle for inquiring cybersecurity practice adoption and adherence by SMEs.

Industrially: offer do-it-yourself capabilities to SMEs as a commercial solution and accompanying consultancy. In addition, we consider standardized education as an option.

7. Your Value Proposition towards Joint Exploitation of SMESEC:

8. Expectations: joint use and evolution of SMESEC homepage, availability of SMESEC tools on SME-compatible terms and integrated into the SMESEC framework.

9. Offering: SMESEC.EU and SMESEC Framework-Frontend use with maintenance and hosting under reasonable commercial terms, CYSEC use for SME guidance for SMESEC Framework tool adoption with maintenance and hosting under reasonable commercial terms.

10. Roadmap: the timeline plan you have for using those assets:

End of project: Integration of FHNW IPR in a commercialization entity.

11. Measurement:

#of SME adopters, #average number of questions answered by SMEs, average maturity level of SMEs (and change of the maturity over time).

12. Positioning:

TBD

WITH WHAT AND WHY

ROADMAP
TIMELINE

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	21 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

2.2 Business Plan

2.2.1 Summary

During Year 2, the market monitoring has continued, and updates have been described in this report in the following domains:

Market monitoring

- Supply side. Competitors.
- Demand side. Market needs.
- Stakeholder analysis.

Business models

- Business Model Canvas SMESEC framework.
- Business Model Canvas SMESEC pilots.

2.2.2 Market Monitoring

The market will be continuously monitored during the project lifespan and any update or new players that prorogue some significant impact on the analysis, would be reported in the forthcoming exploitation documents (D6.4) due by M36.

A detailed market analysis was conducted during Year 1 and the main outcomes were detailed in D6.1 [3] and D6.2 [2]. During this Year 2 period the consortium has focused its monitoring activities in both supply and demand sides of the market and the main conclusions are detailed in the following subsections.

2.2.2.1 Supply Side: Competitors

The unified SMESEC framework, as the integration of multiple products residing in several segments of the security market, competes directly with many third-party solutions.

During Year 1, an extensive Competitors analysis was conducted [2]. During this Year 2 this competitors' landscape has been monitored and each competitor previously identified has been reviewed again for identification of any enhancements they have included in their solutions. The information has been updated in Table 1 below.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	22 of 142		
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

Table 1: Competitor's Analysis

Market	Name of competitor solution	Company	Strengths	Weaknesses
Intrusion Detection and Prevention Systems	FirePower	Cisco	Covers all standard threat protection	High-availability setup, Alerting; Inspect VPN traffic, Blocking traffic
	Network Security Platform	McAfee	Covers all standard threat protection	Inspect VPN traffic, L2 ARP attacks; Blocking traffic; Log searching
	Security Network	IBM	Complete traffic filtering	Cannot add exceptions; No detect and prevent mode
	TippingPoint	TrendMicro	Complete traffic filtering; Administration and reporting	Cannot create own signatures
	NIPS6000	Huawei	Complete traffic filtering	Cannot add exceptions; No detect and prevent mode
Security Information and Event Management	ArcSight	HPE	Excellent Event Detection, Analytics, Visualization; Compliance; Workflow management	No cloud services support; Not intuitive dashboards
	Qradar	IBM	Excellent Event Detection, Analytics, Visualization; Workflow management	No cloud services support; No unlimited correlation rules; Not automatic compliance monitoring
	Security SIEM	Intel	Compliance; Metrics and Dashboards	Not storing network flow data; No advanced correlation rules; No behaviour-based anomaly detection; Not flexible alerting

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	23 of 142
Reference:	D6.3	Dissemination:	PU
	Version:	1.0	Status: Final

	LogRythm	LogRythm	Metrics and Dashboards	No advanced correlation rules; No behaviour-based anomaly detection; Not flexible alerting; No incident life-cycle management
	Splunk Security Intelligence	Splunk	Metrics and Dashboards	Support for custom meta-data fields; Log normalization; Support for Statistical-based and Heuristic correlation; No incident life-cycle management
	Log & Event Manager (LEM)	SolarWinds	Metrics and Dashboards	No advanced correlation rules; No behaviour-based anomaly detection; No incident life-cycle management
Endpoint Detection and Response	Carbon Black	Carbon Black	Excellent detection, containment and remediation; Investigation tools	Botnet detection; No support for MacOS, Android, VMs
	AMP	Cisco	Very good detection; Scanning VMs	Botnet detection; No support for MacOS, Android,
	Crowdstrike	Crowdstrike	Good detection; Some investigation capabilities	Botnet detection; No advanced containment; Only Windows/Linux
	FireEye	FireEye	Malware; Some investigation capabilities	Botnet detection; Restricted containment and remediation; Windows only
Application Security Testing	Fortify	HPE	Excellent static and dynamic analysis; Excellent mobile	-

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	24 of 142
Reference:	D6.3	Dissemination:	PU	Version:	1.0
				Status:	Final

			app security; Very good integrations	
	Security AppScan	IBM	Mobile App security testing; Very good static and dynamic analysis; Integrations	No API/framework support; No parallel testing;
	Veracode	Veracode	Mobile App security testing; Very good static and dynamic analysis; Integrations	No API/framework support; No support for mobile device languages; No parallel testing; No behavioural analysis for mobile; Integration with MDM vendors
	Sentinel	Whitehat security	Mobile App security testing; Very good static and dynamic analysis; Integrations	Support for composite applications; No Windows mobile support;
Web Application Firewall	SecureSphere	Imperva	Great general functionality and integrations	Protection against network-layer DoS; Application Load Balancing
	DenyAll	DenyAll	General functionality	No file upload controls; No protection for buffer overflows; No explicit protection against business logic attacks; Little integration capabilities
	BIG-IP Application Security Manager	F5	Great general functionality and integrations	No file upload controls; Protection against SANS top25 programming errors
	Trustwave	Trustwave	General functionality	No SSL offload support; No protection against

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	25 of 142
Reference:	D6.3	Dissemination:	PU	Version:	1.0
				Status:	Final

				business logic attacks; Lacks some integration capabilities
	WAF	Barracuda Networks	Great general functionality	Lacks virtual patching; Protection against buffer overflows
Unified Threat Management	FortiGate	Fortinet	Excellent threat protection, web security, network firewall;	Lacks email security, Web Application Firewall; No support for Mac
	SG Series	Sophos	Network firewall; Web Security; Device support	File sandboxing; Malware prevention; outbound spam protection
	SonicWALL	SonicWALL	Excellent web security and network firewall; Overall device support	Lacks network and cloud-based sandboxing; Email content filtering and outbound spam protection;
	Meraki MX	Cisco	Great email security and network firewall; Device support	No SSL forward proxy and decryption; Lacks network and cloud-based sandboxing; No available as virtual appliance
	UTM SRX series	Juniper	Email and web security;	No IPv6 support; Support only Windows, Android, iOS
Governance, Risk Management and Compliance	Archer eGRC	EMC-RSA	Excellent Policy, Risk, Compliance, Audit, Threat & Vulnerability, Incident Management;	Limited support for policy templates, customized alerts
	OpenPages	IBM	Risk, Compliance, Audit, Incident management	Lacks contract management (vendor risk); No ticketing

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	26 of 142
Reference:	D6.3	Dissemination:	PU	Version:	1.0
				Status:	Final

				system integration and custom alerts
	MetricStream	MetricStream	Policy, Compliance, Audit, Incident management; Excellent platform integrations	No contract management, risk assessment questionnaires
	Enterprise GRC	RSAM	Compliance, Threat & Vulnerability, Incident management;	No ticketing system integration and contract management; No workpaper management; No Key Risk Indicators (KRI) library
	Risk Vision	Risk Vision	Policy, Compliance, Threat & Vulnerability, Incident management	No Audit management, limited vendor-risk management; No KRI library and assessment questionnaires
Deception Technology	Attivo Networks	Attivo Networks	Identify without known patterns; Great deception techniques; Multiple environments and integrations	Does not protect from MitM, Spear Phishing attacks; no advanced malware protection/sandboxing
	IllisionBLACK	SmokeScreen	Great deception techniques; Multiple environment, deployment types, integrations	No Ransomware protection;
	Deception Grid	TrapX	Many different deception types; Integrations	No dynamic deception updates; Some limited functionality in alerts and general features;

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	27 of 142
Reference:	D6.3	Dissemination:	PU	Version:	1.0
				Status:	Final

	Mazerunner	Cymmetria	All deception types	Deployed only on-prem; No insider threats; Some limited functionality in general features
Secure Web Gateway	Zscaler Web Security	ZScaler	Threat protection; Web Traffic Control; DLP; Integrations	Lacks multiple deployment options (Cloud only)
	Triton AP-Web	ForcePoint	Threat protection; DLP; Deployment options; Integrations	No Botnet defence; No shadow IT discovery
	Web Security Appliance	Cisco	Malware protection; Integrations; Deployment options;	No Botnet defence; No compliance reporting templates; No hybrid (on-prem, cloud) offering
	Web Security	Kaspersky	Threat protection; Complements existing gateway-level defences; internet resource usage control for reducing exposure	No Botnet defence; No hybrid (on-prem, cloud) offering
	Web Security	McAfee	Web Traffic control; DLP; Deployment options	Botnet defence; Mobility support for Web Traffic Control
	Web Security	Symantec	Botnet and malware defence; deployment options	Fewer integrations; no cloud-based sandboxing
	SWG	TrustWave	Malware protection; Web Traffic Control; DLP;	No Botnet defence; No shadow IT discovery; No Cloud or Hybrid deployment support

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	28 of 142		
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

Also, other solutions related to the cybersecurity domain have entered the market, in a similar format (platform) as SMESEC. Some of the identified ones are detailed below:

1. Cyberbit [7] a solution for security orchestration, focused on enterprise level security / Cyber Ranger training simulation / ICS/SCADA security / End point detection and response.



Figure 1: Cyberbit – Cyber Security Platform Functionalities

2. **GCA Cybersecurity toolkit** [9] Improving company’s cybersecurity with a basic toolkit on a free basis. GCA has developed and assembled several tools that can be self-implemented by the SMEs, free of charge.

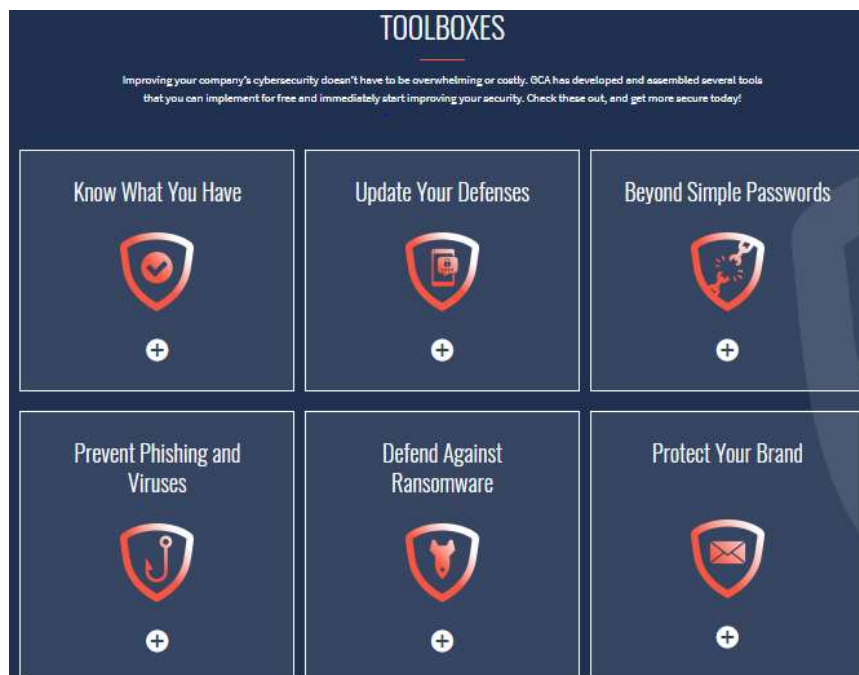


Figure 2: GCA Toolboxes

On September 16, 2015, the **Global Cyber Alliance** was formed to address systemic cyber risks through a proactive risk-based, solution-oriented approach to address and eradicate malicious cyber risks.

GCA also provides other tools to enhance SMEs cyber-security:

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	29 of 142	
Reference:	D6.3	Dissemination:	PU	
	Version:	1.0	Status:	Final

- A solution for email authentication protocols and adds reporting and compliance (DMARC). Free
 - Users protection from accessing known malicious websites (Quad9). Affordable price
 - Website evaluation and removing potential vulnerabilities. (McScrapy)
3. Chronicle [10]Security intelligence products that work together. The 3 products are:
- Backstory: Telemetry storage for one low, fixed price.

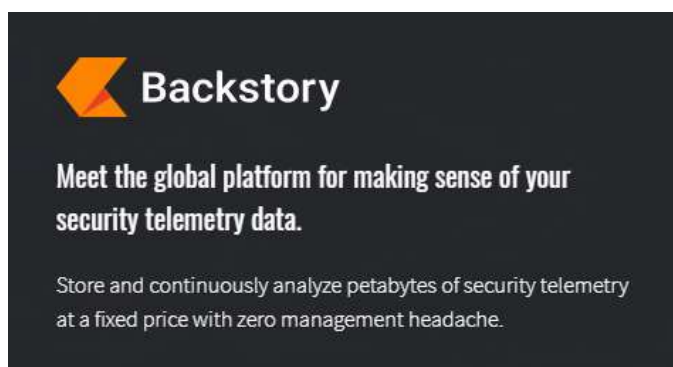


Figure 3: Backstory Tool

- Uppercase: novel tools and techniques to detect emerging threats



Figure 4: Uppercase Tool

- Virus Total: multi-scanner malware insights. (Freemium & premium -API- versions)



Figure 5: Virus Total Tool

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	30 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

4. Fortika [19]. Cyber Security Accelerator for trusted SMEs IT Ecosystems



Figure 6: Fortika Vision

This H2020 cyber-security project can be described as a “brother” project due to its similarities with SMSEC. The FORTIKA project aims at designing a hybrid security solution combining hardware and software in order to protect the assets of the SMEs. Also, FORTIKA proposes a marketplace where various security bundles will be hosted.

As a relevant difference it can be highlighted that:

*“A SME seeking for protecting its network and which has already **put in place** the FORTIKA Gateway (hardware) **in its premises**, will just need to download from the marketplace the security bundles it needs, **install these bundles, and configure them**”.[19]*

This self-service approach will jeopardize the use of those security bundles to any non-self-sufficient, from a technology knowledge point of view, SME.

Although the business model of these solutions (targeted customer segments, deployment, value propositions or revenue structures) do not perfectly match the SMESEC approach, the main **lessons to be learnt** can be summarized in the tips below:

- Reduce Escalations

Empower tier-1 analysts by centralizing IR management, automating manual tasks and simplifying investigations. Reduce escalations by 50% to allow tier-2 and 3 analysts to focus on critical incidents

In the SMESEC case, we can offer this IR management simplification and also offer connecting the SME with tier-2 and 3 analyst services.

- Reduce mean time to respond

The "reduce mean time to respond" is also critical for SME's since they probably have no response plans at all. (here, we will have to come up with default processes.). Side benefits (i.e. "Fast Incident Response can save GDPR fines") [8]

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	31 of 142	
Reference:	D6.3	Dissemination:	PU	
	Version:	1.0	Status:	Final

- Communication pitch

The "focus on what's important" pitch, is a great example about what the consortium can be focus on to trigger SMEs interest/attention (i.e. training & awareness based on business-critical and actual-risks for the SME).

- Budget impact (low or free)

This “cost friendly” approach can be a trigger to attract SMEs to be curious about cybersecurity and specifically about what can SMESEC offer to them.

2.2.2.2 Demand Side: Market needs

As part of the yearly market monitoring activities, the latest market forecast continues showing a growing market in cybersecurity. Allied Market Research valued the cyber security overall market size at \$104.60 billion in 2017 and projects it to reach \$258.99 billion by 2025, growing at a CAGR of 11.9% from 2018 to 2025” [6].

Also, due to frequent cyber-attacks, such as Shadow Brokers, WannaCry, and Petya, private organizations are increasingly deploying security solutions to protect their IT infrastructure. Also, with the growing popularity of the bring your own device (BYOD) among start-ups and SMEs around the world, the need to secure different types of devices used within the business networks is leading to the rapid deployment of antivirus/antimalware solutions by businesses worldwide.

The global enterprise endpoint security market was valued at US\$6.645 billion in 2017 and is projected to expand at a CAGR of 6.60% over the forecast period to reach US\$9.750 billion by 2023. Endpoint security is the process of securing the various endpoint on a network, often defined as end user devices such as mobile, laptop, and desktop among others. Endpoint security aims to adequately secure every endpoint connecting to a network to block access attempts and other risky activity at these points of entry. The gradual increase in the mobile threats has led to significant adoption of endpoint security solutions.

The software segment held a market share of over 80% due to the large-scale deployment of protection solutions such as intrusion prevention systems, antivirus systems, and endpoint application control systems by businesses to prevent malicious threats from infecting their networks.

For the SMEs cybersecurity landscape this translates into the following needs:

- Managing the external threats - Facing the pressure of business digitalization, the vast majority of SMEs are dealing with social collaboration, expanding the use of mobile devices, moving the storage of information to the cloud, digitizing sensitive information and embracing workforce mobility alternatives. This dynamic opens the door for automated exploits of known vulnerabilities, malicious files enclosed as email attachments or botnet attacks against the company website.
- Tackling the internal ignorance – Quite often the start-ups and SMEs are approaching the cybersecurity challenge fighting first with their own employees, as the vast majority is not fully aware of the risks their organizations are facing when going online. Thus, reckless web surfing which affects company network with bot clients, Trojans, spyware and different kinds of malware, reckless use of Wi-Fi hotspots or reckless use of hotels unprotected networks are some

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	32 of 142		
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

of the incidents triggered by the employees' online behaviour with significant consequences on organizational level.

- Implementing comprehensive cyber security strategies and approaches that reduce organizational risk – It became almost mandatory even for the smallest businesses to design internal strategies to regulate the actions when trying to preserve their cyber-integrity.
- Fighting for budget and resources – Even in 2019, a significant percentage of SMEs decision-makers are considering cybersecurity as an IT issue rather than an organizational governance issue and consequently they are setting-up smaller budgets compared with the real needs. Also, it is common that the low number of technical staff can't support the necessary increasing activities to preserve the cyber-integrity of the businesses (i.e. not installing the latest versions of software).

At this respect, SMEs are trying to enhance their monitoring and response capabilities accordingly to the increasing cybercrime activities. A recent study carried out by 451 Research [12] shows a significant increase (14%) in SMEs cybersecurity budgets. Although budget and expertise constraints are still the main barriers for this type of companies [14].

- Almost 86% of SMEs have less than 10% of their IT budget allocation dedicated to cyber security
- 75% of SMEs have less than two IT staff dedicated to cybersecurity.

All this “resource escalation” is a natural reaction to the counterpart: Cybercrime is on the rise. According to latest “Cost of Cybercrime Study”, Accenture 2018 [11], all main cybercrime domains have experienced a significant increase during 2018 (ranges from 8% Phishing to 21% Ransomware)

2.2.2.3 Stakeholder Analysis

The main progress during Year 2 in this analysis have been:

- Initial contacts with the most relevant stakeholders. These are the stakeholders that have been identified to have high power and high interest (Players) in the Mendelow Matrix presented in the report D6.2 [2]
- Get a deeper understanding of the various identified stakeholders (e.g. generic SME, High Tech SMEs, SME with cybersecurity awareness, etc.) and start mapping and understanding their positioning around SMESEC project. This could include but is not limited to evaluating their degree of influence, the degree of importance, and their points of interest and prioritizing them.

To strengthen the analysis, during Year 2 a direct interaction with stakeholders has been initiated. This gave the consortium the opportunity to update the analysis and start defining a more accurate stakeholder model. Many of these initial interactions has been conducted during the dissemination activities planned for Year 2, which include workshops and presentation in the main project-related events. Below is there the updated resume of the initial SMESEC 3 main stakeholders' groups in Figure 7.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	33 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final



Figure 7: Identification of SMESEC stakeholders

- Active stakeholders, mainly the SMEs. We identified several types of SMEs in particular High-tech SMEs we met at several events and through high tech association such as Praxis in Greece. we contacted general and non high-tech SMEs in particular through SMEs associations such as ONTPE in France, PLANETIC in Spain, Schweizerischer KMU-Verbandin Switzerland or Digital SMEs alliance in Europe. We also contacted personnel of public administration where we exchange on cybersecurity matters with a specific questionnaire.
- Enabling stakeholders, who add or provide to the expansion and use of SMESEC framework (who would be a part of the dissemination of this technology –media- or policy, subsidy, or regulations makers that would promote or recommend consumers and providers into using this technology -Public Institutions-). In addition, we identified enabling stakeholders who take part in the SMESEC environment (they are either a part of the ‘consumption’ of SMESEC services or providing SMESEC services (development, maintenance, consultancy, etc.). We met several Security consulting providers or Security related cluster (e.g. SCS Cluster in France) interested by SMESEC as they also advise a large number of SMEs.
- Internal stakeholders involved in the development and establishment of SMESEC (consortium partners). As part of the joint exploitation, partners have initiated discussion around the IPR and commercial agreements to extend the project activity beyond its lifespan.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	34 of 142	
Reference:	D6.3	Dissemination:	PU	
	Version:	1.0	Status:	Final

2.2.3 Business Model

This deliverable D6.3, as a report document, shows the progress done in the business plan which describes the rationale of “how an organization creates, delivers, and captures value”. This intermediate report shows the progress done by the consortium partners on the generation of the business models.

The methodology used in this sub-section is the Canvas model [1] (nine basic building blocks focus on how a company will make viable its business model). The nine blocks cover the four main areas of a business: customers, offer, infrastructure, and financial viability. Figure 8: Business Model Generation Template, presented below takes on a more general and visual perspective:

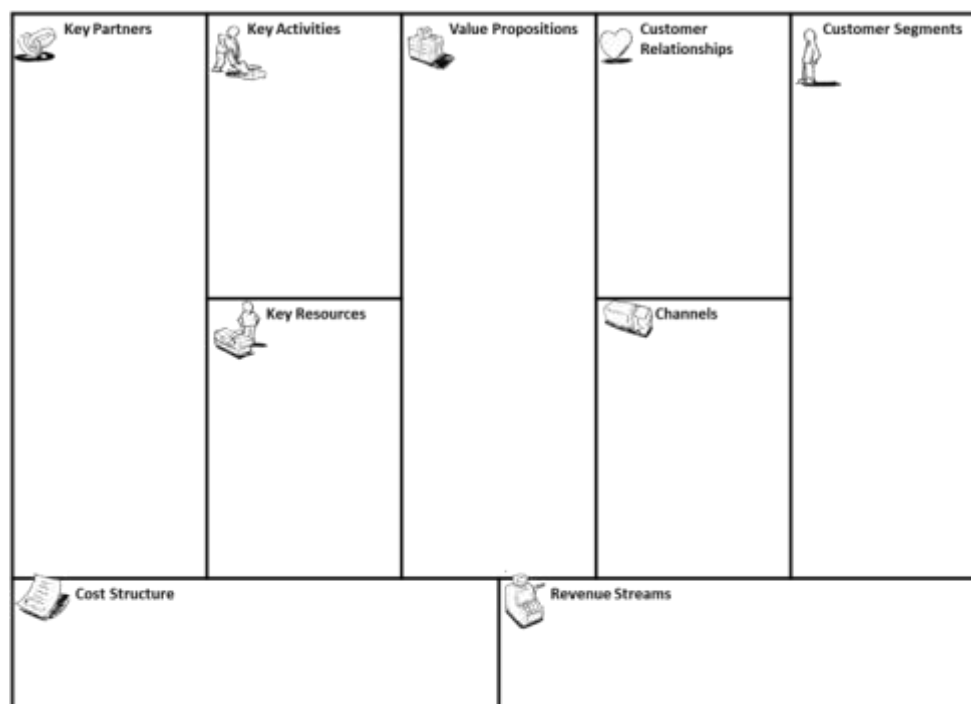


Figure 8: Business Model Generation Template

As part of the SMESEC overall business plan, the consortium has prepared the business model proposal which objective is to ensure it would be profitable enough to be implemented aligning it with real market needs in the EU and beyond. The main purpose is to help transform the innovation of SMESEC into tangible market uptake prospects in targeted market segments. The fine grain Canvas model will be provided in the final deliverable from a **bi-angled approach** (SMESEC **framework** and **pilots**).

This D6.3 includes an update of the business model framework approach and a detailed version of one of the business models’ pilots’ approach. The other pilots’ models are also ready in a draft version and will be refined in the coming months.

All financial information described in the models is a fair assumption of the current market needs, based on direct expertise, feedback from the dissemination and communication activities and they can be modified with updates or changes once a commercial opportunity will be clearly identified.

During the sustainability phase, the business plan will be a reference to ensure that the technical dimension, as it evolves, will fully focus on the market needs.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	35 of 142
Reference:	D6.3	Dissemination:	PU
		Version:	1.0
		Status:	Final

2.2.3.1 SMESEC Framework Business Model Canvas

As it has been mentioned in Year 1 report, the Consortium has continued the preparation of this business model proposal, to ensure it would be profitable enough to be implemented aligning it with real market needs in the EU and beyond. The main purpose is to transfer the innovation of SMESEC into the market accommodated to the specific needs of the target market segments.

Efforts during this Year 2 period have been focussed on the definition of the value proposition (which are the key components must be included in the SMESEC framework) alongside with the costs and revenue streams. Pricing structures is also ongoing and under discussion.

At a later stage of the project (to better accommodate to the specific market needs), a business model canvas per component could be developed, if necessary

The current work around the business model is focus on the identification of which are, out of all the developments, the more mature enough, different types of versions (from free to full or premium) to be included at an early stage in the framework and other information needed to address the building blocks of the canvas methodology. The pricing structure per component will provide the basis to generate the framework pricing options once SMESEC is offered in the market. Table 2 below reflects the work done until this moment:

Table 2: Framework Components Pricing Details

Component	Pricing structure	Cost structure	Freemium version	Premium version
AngelEye				
Risk Assessment Engine (RAE)	As a Service (due to the expertise needed to manage the tool	Outsourcing service FTE rate (upon request): 400€/day; Consulting (upon request) 450€/day Hardware costs between 200-500€/month depending on the systems demands		
EGM-TaaS	Basic on-the-shelves tests suites monthly subscription Advanced on-the-shelves tests suites monthly subscription	basic= 1K monthly advanced= 2 to 5K Monthly on demand= basic specific 5K flatsum - other 500/day expertise= 500 euros/day	1month free try possible	paid services after free try

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	36 of 142
Reference:	D6.3	Dissemination:	PU	Version:	1.0
				Status:	Final

	Specific on demand conformance tests/interoperability plan expertise			
Anti-Rop				
ExpliSAT				
Citrix Web Application Firewall (WAF) Citrix Secure Web Gateway (SWG)"	Free Trial edition (90 days) Freemium (VPX Express) Standalone Citrix ADC VPX License	Third party cloud infrastructure is charged separately. i.e. AWS: https://aws.amazon.com/marketplace/pp/B0796LD46X MS Azure: https://azuremarketplace.microsoft.com/en-us/marketplace/apps/citrix-netscalervpx-120?tab=PlansAndPrice	Citrix ADC VPX Express Up to 20Mbps bandwidth Maximum 250 SSL sessions 20 Mbps SSL throughput https://www.citrix.com/lp/try/citrix-networking-vpx-express.html	Citrix ADC VPX License Ranging from: USD 2440 (ADC VPX Standard - 10Mbps) to USD 43920 (ADC VPX Platinum - 3000Mbps) https://store.citrix.com/
Citrix Gateway	Available via Citrix Cloud, bundled with other products Available for purchase as standalone license (https://www.citrix.com/buy/licensing/product.html)	N/A	N/A	Citrix Gateway License: USD 995 https://store.citrix.com
Cross-layer SIEM (XL-SIEM)	As a Service (due to the expertise needed to manage the tool	Outsourcing service FTE rate (upon request): 400€/day; Consulting (upon request) 450€/day		

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	37 of 142
Reference:	D6.3	Dissemination:	PU	Version:	1.0
				Status:	Final

		Hardware costs between 200-500€/month depending on the systems demands		
End Point Protection Platform (GravityZone)	<p>Price varies according to some variables:</p> <ul style="list-style-type: none"> • size of the customer • the number of end-points protected by the solution, • length of the subscription period • complementary services like after-sales tailored training and/or support etc. <p>Examples:</p> <ol style="list-style-type: none"> 1. a set-up comprising up to 6 servers and 20 end-points costs EUR 455 for a period of 1 year. 2. Another example shows that a more complex set-up, comprising up to 26 servers and 82 devices costs EUR 1.660 for 1 year or EUR 3.320 for 3 years. 	EUR 1.750 for 1 day of tailored assistance	Free version, including all the protective features, for a period of 30 days.	Sold according to the pricing structure described within the designated column.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	38 of 142
Reference:	D6.3	Dissemination:	PU	Version:	1.0
				Status:	Final

EWIS (Early Warning Intrusion Detection)	Free: upon request	Maintenance rate (upon request):400€/day; Consulting (upon request) 450€/day	free	free
Cloud-based IDS (Intrusion Detection System)	Free: upon request	Maintenance rate (upon request):400€/day; Consulting (upon request) 450€/day		
CYSEC				
CYSEC Framework	Free: fast ramp-up coaches Each additional coach: 5€ per month All coaches: 45€ per month Private on-premise: 10€ per year	Hosting: 10k€ per year; Maintenance: 20k€ per year (20%FTE)	fast ramp-up coaches; SaaS or on-premise with anonymous profile sharing to community	all coaches; private on-premise as an option
CYSEC Content				
Training platform	Free	Additional services Deployment, Maintenance, Consulting (upon request): 450€/day	N/A	N/A

This description is an initial approach to the pricing structure and could be modified depending on partner's needs (or additional non-foreseen cost) that may impact their profit & loss models.

On the other hand, the approach to the transfer to the market of the SMESEC solution will be based on the following three main commercial lines, regardless of any other commercial opportunity the consortium considers interesting:

- SMESEC Framework (based on the customer expertise and preferences)
 - SECaas. Outsourcing more specific cybersecurity services allows the in-house IT teams to focus on their BAU activities.
 - In-house deployment. SMESEC framework will be run and operated in the customer's premises. Experts support can be also provided
- 3rd party's application hosting. SMESEC framework will be available, via API, to external Service Provider's applications as a market place to distribute their cybersecurity components to SMEs.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	39 of 142		
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

- SMESEC Hub. Access to the data base repository of the Hub for analysis purposed (GDPR regulation compliance). This could also imply a % discount in the user’s license willing to provide this data

In order to fulfil one of the key project drivers (“budget friendly”), the SMESEC framework has been initially segmented in three commercial packages, based on three different combinations of components that could be provided to the customers. These models are limited in number due to technical efficiency and try to accommodate and anticipate as much as possible to the future customer needs.

- Framework Basic. Limited framework functionality which includes some functionalities of SMESEC framework:

EWIS, Training platform, XL – SIEM, GravityZone






- Framework Premium. Limited framework functionality which includes additional SMESEC components to the basic version:

NetScaler, Angel Eye, RAE

- Framework Security in Code. Full framework functionality which includes all SMESEC components:

Anti-Rop, TaaS

This package distribution could be modified at a later stage depending on technical constraints, if any, not yet identified. The following sub-section describes the consortium approach to the SMESEC business model and the impact of the different building blocks of the Canvas model.

Key partners	Key activities	Value proposition	Customer relationship	Customer segmentations
 1 ATOS 2 WOLDSENSING 3 UoP (Patras) 4 FORTH 5 EGM 6 SCYTL 7 GRIDPOCKET 8 FHNW 9 CITRIX 10 IBM 11 BITDEFENDER	 <ul style="list-style-type: none"> • <i>Market Analysis</i> • <i>Consulting</i> • <i>Integration/ Implementation</i> • <i>Dissemination/ Awareness</i> • <i>Presales</i> • <i>Customization</i> • <i>Training</i> • <i>Maintenance</i> 	 Customer needs <ul style="list-style-type: none"> • <i>Increase level of security against cyber-security threats</i> • <i>Budget and knowledge accommodated to SMEs restrictions</i> Services	 <ul style="list-style-type: none"> ➤ <i>Personal assistance</i> ➤ <i>Self-service</i> ➤ <i>Automated services</i> 	 1-Vertical approach <ul style="list-style-type: none"> • <i>Smart-City</i> • <i>Internet of Things (IoT)</i> • <i>e-Voting</i> • <i>Smart Grids</i>

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	40 of 142		
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final



Figure 9: SMESEC Framework Business Model

The consortium approach to this business model envisages a commercial opportunity which will be analysed and develop (if appropriate after the project ends) and will lead SMESEC into a sustainability phase beyond the project lifespan.

Although the current consortium approach aims for a SMESEC commercialization, any business opportunity would be taken into consideration and the consortium would do its best to accommodate to the customer needs. This would lead to a tailor-made SMESEC components integration that would be addressed once the opportunity pops up.

The following building blocks descriptions are based on the consortium assumptions related to market penetration and customer acceptance and try to reflect in a fair manner the commercial viability of the SMESEC as a profitable business model. Cost and revenue stream are not yet calculated as there are still some discussions going on around pricing, framework packages and the roles of each partner in a commercial exploitation. During Year 3, those topics would be clarified and a forecast of the financial viability, based in a fair assumption of costs and incomes, would be generated.

2.2.3.1.1 Value Proposition

Which is the **added value** SMESEC can provide and a user would be **willing to pay for it?**

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	41 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

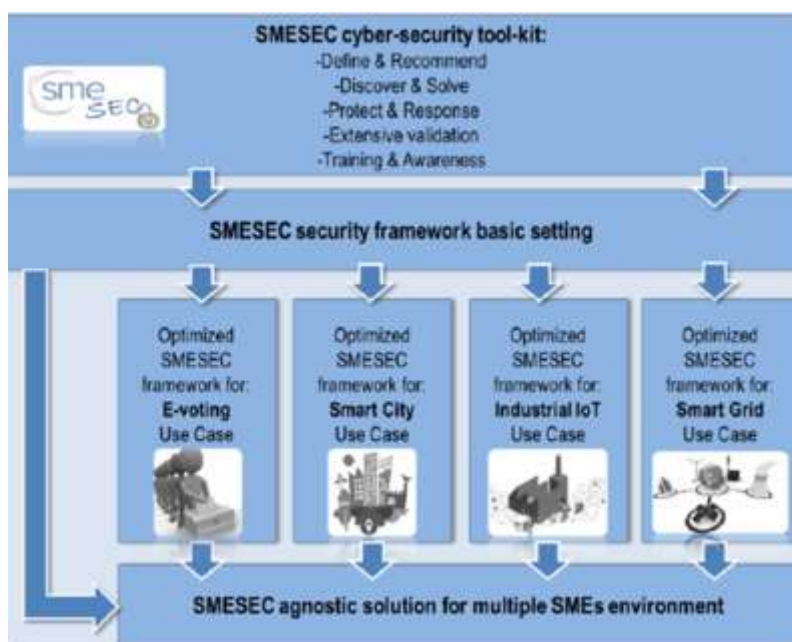


Figure 10: SMESEC Functionalities

“Improve the level of security and protection against cyber-security threats of today smart service and product provided from SMEs to European end-users (big companies and infrastructure, citizens, public administration, etc.).

Table 3: SMESEC Functionalities and Additional Services

Pillars (main functionalities)	Additional Services
SMESEC Framework	Implementation & deployment Consulting Training Application hosting Information Data Base access/sharing

2.2.3.1.2 Customer Segment

Which are the **different target groups** of people or organizations in order to provide SMESEC as a product/service? For whom are we creating value? Who are our most important customers? The main targeted groups are described in Table 4 below.

Table 4: Customer Segmentation Forecast

Concept	Year 1	Year 2	Year 3
Target countries	France, Greece, Spain, Romania, Israel,	France, Greece, Spain, Romania, Israel,	France, Greece, Spain, Romania, Israel,

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	42 of 142	
Reference:	D6.3	Dissemination:	PU	
	Version:	1.0	Status:	Final

	Netherlands Switzerland (EC Europe)	Netherlands Switzerland (EC Europe)	Netherlands Switzerland (EC Europe)
Target Industry	Public Sector Private Sector	Public Sector Private Sector	Public Sector Private Sector
Target customer type	1-SMEs associations 2-3 rd parties services providers 3- End users	1-SMEs associations 2-3 rd parties services providers 3- End users	1-SMEs associations 2-3 rd parties services providers 3- End users
Target final users (estimation)	1- TBD 2- TBD 3- TBD	1- TBD 2- TBD 3- TBD	1- TBD 2- TBD 3- TBD

The market segmentation has been done during the first phases of the project. During the next months, once the **open call** results and the contacts with the **SMEs association** information is analysed, a more accurate forecast could be done, showing a more defined market penetration and the estimation of target users.

2.2.3.1.3 Distribution Channels

How will we **communicate and contact/reach** our Customer Segments to deliver a Value Proposition? Or the way around, how our Customer Segments **want to be reached**?

Main channels to distribute the toolkit will be: Own (from a web site or market place)

This initial approach can be accommodated to the needs identified during the interaction with future customers

2.2.3.1.4 Customer Relationships

Types of relationships established with the different customer segments. What are our customer segments' expectations related to the type of relationship with us? Are they cheap or expensive?

The main relationship with the customer will be carried out via:

- Personal assistance. There is a direct interaction between the customer and the company (dedicated helpdesk, consultancy projects);
- Self-service. No direct contact with the customers (i.e. training courses);
- Automated services. Customized services depending on the customer profile (i.e. access to data bases, security reporting, application uploading).

This initial approach can be accommodated to the needs identified during the interaction with future customers

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	43 of 142		
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

2.2.3.1.5 Revenue Streams

How will we **generate incomes** from the different customer segments? Are they all eligible to pay the same? Which is the pricing structure per component or service?

Main revenue stream approach will come from Fee structure (subscription, usage, broker, etc.) or licensing although the option to sell components could be considered if a commercial opportunity pops up.

Table 5 describes the pricing differentiation per customer during the Year 3 forecast of the business model:

Table 5: Revenue Streams Year 1-Year 3

Scenario 1: Differential Pricing (Service feature dependent)	Price User/Year	Year 1	Year 2	Year 3
1-Technology providers	1- On premises XXX€/per year	1- xxx€	1- xxx€	1- xxx€
2-Services providers	1'- Outsource XXX€/per year	1'- xxxxx€	1'- xxxxx€	1'- xxxxx€
	2- xxx/per application	2-xx€	2-xx€	2-xx€
	hosting/year	3- xx€	3- xx€	3- xx€
	3-Hub information			

2.2.3.1.6 Key Activities

Which are the most important actions we must carry out to make this business model work? What is required to make our value propositions available to our customer?

- Dissemination / Awareness
- Presales
- Consulting (Market Analysis, Gap analysis, Customization, etc.)
- Integration / Implementation
- Training
- Maintenance
- Standardization

2.2.3.1.7 Key Resources

Which are the most important **resources needed** (in order to support our value propositions, distribution channels, customer relationships, revenue streams, etc.) to make our **business model work**?

- Persons (who are going to deliver the value proposition itself)
- Knowledge (brands, patents, copyrights)
- Software/Hardware (specific SMESEC components)
- Economic/Finance (credit lines, grants, own funding, etc.)

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	44 of 142
Reference:	D6.3	Dissemination:	PU	Version:	1.0
				Status:	Final

2.2.3.1.8 Key Partners

- Public/Semi-public sector
 - FORTH
- Private sector
 - ATOS
 - GRIDPOCKET
 - WORLDSENSING
 - SCYTL
 - EGM
 - IBM
 - CITRIX
 - BITDEFENDER
- Academic sector
 - UoP
 - FHNW
 - UU

2.2.3.1.9 Cost Structure

The Cost Structure describes all costs incurred to operate business activities. What are the main costs attached to our business model? Which Key Resources/Activities have a higher cost?

This building block (Table 6) represents the economic expenditure to be carried out by the consortium to run a new business operation including a range of expenditure items such as **Capex** (Capital expense, investment regardless of the volume produced) and **Opex** (Operating expense heavily dependent on the volume of output generated):

Table 6: Cost Structure Year 1-Year 3

ID	Cost Element	Description	Type (CAPEX/OPEX)	In Scope (Yes/No)	Year 1	Year 2	Year 3
C. 1	IT Platform Implementation Costs				€ -	€ -	€ -
C. 1.0	System Integration (Platform - ID Providers)	Analysis, Design, Development, Testing, Deployment and Roll-out of the MPAS Platform + Contingencies	CAPEX	Yes	€ -	€ -	€ -

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	45 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

C. 1.1	HW Procurement	HW Costs to be sustained (Eventual backup systems implementation costs have to be considered to guarantee a high level of reliability). (If a Cloud-based solution is chosen you should not fill this field and see C.2.1)	CAPEX	No	€ -	€ -	€ -
C. 1.2	SW Procurement	SW Costs to be sustained (If a Cloud based solution is chosen you should not fill this field and see C.2.1)	CAPEX	Yes	€ -	€ -	€ -
C. 2	IT Platform Operating Costs				€ -	€ -	€ -
C. 2.1	Infrastructure Operation Costs (Infrastructure/Software Usage Fee in case of IAAS/SAAS)	Facilities, Hosting, Personnel, Service Desks Support (Infrastructure/Software Usage Fee in case of IAAS/SAAS)	OPEX	Yes	€ -	€ -	€ -
C. 2.2	IT Help Desk Support	Cost for maintain a Help Desk Support (from first to third support level)	OPEX	Yes	€ -	€ -	€ -
C. 2.3	HW Maintenance	This field should be skipped in case of Cloud-based solution	OPEX	No	€ -	€ -	€ -

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	46 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final






C. 2.4	SW Maintenance	This field should be skipped in case of Cloud-based solution	OPEX	No	€ -	€ -	€ -
C. 2.5	SW Evolution		OPEX	Yes	€ -	€ -	€ -
C. 2.6	Connectivity costs	Connectivity related costs (redundancy, different paths and providers, etc)	OPEX	No	€ -	€ -	€ -
C. 3	Business Operating Costs				€ -	€ -	€ -
C. 3.1	Business Integration (Service Providers)	Definition and implementation of Commercial Agreements with Service Providers (consider also a technical analysis of feasibility to be performed in the negotiation process)	OPEX	Yes	€ -	€ -	€ -
C. 3.2	Archive Maintenance	Documents, logs and other data to be stored for regulatory, fiscal purposes (if any)	OPEX	No	€ -	€ -	€ -
C. 4	Marketing and Distribution Costs				€ -	€ -	€ -
C. 4.1	Marketing Activities	Marketing activities to sustain customer acquisition campaigns. (Service Providers)	CAPEX	Yes	€ -	€ -	€ -

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	47 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

C.4.2	Distribution Costs	Costs to be sustained to reach the target customers (cover the five-dimension phases of distribution channels)	OPEX	Yes	€ -	€ -	€ -
	Total CAPEX				€ -	€ -	€ -
	Total OPEX				€ -	€ -	€ -
	TOTAL COSTS/YEAR				€ -	€ -	€ -
	Total COSTS CUMULATIVE				€ -	€ -	€ -

2.2.3.2 SMESEC Pilots Business Model Canvas WoS

The following sub-section describes the Worldsensing's approach to the SMESEC business model and the impact of the different building blocks of the Canvas model.

Key partners	Key activities	Value proposition	Customer relationship	Customer segmentations
 <ul style="list-style-type: none"> -HW components manufacturers -Communication providers -Digital security experts -Data scientists -System integrator -HW installers entities 	 <ul style="list-style-type: none"> -End-to-end solution for digital transformation in critical infrastructure (HW + SW) -Infrastructure monitoring -IT system monitoring -Alerts management 	 <p>Customer needs</p> <ul style="list-style-type: none"> -Improve detection, maintenance and response to emergency <p>Services</p> <ul style="list-style-type: none"> -Help-desk and support -Deployment -Training -Consulting 	 <ul style="list-style-type: none"> -After sale services: deployment, training, support, etc. 	 <ul style="list-style-type: none"> -Critical infrastructure managers -Utilities -Maintenance service providers

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	48 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

Key resources



- HW components
- SW sub-systems and modules
- Security SW tools

Channels



- Local and global Distributors
- Trade fares, workshop, seminars, etc.
- Direct sales: meeting with CTOs

Cost structure



- HW/SW components and sub-system
- HW/SW development
- Trainings and support organization
- Sales network
- Distributors fee

Revenue streams



- Direct HW product sale
- SW product with Basic and Gold SaaS licence
- Solution project (customized SW product)
- Related service: training, HW deployment, consulting, etc.

Figure 11: WoS Business Model Canvas

The company's business model approach relies on the adoption of the SMESEC cybersecurity framework in the Loadsensing portfolio, enriching the value proposition of this vertical product (industrial IoT). As a matter of fact, the final objective is launching to the market the first "secured" IoT technology with a user-friendly interface for non-cybersecurity experts. Value Proposition

The value proposition that SMESEC provides cannot be decoupled from that offered by Loadsensing as a whole (hardware + software). Actually, the SMESES added-value is to increase the resilience of IoT infrastructures to cyberattacks, providing well-defined response and mitigation actions for non-expert users' profiles.

Loadsensing is marketed following two different routes; as a product or a solution.

In the first one, IoT nodes (HW) and the data platform (SW) are sold either independently or merged. While the revenues directly linked to the IoT nodes (HW) is obtained only once (nodes trading), the software generates a steady flow of cash proportional to the total number of interconnected gadgets and systems, through a license invoicing mechanism.

Considering the pilot's architecture, the SMESEC security elements will be basically added to the SW layer as an optional extra of the final product. In fact, incorporating cybersecurity tools to the data platform should impact the final fee (license) to be paid per connected sub-system.

On the other hand, Loadsensing can be also marketed as a solution in which a particular deployment is generated from scratch in a tailor-made project (consulting). Here, the security elements (SW layer) are also optionally added to Loadsensing.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	49 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

Independently from the marketing option, up to four services can be offered on the top of the mere technology elements (HW & SW). SMESEC elements will be present in each of them as a submodule, whose scope and contents need to be defined along the project implementation.

Table 7 summarizes the above description of the go-to-market strategy of Loadsensing. Here, gold support is defined as the service with the highest Quality of Service to be offered by Worldsensing.

Table 7: Loadsensing Go-to-market Strategy

Sales business model	Components	Price / Cost	Security	Service			
				Training	Support	Consulting	Deployment
Product	HW	Fixed x unit	No, by default	Yes, optional	Gold or Basic	Yes, optional	Yes, optional
Product	SW	Fixed x sub-system connected	Yes, optional	Yes, optional	Gold or Basic	No	Yes, optional
Solution	SW	Customized	Yes, optional	Yes, optional	Gold or Basic	Yes	No, by default

2.2.3.2.1 Customer Segment

Loadsensing is a technology which is present worldwide (see Figure 12) but nonetheless the bulk of end-users have been restrained to infrastructure operators only. The progressive enrichment of the software layer which includes new features like operational intelligence capabilities will progressively increase the range to utilities (i.e. water and gas) and above all maintenance service providers.

For this new segment of customers, the prediction about the infrastructure status (not only real-time monitoring) is crucial to optimize their processes, resulting in a more efficient process. This progressive change has already started, and it is the cornerstone of the growth rate foreseen for Worldsensing in the coming years.

As a rule of thumb, most of the target customers up to now have been direct end users. This is expected to change to services providers and to a lesser extent, technology providers, who will adopt Loadsensing to optimize their core businesses.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	50 of 142		
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final



Figure 12: LoadSensing Customers and Distributors Worldwide

Depending on the infrastructure and each country idiosyncrasy, both the public and private sectors are target industries, particularly in Europe. Nevertheless, the private sector takes over the current market and this situation is not expected to change in the mid-term.

How the market will bring in the new features offered by LoadSensing is subject to a long discussion, particularly in verticals like construction in which the digitalization remains in its infancy.

Table 8 summarizes the current situation: the main market of LoadSensing will progressively shift from Europe to America, in which the private sector is dominant. For the first year, the product will continue reaching end users but according to the abovementioned plan will diversify the type. What is clear that LoadSensing will penetrate different verticals, being construction and rail the first targeted ones.

Table 8: Customer Segmentation Forecast

Concept	Year 1	Year 2	Year 3
Target countries	EC Europe, UK and Australia	South America	US
Target Industry	Public Sector Private Sector	Public Sector Private Sector	Public Sector Private Sector
Target customer type	1-Technology providers 2-Services providers 3-Direct end users	1-Technology providers 2-Services providers 3-Direct end users	1-Technology providers 2-Services providers 3-Direct end users
Target final users (estimation)	1 vertical (infrastructure)	2 verticals (infrastructure and rail)	3 verticals (infrastructure, rail and new one)

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	51 of 142
Reference:	D6.3	Dissemination:	PU	Version:	1.0
				Status:	Final

2.2.3.2.2 Distribution Channels

Worldsensing reach the market in a two-side approach. Using the own channels (website and company’ sales force) and the participation of key vendors worldwide with high knowledge of the local markets.

The first one has been the main choice up to know for Loadsensing and it will continue like this in the “solutions” business model. However, the exponential growth of Loadsensing makes necessary seeking alliances with key commercial players like Geomotion and Geosense which sells the product in a more systematic way (HW + SW). These alliances have already been established and SMESEC features could be easily added to the existing portfolio.

2.2.3.2.3 Customer Relationships

Due to the immaturity of the IoT market, most of the customers do not fully understand the value proposition that Worldsensing’ solutions provide. For this reason and despite some of our devices are sold by third parties (vendors), Worldsensing keeps a direct relationship with customers through helpdesk facilities. It goes without saying that this binding is even more strength in “solutions” projects (consultancy). This can be crucial to articulate the SMESEC services in general and the “support” and “training” in particular.

2.2.3.2.4 Revenue Streams

How will we **generate incomes** from the different customer segments? Are they all eligible to pay the same? Which is the pricing structure per component or service?

Main revenue stream approach will come from Fee structure (subscription, usage, broker, etc.) or licensing although the option to sell components could be considered if a commercial opportunity pops up.

Table 9 describes the pricing differentiation per customer and the revenue during the Year 3 forecast of the business model:

Table 9: Revenue Streams Year 1-Year 3

Scenario 1: Differential Pricing (Service feature dependent)	Price User/Year	Year 1	Year 2	Year 3
1 Product	Loadsensing HW: 1 k€	1 5.6 M€	1 8.4 M€	1 13.9 M€
2 Solutions	Loadsensing SW: TBD	2 - M€	2 0.7 M€	2 6.9 M€
	Solution project: 250 k€			

2.2.3.2.5 Key Activities

- Dissemination / Awareness:
 - Presales.
 - Consulting (Solutions project).
 - Training on SMESEC tools to end-users.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	52 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

2.2.3.2.6 Key Resources

SMESEC tools can be easily added to the existing Loadsensing’s distribution channels without major problems. Nevertheless, it is obvious that Worldsensing will need access to the specific SMESEC software components to enrich the product with a cybersecurity layer. To that end, it is mandatory that Worldsensing and SMESEC partners (solution providers) establish a stable and long-term collaboration framework in which the license and fees to be paid per product use are clearly defined.

2.2.3.2.7 Key Partners

- Public/Semi-public sector
 - EC (European Commission)
 - FORTH
- Private sector
 - ATOS
 - GRIDPOCKET
 - WORLDSENSING
 - SCYTL
 - EGM
 - IBM
 - CITRIX
 - BITDEFENDER
- Academic sector
 - UoP
 - FHNW
 - UU

2.2.3.2.8 Cost Structure

Considering the above description, the main costs are directly linked to the accommodation of SMESEC tools to the Loadsensing data platform (OneMind) can be labelled as Capex, and it has been covered by EU funds (SMESES project) and own resources. From a practical point of view, most of the cost elements for specific projects can be labelled as Opex except for ad-hoc systems integrations derived from “Solutions-Consulting” projects and the flat-rate expenses linked to marketing activities.

Table 10: Cost Structure WoS Year 1-Year 3

ID	Cost Element	Description	Type (CAPEX/OPEX)	In Scope (Yes/No)	Year 1	Year 2	Year 3
C.1	IT Platform Implementation Costs				€ 0	€ 35.000	€ 345.000

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	53 of 142		
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

C.1 .0	System Integration (Platform - ID Providers)	Analysis, Design, Development, Testing, Deployment and Roll-out of the MPAS Platform + Contingencies	CAPEX	Yes in Solutions	€ 0	€ 35.000	€ 345.000
C.1 .1	HW Procurement	HW Costs to be sustained (Eventual backup systems implementation costs have to be considered to guarantee a high level of reliability). (If a Cloud-based solution is chosen you should not fill this field and see C.2.1)	CAPEX	No	€ -	€ -	€ -
C.1 .2	SW Procurement	SW Costs to be sustained (If a Cloud based solution is chosen you should not fill this field and see C.2.1)	CAPEX	No	€ -	€ -	€ -
C.2	IT Platform Operating Costs				€ 105.000	€ 250.000	€ 270.000

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	54 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

C.2 .1	Infrastructure Operation Costs (Infrastructure/Software Usage Fee in case of IAAS/SAAS)	Facilities, Hosting, Personnel, Service Desks Support (Infrastructure/Software Usage Fee in case of IAAS/SAAS)	OPEX	Yes	€ 90.000	€ 120.000	€ 220.000
C.2 .2	IT Help Desk Support	Cost for maintain a Help Desk Support (from first to third support level)	OPEX	Yes	€ 15.000	€ 30.000	€ 30.000
C.2 .3	HW Maintenance	This field should be skipped in case of Cloud-based solution	OPEX	Yes	€ -	€ -	€ -
C.2 .4	SW Maintenance	This field should be skipped in case of Cloud-based solution	OPEX	Yes	€ -	€ -	€ -
C.2 .5	SW Evolution		OPEX	Yes	€ -	€ 20.000	€ 20.000
C.2 .6	Connectivity costs	Connectivity related costs (redundancy, different paths and providers, etc.)	OPEX	No	€ -	€ -	€ -

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	55 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

C.3	Business Operating Costs				€ 20.000	€ 60.000	€ 120.000
C.3 .1	Business Integration (Service Providers)	Definition and implementation of Commercial Agreements with Service Providers (consider also a technical analysis of feasibility to be performed in the negotiation process)	OPEX	Yes	€ 20.000	€ 60.000	€ 120.000
C.3 .2	Archive Maintenance	Documents, logs and other data to be stored for regulatory, fiscal purposes (if any)	OPEX	No	€ 0	€ 0	€ 0
C.4	Marketing and Distribution Costs				€ 15.000	€ 30.000	€ 30.000
C.4 .1	Marketing Activities	Marketing activities to sustain customer acquisition campaigns. (Service Providers)	CAPEX	Yes	€ 15.000	€ 30.000	€ 30.000
C.4 .2	Distribution Costs	Costs to be sustained to reach the target	OPEX	Yes	€ -	€ -	€ -

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	56 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

		customers (cover the five-dimension phases of distribution channels)					
	Total CAPEX				€ 15.000	€ 65.000	€ 375.000
	Total OPEX				€ 125.000	€ 230.000	€ 390.000
	TOTAL COSTS/YEAR				€ 140.000	€ 295.000	€ 795.000
	Total COSTS CUMULATIVE				€ -	€ -	€ -

2.2.3.2.9 Conclusions

All figures included in this business model have been generated considering fair assumption of WoS based on the potential the company value the SMESEC enhancements can provide to their current service portfolio.

Provisional figures considering the maturity level of SMESEC functionalities in Year 2. This impact represents a 5% of total Loadsensing business income.

Break Even point will be achieved in Year 1 (after the exploitation of the enhance functionalities by WoS)

ROI decreases with the evolution of “Solutions” project since more tailor-made actions are needed. Besides the amount the licences to the partners increases as well.

Table 11: Business Model Indicator

Concept	Year 1	Year 2	Year 3
Total Income	€ 230.000	€ 455.000	€ 1.040.000
Total Costs	€ 140.000	€ 295.000	€ 795.000
ROI (Return on investment)	64%	54%	30%
Breakeven point/Year	Year 1		

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	57 of 142		
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

3 Dissemination Activities

The dissemination activities aim at widely disseminating and explaining the SMESEC project contributions to the scientific and technical communities. In D6.1 and D6.2, we specified our targeted audience, the channels where they can be reached and provided customisation suggestions to the consortium. During the second year, dissemination concentrated on activities through which the consortium will trigger widespread awareness with market outreach (see section 2) and standardisation activities in mind (see section 4). D6.1 also specified the project branding to provide a uniform graphic layout for the dissemination and the SMESEC framework.

The work has been split into the following communication processes:

- Maintenance of the public Web portal www.smesec.eu promoting the project research with an up-to-date overview of the scientific results, information about standardisation, market information relative to the context of the SMESEC project,
- To support online and offline dissemination, a leaflet, a poster and presentation slides have been updated with information about the SMESEC framework that is being validated with the use case SMEs and the third parties that joined the work as part of the open call,
- To maintain a project blog,
- To maintain the publication on social media including Twitter, Facebook, LinkedIn, and YouTube to broadcast announcements of the project participation in public events, key achievements, publications, and the open call,
- To publish in major European and Non-European technical conferences as well as in specialised journals and magazines in the project related areas,
- To organise workshops with international events (EU meeting, conferences) facilitating the security awareness roadmap and its implementation in WP2 and WP3,

The publication of newsletters taking into account identified needs of registered members and the organisation of training courses organisation has been planned in preparation of the third year of the SMESEC project in accordance with the security awareness roadmap and its implementation in WP2 and WP3.

This chapter is structured as follows. Section 3.1 provides a summary of the dissemination strategy defined in D6.1 and decisions for adaptations to that strategy based on the project progress and lessons learned. Section 3.2 reports on the communication performed for the Open Call. Section 3.3 describes the updates to the dissemination tools. Section 3.4 reports the work performed during Y2 and the current status of dissemination at the end of Y2. Section 3.5 summarises and concludes.

3.1 Dissemination Strategy, incl. Updates

As part of an experience-based project, the SMESEC framework will be built upon and developed through the consistent feedbacks from its integrated use cases, more specifically IoT, Smart Cities, Smart grids and eVoting, as those defined in the DoW. The underlying purpose of the overall framework is no other than to offer a top-quality, robust and cost-efficient solution for SMEs.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	58 of 142		
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

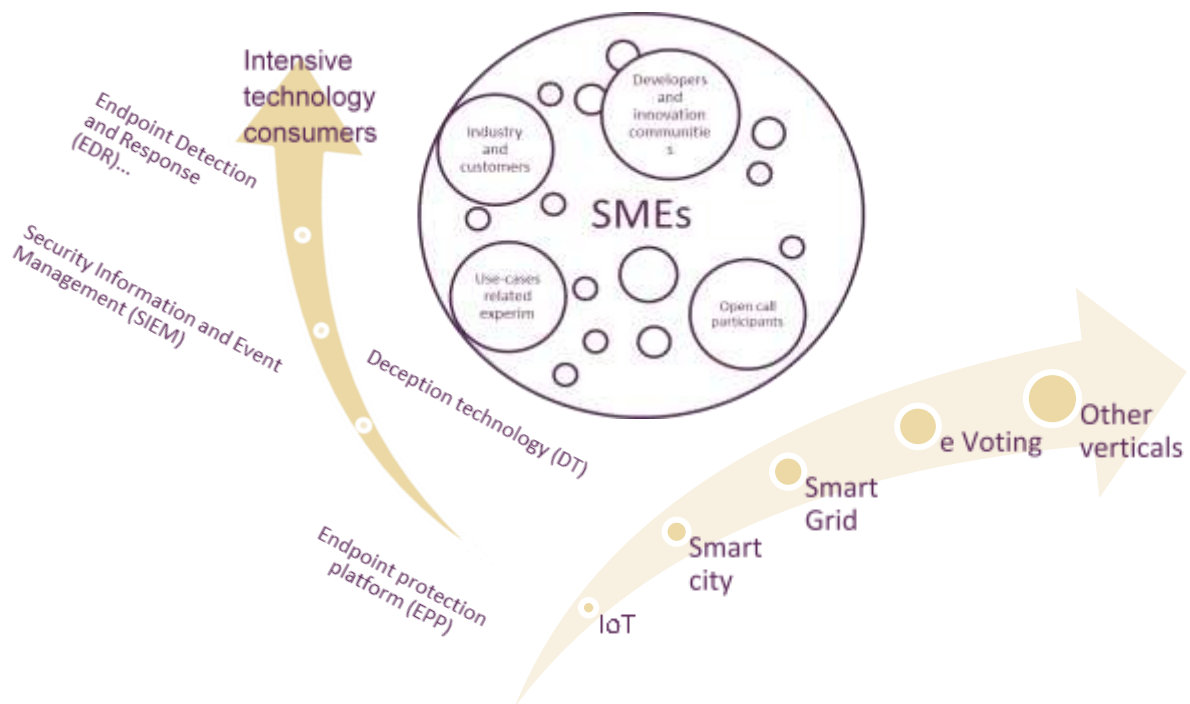


Figure 13: Overview of SMESEC dissemination approach

As presented in Figure 13, the consortium will develop a multi-channel plan to attract the widest audience addressing dedicated actions towards SMEs via direct interactions within the open call process, through SMEs organization, offering a wide network of relevant project stakeholders. This main channel will be strengthened by a set of verticals-based actions, taking advantage of use cases experience to attract SMEs and a technology-based approach, focusing on security, privacy and cybersecurity specialized events and networks.

3.1.1 Updated target audiences and approach to reaching SMEs:

During the Y1 and Y2 of the SMESEC project, we learned that SMEs are won as subscribers and customers on a one-by-one fashion. Each SME needs to be aware of the relevance of cybersecurity and convinced to initiate actions towards improving its capabilities. We learned that awareness can be achieved by building on European, national, and regional initiatives that utilise existing communication networks already. The created awareness can then be used to meet and channel SMEs to instruments for interacting with them, including the open call, registration as a member, and eventually try and use the SMESEC framework. Hence, the SMESEC consortium decided to continue serving the dissemination target groups already defined in D6.1 and D6.2 while adding a focus on the following pillars for effectively reaching SMEs.

1) **Sustaining presence in verticals:** SMESEC appeared and continues to appear at events dedicated to the verticals reflected by the SMESEC use case SMEs (see Figure 13 – right-hand arrow). The aim is to test the SMEs’ awareness for cybersecurity and the SMESEC framework as a tool for helping them to defend themselves. The events that SMESEC joined are reported in section 3.4.1.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	59 of 142	
Reference:	D6.3	Dissemination:	PU	
	Version:	1.0	Status:	Final

2) **Adding cooperation with stakeholders managing SME ecosystems, including SME associations, insurances, chambers of commerce, and related initiatives that target SMEs:** SMESEC mapped relevant SME associations, initiated contact through the relevant local partners, and started collaboration on raising awareness and spreading knowledge about SMESEC.

The following table lists the identified SME associations and the status of cooperation as of M24.

Table 12: Identified SME associations and status of cooperation as of M24.

SME Association	Country	Partner	Status
SESCA (Self-employed and small companies association)	Spain	ATOS	Contacted
CEA - Confederación Empresarios de Andalucía	Spain	ATOS	Contacted
Confederación Española de la Pequeña y Mediana Empresa	Spain	ATOS	Contacted
Confederación de Empresarios de Málaga	Spain	ATOS	Contacted
Asociación de empresarios de Gipuzkoa (ADEGI)	Spain	ATOS	Contacted
AMEC - Asociación de empresas industriales internacionales	Spain	ATOS	Contacted
European entrepreneurs CEA-PME	EU	EGM	Cooperation ongoing
AFDEE - Association Francaise des Dirigeants d'Entreprises en Europe	France	EGM	Cooperation ongoing
CPME - Confédération des PME	France	EGM	Contacted
ONTPE (small businesses)	France	EGM	Workshop organised. Cooperation ongoing
European Digital SME Alliance	EU	FHNW, EGM, UU	Cooperation ongoing
Schweizerischer KMU-Verband	Switzerland	FHNW	Cooperation ongoing
Schweizerische Akademie der Technischen Wissenschaften SATW	Switzerland	FHNW	Cooperation ongoing
Podlaski Klub Biznesu	Poland	GRIDPOCKET	Identified
CPR - Confederatia Patronatului Roman	Romania	BITDEFENDER	Identified
ANIS - Asociația Patronală a Industriei de Software și Servicii	Romania	BITDEFENDER	Contacted
InnovationLabs	Romania	BITDEFENDER	Contacted
Israel Advanced Technology Industries	Israel	IBM	Identified

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	60 of 142
Reference:	D6.3	Dissemination:	PU	Version:	1.0
				Status:	Final

SME Association	Country	Partner	Status
Start-Up Nation Central	Israel	IBM	Identified
The Israel Small and Medium Enterprises Authority (ISMEA)	Israel	IBM	Identified
PRAXIS network	Greece	FORTH	Contacted
MKB Nederland organisation	Netherlands	UU	Identified
KVK - Kamer van Koophandel	Netherlands	UU	Contacted
ESBA - European Small Business Alliance	EU	EGM, UU	Cooperation ongoing

3) **Sustaining local national/regional outreach:** SMESEC continued to interact with SMEs by organising or joining workshops and local events and interacting with the SMEs individually. The external events are reported in section 3.4.1, the SMESEC workshops in section 3.4.5.

4) **Continue the interaction with other stakeholders:** including Open-Source Software Communities, Academia (section 3.4.4), Policy (section 3.4.4), Individuals, and Standardisation (section 4).

3.1.2 Strategy and Roadmap

The dissemination objectives are shown in Figure 14. For the year 2, dissemination intends to raise interest in the SMESEC framework and the desire to collaborate with the consortium. Important instruments are the information about the SMESEC framework and the open call for expanding the work performed by the SMESEC consortium. The year 2 was expected to create the seed for a community of SMEs and stakeholders actively working on the protection against cyber threats.



Figure 14: Overview of SMESEC dissemination objectives

Figure 15: Dissemination plan shows how all these activities are aligned with the SMESEC project plan. The plan consists of a series of phases that lead to the recruitment of open call participants and SMESEC framework users upon the initiation of exploitation.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	61 of 142		
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

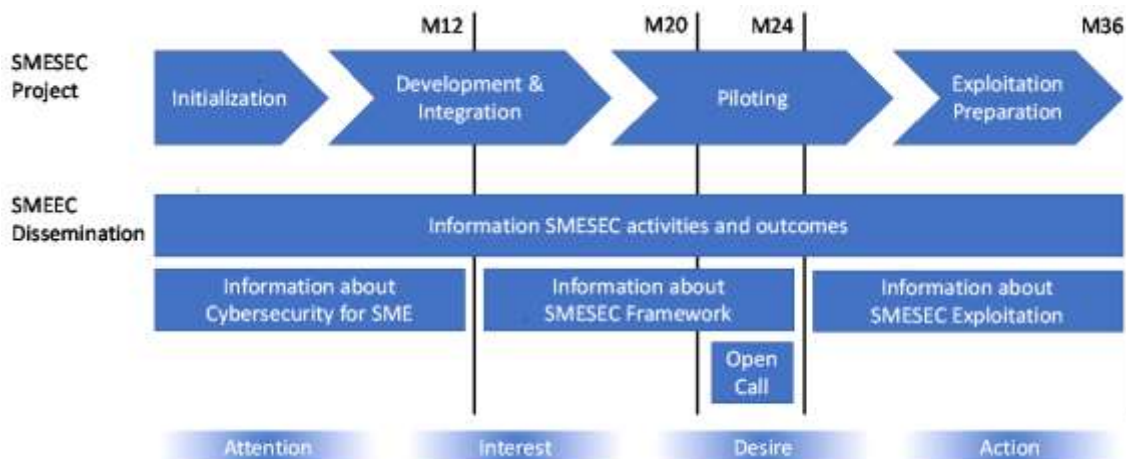


Figure 15: Dissemination plan

3.1.3 Updates to Target Audiences and Messages

SMESEC started to implement the dissemination with a series of contents or stories that are kept consistent across channels. For the year 2, they include the SMESEC framework vision and tools, and the open call for joining the SMESEC work. The dissemination messages have been stable with just small modifications during year 2 to refine the information about the SMESEC framework and the addition of the Open Call.

Table 13 shows the message to be communicated by SMESEC dissemination.

Table 13: Dissemination message (modifications in comparison to D6.2: SMESEC Framework and Open Call)

Theme	Messages		
Importance of cybersecurity for SMEs	60% of all cyber-attacks or breaches in 2016 were aimed at SMEs. 68% of SMEs have no systematic approach to ensuring cybersecurity. 60% of SMEs who were victims of cyber-attacks did not recover & shut down within 6 months.		
Threats of importance for SMEs	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">DoS and DDoS Vulnerable Software Broken Authentication Misconfigurations Injection</td> <td style="width: 50%;">Cross-Site Scripting Sensitive Data Exposure Garbage Data Malicious Insiders</td> </tr> </table>	DoS and DDoS Vulnerable Software Broken Authentication Misconfigurations Injection	Cross-Site Scripting Sensitive Data Exposure Garbage Data Malicious Insiders
DoS and DDoS Vulnerable Software Broken Authentication Misconfigurations Injection	Cross-Site Scripting Sensitive Data Exposure Garbage Data Malicious Insiders		
Goals of Cybersecurity for SMEs	Cybersecurity must... ...be based on up-to-date facts and events ...activate and motivate all employees ...offer lightweight defences against cyber threats		

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	62 of 142				
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

Theme	Messages
SMESEC Framework	<p>SMESEC offers a lightweight cybersecurity framework for thorough protection, including:</p> <p>Framework with...</p> <ul style="list-style-type: none"> ...Security Information and Event Manager XL-SIEM <p>Social Tools...</p> <ul style="list-style-type: none"> ...Cybersecurity Coach CYSEC ...Securityaware.me Training Platform <p>Technical Tools...</p> <ul style="list-style-type: none"> ...GravityZone ...Early Warning Intrusion Detection System EWIS ...Citrix Application Delivery Controller ...IBM Anti-ROP Compiler Plugin ...Test-as-a-Service TaaS
SMESEC Methodology	<p>Framework Tested on Real-World SMEs in...</p> <ul style="list-style-type: none"> ...IoT ...Smart City ...Smart Grid ...e-Voting ...Digital Start-ups
Advantages of SMESEC	<p>Do it yourself: step-by-step guidance for meeting customer requirements and standards</p> <p>Keep the investment small: cost-effective tutorials and tools suitable for a busy environment</p> <p>Keep it simple: practices adapted to the company instead of complicated formal policies and procedures</p>
Open Call	<p>The SMESEC project invites third-parties for broad validation:</p> <ul style="list-style-type: none"> ...red team for evaluation of framework security ...SME association, community, or ecosystem for community feedback ...new use case SMEs for SME feedback ...SMEs offering extensions to the framework

The core values being pursued with the design are trust in SMESEC, respect of the expertise of the SMESEC consortium, and simplicity of the SMESEC framework. A professional designer packaged these values in the visual design used to communicate the SMESEC message to the target audience.

3.2 Updates to the Dissemination Tools

The dissemination tools have been updated to communicate the refined description of the SMESEC framework. The following tools have been updated:

- To provide a central point of information about SMESEC, the webpage has been updated.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	63 of 142				
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

- To support the presence of SMESEC at conferences and fairs, a flyer, a poster, and a roll-up were created. All are available in multiple formats, adapted to the needs of the SMESEC consortium partners. The material is printed upon demand.
- To support partners who give talks about SMESEC, the standard presentation slides have been updated. They are available to each partner for inclusion in their presentation slides.

This section shows the updated material.

3.2.1 Webpage

The presentation of the SMESEC framework was updated on www.smesec.eu/framework.html. The webpage now describes the tools that are part of the SMESEC framework, the value proposition of these tools, and quotes from SMEs that were using these tools and reflect the impact of the tools on the SMEs. Each tool is presented with a short description, a visualisation of the graphical user interface, three key features, and two quotes. To provide insights about the framework, two quotes for SME use cases round up each tool presentation. The following screenshots show the updates.



Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	64 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

– DETECTION & ALERTING –

Security Information and Event Manager XL-SIEM

Realtime alerts for securing the SME.

The SMESEC XL-SIEM is a platform for collecting cybersecurity alerts and deviations from correct behaviour in a system. The information comes from the correlation of several monitoring tools focusing in different areas of the target system. The tool provides real-time analysis of the alerts and information about them in an easy and accessible way. In contrast to other SIEM tools the XL-SIEM guides end-users with concrete and actionable recommendations of what to do against specific alerts and protect better their organization.

Features

Provides total control for creating relevant alarms and full event history.

Lets the user aggregate different sources of SMESEC input data to provide a good insight of attacks.

Recommendations guide the user to the right tools and actions to be performed.



« For the first time, I felt to be in control. »

Rodrigo Díaz, ATOS

« It was easy to understand what happens and take immediate action. »

Olimo Rayón, WorldSensing

– TRAINING COURSES & MATERIAL –

Cybersecurity Coach CYSEC

Assess, plan, and track improvements in cybersecurity.

CYSEC provides SMEs with the ability to assess, plan, and track improvements in cybersecurity in a simple, do-it-yourself fashion. For an SME that is aware of cyber risks, CYSEC offers easily understandable cybersecurity advice and offers a personalized, self-adaptive journey of building cybersecurity capabilities to protect the SME. For the open cybersecurity expert community serving SMEs, CYSEC gives insights into how cybersecurity practices are adopted and a channel for helping SMEs to solve their difficult challenges.



Features

The what, why, and how for each cybersecurity improvement in the SME.

Recommends the next step in the SME's improvement journey.

Awards badges that certify your SME's achievements in getting protected.

« CYSEC gave us holistic awareness about cybersecurity. »

Andreas Last, GridPocket

« The CYSEC tool provided valuable insight into the security level of the company by just doing a quick survey. »

Jordi Cucumell, Scyt

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	65 of 142	
Reference:	D6.3	Dissemination:	PU	
	Version:	1.0	Status:	Final

– DETECTION & ALERTING –

GravityZone

AI and heuristics for comprehensive protection of workstations and servers.

SMESEC GravityZone from BitDefender gives small and medium-sized companies a unified approach to security management that addresses the scalability and performance challenges your organization is facing today. GravityZone is architected from the ground up to unify security control over virtualized, physical, and mobile environments. It protects all the things that keep your business going: workstations, servers, mailboxes and mobile devices. It is incredibly easy to install and right on your resources.

Features

- Comprehensive security and efficient management with layered protection for the SME's endpoints.
- Artificial intelligence and machine learning, perfected for best protection and best performance.
- Web-based security for full control and enhanced business productivity.



« I now spend less than one hour a month on security because GravityZone takes care of almost everything. »

Denis Muckensturm, Les Jardins de Gaïa

« It's an additional layer of security that protects us from the most advanced attacks. »

Simon Gassmann, Quilvest Switzerland

– DETECTION & ALERTING –

Early Warning Intrusion Detection System EWIS

Light intrusion detection that is also able to attract attacks away from the systems.

EWIS is a honeypot-based intrusion detection solution tailored for SMEs. It can run in parallel with the real system, attracting attacks away from the SME's systems. EWIS also provides a graphical interface visualizing the events that are captured by our sensors, this interface is part of the final SMESEC framework.



Features

- Emulates production services like the ones SMEs are using.
- Non-intrusive detection of malicious network events.
- Visual representation of real-time and passed network events.

« I gained new insights into the overall security events in the system. »

A Geek company in the defence sector

« It was easy to retrieve and query for security events. »

Christos Tzanaris, sense.city

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	66 of 142
Reference:	D6.3	Dissemination:	PU
	Version:	1.0	Status:
			Final

— DETECTION & ALERTING —

Citrix Application Delivery Controller

Complete visibility and control over the web traffic.

SMESEC partially integrates the industry-leading Citrix Application Delivery Controller, which provides solutions for granting SMEs the visibility and control they need over encrypted traffic, thus ensuring compliance with their privacy, regulatory, and acceptable user behaviour. To keep users safe inside an organization, all communications must be inspected, not just clear-text traffic. Without, organizations are at risk from attacks. Hackers can infiltrate malware and steal data across multiple endpoints in the general encrypted traffic.



Features

- Selectively decrypts traffic according to URL, category, reputation, or customer list.
- Blocks malicious websites such as malware, spam, and phishing sites.
- Analytics, visibility, and reporting for communication networks and user data.

« We could see issues right away and address them proactively. »

Christo Tranter, Swiss ABB unit

« With Citrix, giving users access was as simple as checking a box, and it all worked. »

And Akrot, Aramex

— PROTECTION & RESPONSE —

IBM Anti-ROP Compiler Plugin

Protect software with the moving target defense technology.

IBM Anti-ROP Compiler Plugin (Shakedown) allows compiling a C/C++ program with binary shuffling enabled so that the resulting executable is different for each build. The shuffling prevents buffer overflow and ROP attacks scale out: an exploit that targets one instance of the application will not successfully execute on other instances.

Features

- No modifications to project's source code is required.
- Generates many versions of single binary executable, all different in binary layout but identical in functionality.
- Performs different types of randomizations to make it difficult for the attacker to circumvent.



« We successfully used it on industrial IoT devices. »

Ölüm Kayın, Worldsensing

« A simple compiler wrapper allowed me to do the shuffling. »

Ölüm Kayın, Worldsensing

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	67 of 142	
Reference:	D6.3	Dissemination:	PU	
	Version:	1.0	Status:	Final

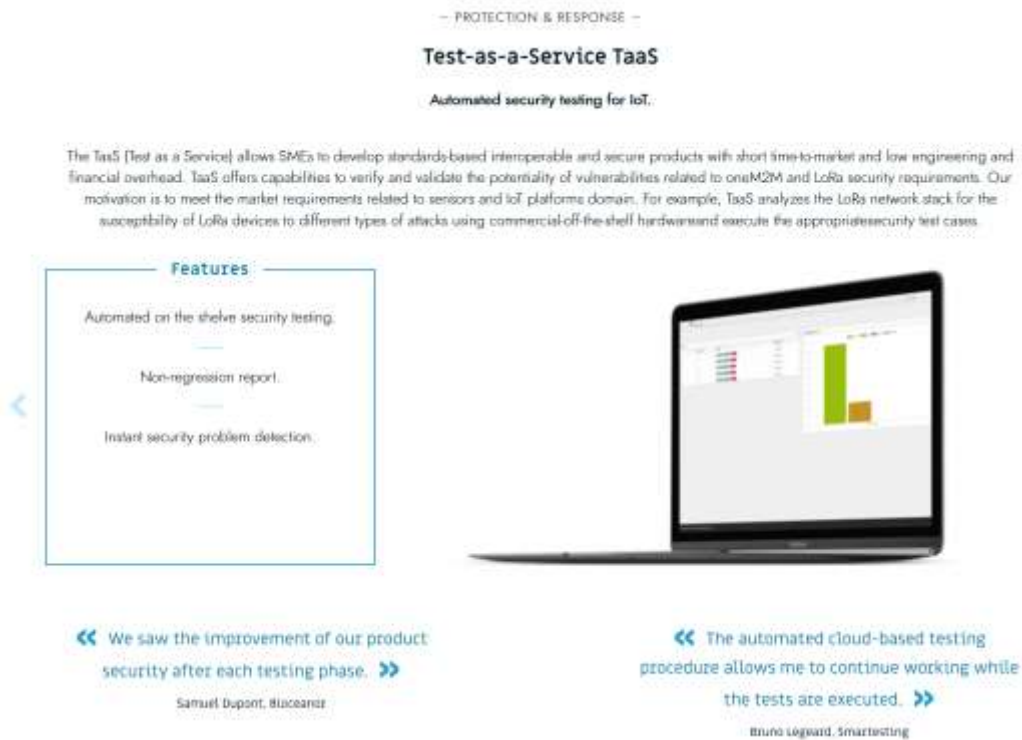


Figure 16: SMESEC tools presentation on www.smesecu.eu.

A call for action concludes the tool presentation: “How secure is your company? Head to the Member section! [Login/Register],” see Figure 17.

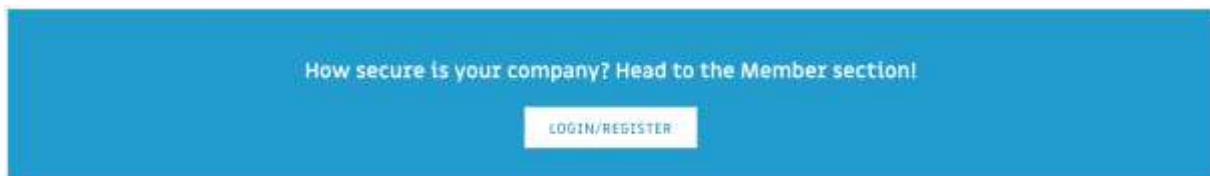



Figure 17: Call for action.


3.2.2 Flyer/Leaflet

An updated flyer was created that now describes the tools that are part of the SMESEC framework, the value proposition of these tools, and quotes from SMEs that were using these tools and reflect the impact of the tools on the SMEs. Each tool is presented with a short description, a visualisation of the graphical user interface, three key features, and two quotes. To provide insights about the framework, two quotes for SME use cases round up the flyer.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	68 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final



a lightweight cybersecurity framework for thorough protection




The SMESEC framework is based on operational information about Cybersecurity. The SMESEC framework provides SMEs with the ability to build Cybersecurity that will just work. SMESEC makes Cybersecurity accessible for SME and helps to prevent and mitigate cyber risks at a large part of the European economy.

GravityZone

AI and heuristics for comprehensive protection of workstations and servers.

SMESEC GravityZone has 360-degree virus and malware protection. It is a cloud-based solution that adapts to your environment. GravityZone is built on the ground up to fully control your endpoints, physical, and mobile environments. It protects the things that keep your business going.

GravityZone provides a single console to manage all your devices. It is incredibly easy to install and light on your network.



FEATURES

- Comprehensive security and efficient management with layered protection for the SME's endpoints.
- Artificial intelligence and machine learning protected for best protection and best performance.
- Workload aware for full control and enhanced business productivity.

It is easy to install and use. It is a cloud-based solution that adapts to your environment. It is incredibly easy to install and light on your network. It provides a single console to manage all your devices. It is incredibly easy to install and light on your network.

Cybersecurity Coach

Assess, plan, and track improvements in cybersecurity.

CYSEC provides SMEs with the ability to assess, plan, and track improvements in cybersecurity in a simple, dashboard-driven way. CYSEC offers a range of cyber advice and offers a personalized, self-guided course of building cybersecurity capabilities to protect your SME. For the open cybersecurity expert, CYSEC offers a range of how-to guides and a channel for helping SMEs to solve their difficult challenges.



FEATURES


- The what, why, and how for each cybersecurity improvement in the SME.
- Recommend the next step in the SME's improvement journey.
- Awards badges for every year SME's achievements in getting protected.

It is easy to use and provides a range of cyber advice. It offers a personalized, self-guided course of building cybersecurity capabilities to protect your SME. For the open cybersecurity expert, it offers a range of how-to guides and a channel for helping SMEs to solve their difficult challenges.

Security Information and Event Manager XL-SIEM

Real-time alerts for securing the SME.

The SMESEC XL-SIEM is a solution for collecting cybersecurity alerts and deviations from correct behavior in a system. The information comes from the correlation of several monitoring tools focusing in different areas of the target system. This tool provides real-time analysis of the alerts and information about them in an easy and accessible way. It is designed for SMEs with a limited number of servers with complex and active network environments of SMEs. It provides specific alerts and protect faster their operations.



FEATURES

- Provides real control for creating relevant alerts and full event history.
- Let the user aggregate different sources of SMESEC input data to provide a good insight of alerts.
- Recommendations guide the user to the right tools and actions to be performed.

It is easy to use and provides a range of cyber advice. It offers a personalized, self-guided course of building cybersecurity capabilities to protect your SME. For the open cybersecurity expert, it offers a range of how-to guides and a channel for helping SMEs to solve their difficult challenges.

Securityaware.me Training Platform

Interactive training courses.

Securityaware.me is an online platform for creating and managing interactive training courses (e.g. webinars, webinars, etc.). Courses to other training platforms. Securityaware.me focuses only on cybersecurity. All training courses are created by experts from SMESEC. The courses are interactive and include a range of exercises and a range of exercises. The training is available for many different security topics and levels of experience.



FEATURES

- These courses that are open to the public, or made available privately to selected registered users.
- Provides course managers with the ability to create their own courses, host their own private or public courses to present a personalized training experience to their users.
- The training courses can be associated directly with Securityaware.me or exported to be trained in other learning management systems (e.g. Moodle).

It is easy to use and provides a range of cyber advice. It offers a personalized, self-guided course of building cybersecurity capabilities to protect your SME. For the open cybersecurity expert, it offers a range of how-to guides and a channel for helping SMEs to solve their difficult challenges.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	69 of 142
Reference:	D6.3	Dissemination:	PU
Version:	1.0	Status:	Final

Early Warning Intrusion Detection System EWIS

Light intrusion detection that is also able to attack attacks away from the system.

EWIS is a honeypot-based intrusion detection solution tailored for SMEs. It can run in parallel with the real-time intrusion detection system (IDS) to detect and alert on suspicious activity. EWIS also provides a graphical interface enabling the user to view and manage the alerts. It is a part of the full SMESEC framework.



Features

- Enables production services like the ones that are using.
- Non-intrusive detection of malicious network events.
- Visual representation of malware and phishing network events.

30 / 30 years new insights into the world of malware and phishing events in the system. 05

© SMESEC 2018. All rights reserved.

Citrix Application Delivery Controller

Complete visibility and control over the web traffic.

SMESEC perfectly integrates the industry-leading Citrix Application Delivery Controller, which provides solutions for web traffic management, load balancing, and security. It also provides a graphical interface for managing the system. It is a part of the full SMESEC framework.



Features

- Selectively decodes traffic according to URL category, reputation, or malware list.
- Blocks malicious websites such as malware, spam, and phishing sites.
- Analyzes, validates, and reports for communication networks and user data.

30 / 30 years new insights into the world of malware and phishing events in the system. 05

© SMESEC 2018. All rights reserved.

IBM Anti-ROP Compiler Plugin

Protect software with the moving target defense technology.

IBM Anti-ROP Compiler Plugin (Shibboleth) allows developers to protect their applications from Return-Oriented Programming (ROP) attacks. The plugin prevents buffer overflows and ROP attacks. It is a part of the full SMESEC framework.



Features

- No modifications to program source code required.
- Generates many versions of single binary executable, all different in binary layout but identical in functionality.
- Performs different types of randomizations to make it difficult for the attacker to instrument.

30 / 30 years new insights into the world of malware and phishing events in the system. 05

© SMESEC 2018. All rights reserved.

Test-as-a-Service Taas

Automated security testing for IoT

The Taas Plug-in is designed to allow developers to quickly test their IoT devices for vulnerabilities and security weaknesses. It is a part of the full SMESEC framework.



Features

- Automated or the ability security testing.
- Non-intrusive approach.
- Validated security problem detection.

30 / 30 years new insights into the world of malware and phishing events in the system. 05

© SMESEC 2018. All rights reserved.

SMESEC FRAMEWORK

How secure is your company?



AtosS, Soryl, GASTROCKET, n7, citrix, IBM, Blackboard, and other partners are part of the SMESEC framework.

30 / 30 years new insights into the world of malware and phishing events in the system. 05

© SMESEC 2018. All rights reserved.

Figure 18: Updated SMESEC Flyer

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	70 of 142
Reference:	D6.3	Dissemination:	PU
		Version:	1.0
		Status:	Final

The flyer is being used as a basis for the update of the webpage, which describes each tool with the same visuals and information. The overview of the tools is also being used as a basis for the updated poster and roll-up.

3.2.3 Presentation slides

Updated with information about the tools has also been the SMESEC standard presentation that is available for any SMESEC partner giving a talk about SMESEC. The figure below shows how again the same elements, the short description, the visual, the features, and the quotes, are provided for use by the speaker.



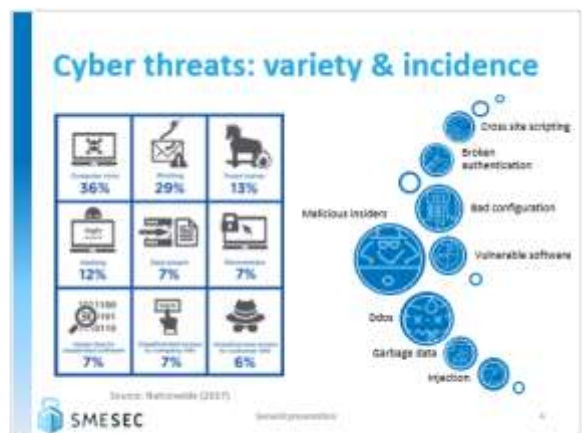
1



2



3




4

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	71 of 142
Reference:	D6.3	Dissemination:	PU
Version:	1.0	Status:	Final



5

The SMESEC Framework



SMESEC

6

The SMESEC Framework

Technical oriented

- Detection and Alerting:** properly identify cybersecurity-related risks for the organization (systems, assets, users, data, etc.), incorporate a tailor-made cybersecurity solution and discover cybersecurity events in real-time
- Protection and Response:** employ appropriate safeguards for the organization and response & recovery plans for detected cybersecurity incidents

Human oriented

- Capability and Awareness Strategy:** SME-tailored tools and methods to plan in-house cybersecurity capabilities, increase employee awareness, join events, and promote self-evaluation and improvement
- Training Courses and Material:** SMESEC Framework specially designed training material for understanding and employing a robust cybersecurity system

SMESEC

7

Detection and Alerting

AtoS

- Risk Assessment Engine**
- Analysis the business profile of the organization and provides a report of vulnerabilities at both technical and management level

SMESEC

8

Detection and Alerting

Test-as-a-Service TaaS

Automated security testing for IoT

The Test Plan is a critical document to develop, develop based on requirements and security profiles with a questionnaire for engineering and financial approval. Test plan conditions to verify test values, the quantity of vulnerabilities, ability to penetrate security requirements. Use automation to meet the manual requirements related to security and/or software domain. For example, Test analysis for the network and for availability of IoT devices in different types of attack using commercial/external hardware and network. The automation security test plan.

Features

- Automated for the cyber security testing
- Non-regression report
- Automated security problem detection

IT devices for:

- Integration of IoT devices security perimeter
- Integration: IT

IoT cloud based & enterprise testing capabilities. Integration to enterprise security center. Non-regression: IoT



SMESEC

9

Detection and Alerting

IBM

- IBM AngelEye**
- Solution for patching vulnerabilities and exploits in systems using AI techniques

SMESEC

10

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	72 of 142
Reference:	D6.3	Dissemination:	PU
	Version:	1.0	Status: Final



Detection and Alerting

- **IBM ExpISAT**
- Test the source code of an application with a fuzzing engine to find runtime vulnerabilities



General presentation 11



Detection and Alerting

IBM Anti-RDP Compiler Plugin
Protect software with the rising target defense technology

IBM Anti-RDP Compiler Plugin (libatls) allows installing a CPU- or program-specific plugin needed to find the runtime vulnerability in a target code. The plugin takes source and RDP attack code and an exploit that targets the weakness of the application software successfully installed in other systems.

Features

- Real-time detection in program source code (compiled)
- The general security system of single code is necessary, all elements of the system are based on a technology
- Performs different types of modifications in order to detect the application in a system

• It has a security level 4 (not recommended for Linux 15) • It supports a single program using a complex security system (multiple protection, 15)



General presentation 12



Protection and Response

GravityZone
AI and heuristics for comprehensive protection of workstations and servers.

Bitdefender GravityZone provides a unified approach to security management for addresses the complexity and performance challenges your organization is facing today. Combining AI heuristics on the ground up to early security control over contextual, physical, and mobile environments. To protect all the things that keep your business going: workstations, servers, mobile devices, and mobile devices. It is available in a way to install and update your systems.

Features

- Comprehensive security and efficient management with layered protection for the SME + enterprise
- Analytical intelligence and machine learning, perfected for best protection and best performance
- Multilayered security for full control and enhanced business productivity

• It has a security level 4 (not recommended for Linux 15) • It supports a single program using a complex security system (multiple protection, 15)



General presentation 13



Protection and Response

Citrix Application Delivery Controller
Complete visibility and control over the web traffic.

SD-WAN centrally manages the network traffic. Citrix Application Delivery Controller, which provides solutions for granting SD-WAN the visibility and control to manage and manage traffic. This ensures compliance with the process, regulatory, and acceptable use behavior. To keep users safe, create an organization, all communications must be tracked, not just the web traffic. Without organizations are at risk from attacks. Network can utilize network, and that the network is the gate of protected traffic.

Features

- Network-based traffic according to SD-WAN category, application, or customer ID
- Multi-protocol solution with a multi-protocol, multi-protocol, and multi-protocol
- Analytical, visibility, and reporting for comprehensive network and user data

• It has a security level 4 (not recommended for Linux 15) • It supports a single program using a complex security system (multiple protection, 15)



General presentation 14



Protection and Response

Security Information and Event Manager XL-SIEM
Real-time alerts for securing the SME.

The SIEM: XL-SIEM is a platform for collecting information, alerts, and detection from a central location in a system. The information comes from the combination of several monitoring tools focusing on different parts of the organization. The tool provides a unified analysis of the data and information about them in a secure and accessible way. In contrast to other SIEM tools, the XL-SIEM guides and supports with a secure and accessible way to install and update your systems.


Features

- XL-SIEM provides real-time alerts for security events across all the systems
- Lets the user aggregate different sources of SIEM data into a single table for analysis
- Recommendations guide the user to the right tools and system to be installed

• It has a security level 4 (not recommended for Linux 15) • It supports a single program using a complex security system (multiple protection, 15)



General presentation 15



Protection and Response

Early Warning Intrusion Detection System EWIS
Light intrusion detection that is also able to attract attacks away from the systems.

EWIS is a non-intrusive intrusion detection system tailored for SMEs. It is able to run in parallel with the real system, allowing attacks away from the SME's systems. EWIS also provides a graphical interface showing the events that are captured by the sensors. The interface is part of the final SIEM's framework.

Features

- Eviction of production services like the ones SMEs are using
- Hierarchical detection of malicious network events
- Visual representation of real-time and passed network events

• It has a security level 4 (not recommended for Linux 15) • It supports a single program using a complex security system (multiple protection, 15)



General presentation 16

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	73 of 142
Reference:	D6.3	Dissemination:	PU
		Version:	1.0
		Status:	Final



Capabilities and Awareness

Cybersecurity Coach CYSEC

Assess, plan, and track improvements in cybersecurity

Features

- The sleek, plug-and-play tool for easy cybersecurity improvement for the SME
- Recommended use also in your SME's investment journey
- Helps the early stage SME's achievement in getting certified

By 2022 all SMEs in EU countries without any national level initiatives in

By 2025, using a tool support, trained by SMEs in

SMESEC

17



Training Courses and Material

Securityaware.me Training Platform

Interactive training courses

Features

- Securityaware.me is an online platform for creating and managing interactive training courses using real infrastructures and methods (services, computers, networks, etc.);
- Securityaware.me focuses only on cybersecurity; All hosted courses are created by experts from security companies and institutes around Europe and include training material for many different security topics and levels of expertise.

SMESEC

18



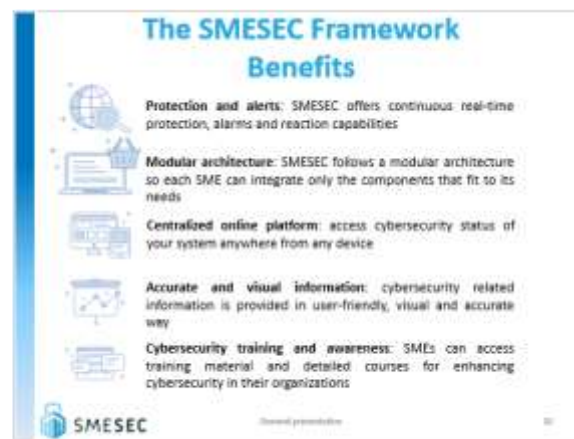
SMESEC

SOLUTION BENEFITS

- Centralized information on Cybersecurity
- Highlight defenses against Cyber threats
- Monitor and motivate your employees

SMESEC

19



The SMESEC Framework Benefits

- Protection and alerts:** SMESEC offers continuous real-time protection, alarms and reaction capabilities
- Modular architecture:** SMESEC follows a modular architecture so each SME can integrate only the components that fit to its needs
- Centralized online platform:** access cybersecurity status of your system anywhere from any device
- Accurate and visual information:** cybersecurity related information is provided in user-friendly, visual and accurate way
- Cybersecurity training and awareness:** SMEs can access training material and detailed courses for enhancing cybersecurity in their organizations

SMESEC

20



The SMESEC Framework Benefits

- Do it yourself:** Step-by-step guidance for meeting customer requirements and standards
- Keep the investment small:** Cost-effective tutorials and tools suitable for a busy environment
- Keep it simple:** Practices adapted to your company instead of complicated formal policies and procedures

SMESEC

21



SMESEC

OUR ONGOING WORK

SMES ANALYSIS AND CYSEC BETA TESTS (CYBERSECURITY AWARENESS TOOL)

22

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	74 of 142
Reference:	D6.3	Dissemination:	PU
	Version:	1.0	Status: Final

Our SME Study Subjects- 4 use cases



E-voting
Smart Grid
Industrial IoT
Smart cities

SMESEC

23

Lessons about Cybersecurity for SME...

Cybersecurity has become a problem, also for SME

- SME may be busy, not have experts, and not willing to invest much

Large companies know how to mature cybersecurity

- comprehensive, evolving, expert-dependent

Adoption and adherence to good practice depends on:

- reward vs. cost | threat vs. coping appraisal | employee involvement

Cybersecurity for SME should be:

- user-controlled, stepwise guided learning with fast results

SMESEC

24

The patient does not take the pill



Up to 90% non-adherence rates

SMESEC

25

Factors for Adoption and Adherence

SMESEC aims at addressing the reasons for (non-) adoption and adherence of cybersecurity in SMEs.

- Protection Motivation: Can I live with the threats?
- Technology Threat Avoidance: Also, is the effort reasonable?
- General Deterrence: Will I be punished? Hard?
- Rational Choice: Do the rewards outweigh the cost?



SMESEC

26

Capability Improvement for SME

a lightweight Cybersecurity framework for thorough protection



SMESEC

27

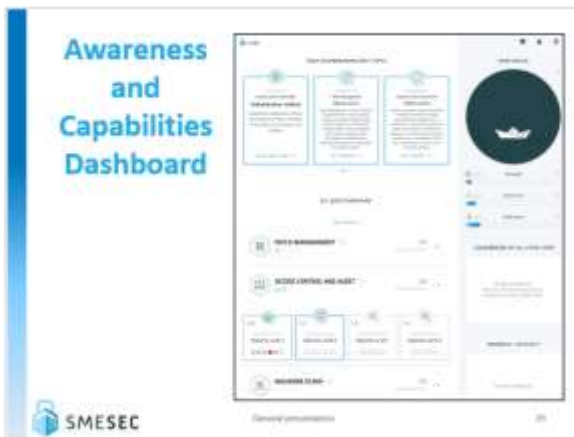
Learn, Act and Track results



SMESEC

28

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	75 of 142
Reference:	D6.3	Dissemination:	PU
	Version:	1.0	Status: Final



29



30



31



32



33



34

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	76 of 142
Reference:	D6.3	Dissemination:	PU
	Version:	1.0	Status: Final



Figure 19: SMESEC General Presentation Slides

3.3 Communication of the Open Call

The SMESEC consortium invited SMEs to participate in the validation of the SMESEC framework. By participating in the open call, an SME not only influence the evaluation of the SMESEC framework, but also improve the own company's security and get up to €20'000 of funds. SMESEC offered to participants a) to improve security and reduce the risk of cyberattacks, b) increase security awareness for employees, and b) provide up to €20'000 of funds per participant.

The open call consisted of a two-step process. In the first stage, at the time of writing this deliverable, the applications had been selected and were in the process of being evaluated. After the selection of applications, a hands-on workshop was planned to be performed with the selected new partners, guidance for using the SMESEC framework provided, and instructions shared for reporting about the experience using the SMESEC evaluation procedures. In the second stage, the results were planned to be collected for evaluating the SMESEC security framework by the selected open call partners.

To achieve a broad validation of the SMESEC framework, four categories of applications were defined:

- Category 1: 1 Red Team. The Red Team will assess the security level of the involved SMEs before and after the deployment of the SMESEC Framework. The applicants will be evaluated based on the proved experience in assessing systems for cyber-threat, their cybersecurity expertise and overall IT experience.
- Category 2a: up to 5 new use case SMEs. The use case SMEs will incorporate SMESEC framework and take advantage of the features provided by SMESEC, including threat protection and response tools, security awareness and training, testing and recommendations. As SMESEC was seeking for a diverse set of SMEs for this category, the applicants were placed into three categories (high, medium, low) based on the expertise on IT and the adoption level of ICT to their day-to-day operations. 2 applicants were foreseen for the high category, 2 for the medium category, and 1 for the low category.
- Category 2b: up to 3 SMEs with extensions for the SMESEC framework. The extensions were expected to represent cybersecurity solutions. The collaboration with the framework-extending SMEs was expected to focus on testing the external integration API,

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	77 of 142	
Reference:	D6.3	Dissemination:	PU	
	Version:	1.0	Status:	Final

incorporating the third-party solutions to the solutions of the SMESEC framework. Sought were experienced SMEs with a strong background in cybersecurity.

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

SMESEC dissemination was involved in the open call for advertising the call and collecting the applications from participating third parties. The call was opened on March 12, 2019, and the submission deadline was May 15, 2019. The start of participation in SMESEC was planned for June 2019.

3.3.1 Advertisement of the Open Call

The open call was published with a call information page and an online facility to register for the open call and submit an application. The screenshot below shows the Open Call page published on the SMESEC homepage, <https://www.smesec.eu/opencall.html>. Note that the current status of “Open Call Closed” was replaced by “Submit Application” while the open call was open.



Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	78 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

– INTRODUCTION –

Objective of the SMESEC project

Small and Medium size Enterprises (SMEs) are an important driver for innovation and growth in the EU. At the same time, SMEs also stand to gain the most from innovative technologies that promise convenient deployment and economical operation of ICT. Taking into account cybersecurity, SMEs do not always understand all the risks and business consequences for the development of technologies without the adequate level of protection against cyber crime.

The European Union Agency for Network and Information Security (ENISA) declares in the "Information Security and Privacy Standards for SMEs" study of 2016 that, despite rising concerns about information security risks, the level of SMEs information security and privacy standards adoption is relatively small.

THE OBJECTIVE OF THE PROJECT CAN BE SUMMARIZED TO THE FOLLOWING:

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

– BENEFITS –

What we offer

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

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

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

TO ACHIEVE A BROAD VALIDATION OF ALL THE FEATURE PROVIDE BY THE SMESEC FRAMEWORK WE HAVE DEFINED THREE DIFFERENT CATEGORIES:

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

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	79 of 142	
Reference:	D6.3	Dissemination:	PU	
	Version:	1.0	Status:	Final

– ELIGIBILITY –

What is expected of participating Companies?

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

All selected SMEs must:

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

– MILESTONES –

Important dates



– HELP –

How to get help

If you have any questions, need more information or just want to tell us your opinion, please don't hesitate to contact us by email opencall@smesecc.eu.

Submit your application to participate in SMESEC Open call (login required)

Participate now to improve your company security, evaluate our framework and get up to €20.000 of funds!

OPEN CALL CLOSED

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	80 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

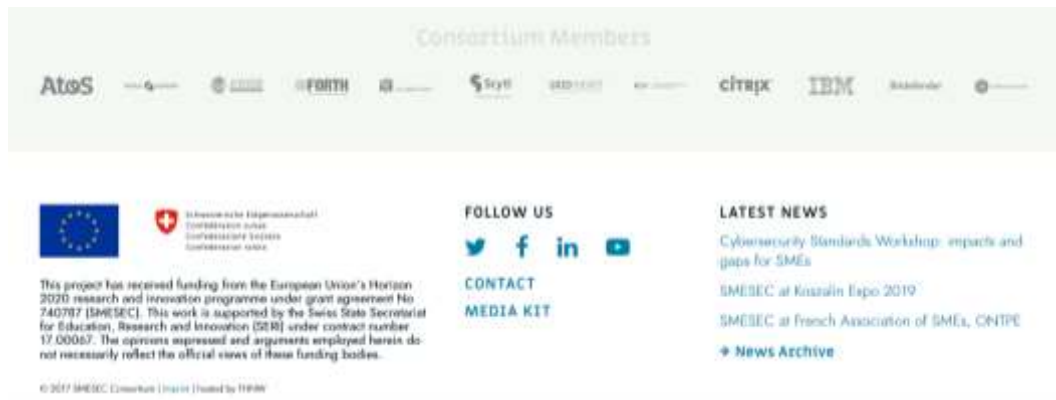


Figure 20: Open Call Page.

The open call was advertised by letting the consortium members spread information about the open call within their local networks. They were encouraged to use the customer and partner contact databases and advertising the call through social and physical media as well as personal contacts to relevant third parties that would qualify for participating in the open call.

3.3.1 Online Campaigns

SMESEC dissemination launched online campaigns on Twitter and Facebook. Twitter was chosen because SMESEC had the largest follower-base on these networks. Facebook offered campaigning capabilities with dedicated targeting of the interesting audience of European SMEs and entrepreneurs, called “boosting.” With the boosting, SMESEC hoped to reach a large share of the relevant SME and entrepreneur audiences and increase the follower numbers.

The following Tweets were posted in a first twitter campaign that emphasized on the open call. The SMESEC partners were encouraged to talk about the tweets and like and retweet the tweets in their local language.



Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	81 of 142	
Reference:	D6.3	Dissemination:	PU	
	Version:	1.0	Status:	Final



Figure 21: Twitter campaign 1.

In a second Twitter campaign, the following tweet was posted:



Figure 22: Twitter campaign 2.

The following Posts were placed on Facebook. Also here, the SMESEC partners were encouraged to talk about the tweets and like and place the posts in their personal feeds.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	82 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final



Figure 23: Facebook campaigns 1 and 2.

The campaigning was supported by reminding the SMESEC partners regularly about the open call and the need of advertising it and by offering feedback on the effectiveness of advertisement actions.

3.3.2 Campaign Monitoring

The campaign produced the outcomes presented in the table below.

Table 14: Access and download statistics of the open call.

Month	Open Call Page	Open Call Downloads
March 2019	Views: 947	Downloads: 45
April 2019	Views: 29'302 (majority coming from the domain sfr.net, a French telecom operator)	Downloads: 90
May 2019	Views: 238	Downloads: 36
Total	Views: 30'487	Downloads: 166


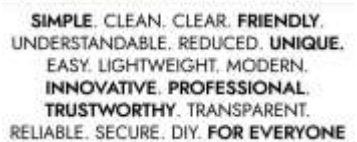
Ignoring the large number of hits from sfr.net, which may be due to an attack on the smesec.eu webpage, the open call page was accessed more than 1'000 times and the PDF version of the page downloaded more than 150 times. This traffic for accessing detailed information indicates that sufficient attention and desire to know more about the open call could be generated.

The majority of the page accesses and open call downloads was generated by directing visitors from channels other than the social media. The numbers below indicate that the online campaigns were effective at generating awareness of the open call but ineffective in creating page visits.

Table 15: Summary statistics for the campaigns on Twitter and Facebook.

Campaign	Twitter	Facebook
Campaign 1	Means: posting, use of followers and offline network	Means: posting, paid boosting to SMEs and entrepreneurs

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	83 of 142	
Reference:	D6.3	Dissemination:	PU	
	Version:	1.0	Status:	Final

Campaign	Twitter	Facebook
	Impressions: 7882 Retweets and likes: 45 Link clicks to open call page: 9 Conversion rate: 0.1%	Impressions: 1911 Likes: 115 Link clicks to open call page: 2 Conversion rate: 0.1%
Campaign 2 	Means: posting, use of followers and offline network Impressions: 1348 Retweets and likes: 12 Link clicks to open call page: 5 Conversion rate: 0.4%	Means: posting, paid boosting to SMEs and entrepreneurs Impressions: 4927 Likes: 514 Link clicks to open call page: 7 Conversion rate: 0.1%

The impressions on Twitter were much dependent on the consortium partner’s activities to make the tweets visible in their personal network. For example, the campaign 1 was translated into for national languages. The German, Spanish, and Greek tweets contributed about one third of the impressions. Each re-tweets or like generated between 100 and 200 impressions.

The impressions on Facebook were much dependent on the amount paid to Facebook for placing the post as an advertisement. We paid 3.4 times more for the campaign 2 and produced 2.6 times as many impressions with that campaign.

3.3.1 Discussion

The conversion rates from social media posts to clicks to the open call page were low, suggesting the interpretation that the social media channels were ineffective for raising interest in the open call among SMEs. Among the possible reasons are a) a lack of SMEs following the SMESEC project, b) lack of clarity of the value proposition of the SMESEC framework, and c) perceived low priority for cybersecurity improvements in the own company. Each of these potential reasons is critical for the future exploitation of SMESEC and is being investigated and influence the dissemination work of the coming months.

Lack of SMEs following the SMESEC project: as described in Section 3.4.3, five SME-related organisations and 10 SMEs were following the SMESEC Twitter channel. The low number of SME followers could be one explanation to why the conversion rate was low. Research is needed to understand how frequent the social media use is among SMEs and, from the perspective of the SMEs, what the barriers are for SMEs to follow the SMESEC project.

Lack of clarity of the value proposition of the SMESEC framework: the work of refining the definition of the SMESEC value proposition was ongoing at the moment of the open call. As a result, the campaigns could not draw on sharp statements about the capabilities of the framework and its components, respectively of sharp statements about the impact the framework generated in SMEs. The campaigns have accelerated the refinement work and, in the meantime, have culminated in an updated flyer, poster, roll-up, and presentation of the SMESEC framework on the webpage. Work on further testing the communication has been planned to be performed in conjunction with the parties joining the SMESEC project as part of the open call.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	84 of 142		
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

Perceived low priority for cybersecurity improvements in the own company: the challenge of adopting cybersecurity and adhering to good practice is the central challenge that SMESEC addresses and has been recognized since the launch of the SMESEC project. Once the value proposition is refined, the messages spread by the SMESEC dissemination should change to reflect the criticality of the cyberthreats addressable by the framework, the simplicity and low cost of using the SMESEC framework, and the benefits from using the framework as an individual SME and the whole community of SMEs.

The outcomes and reflections about the open call experience will be essential for guiding the third year's dissemination work, aiming at preparing the community of SMEs for the take up of the eventually released SMESEC framework.

3.4 Dissemination Report

3.4.1 Blog with External Events

In the second year, partners investigated different channels participating in various events implying different communities. Mostly accompanied by project presentation, these activities were the opportunity to access all channels such as technology-oriented stakeholders, other sister projects but also SMEs specialized events.

Feedbacks from these events and workshops are promising and partners will pursue in the coming year to enhance the SMESEC audience. The SME channels are already established, and the consortium established contacts with the CEA PME, the European SMEs organization and the AFDEE, the French association, that will help us in disseminating the project outcomes.

Table 16 shows the event participation of SMESEC consortium members during Year 2 and summarizes the dissemination activities from June 2018 to May 2019. The event presentation and the role of SMESEC is presented in the following sections.

Table 16: External Events with SMESEC Involvement

Target	Activity	Event / Channel	Partner	Date	Place
Cybersecurity	Conference Participation	ETSI Security Week	EGM	Jun, 2018	Sophia Antipolis, France
Cybersecurity	Summer School	(CySeP) Summer School	FORTH	Jun 2018	Stockholm, Sweden
Cybersecurity	Booth	Swiss SME Association SKV	FHNW	August, 2018	Zurich, Switzerland
Cybersecurity	Conference Talk	RAID 2018	FORTH	Sep 2018	Heraklion, Crete, Greece

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	85 of 142		
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

Target	Activity	Event / Channel	Partner	Date	Place
Cybersecurity	Workshop Talk	1st SMESEC Workshop	FORTH	Sep 2018	Heraklion, Crete, Greece
Cybersecurity	Workshop Talk	IOSEC-CIPSEC Workshop	UU, UOP, IBM, Bitdefender	Sep 2018	Heraklion, Crete, Greece
Cybersecurity	Summer School	NIS Summer School	FORTH	Sep 2018	Heraklion, Crete, Greece
Cybersecurity	Workshop Talk	Cyberwatching.eu first Annual Workshop	Atos	Oct 2018	Krakow, Poland
Industry	Booth	IoT Solutions World Congress	FHNW, EGM	Oct 2018	Barcelona, Spain
Cybersecurity	Webinar	Cyberwatching.eu Webinar in Cyber Risk Management from the SME Point of View	FHNW	Oct 2018	-
Industry	Booth	Swiss Innovation Forum	FHNW	Nov 2018	Basel, Switzerland
Industry	Talk	European Utility Week 2018	GridPocket	Nov 2018	Vienna, Austria
Industry	Booth	ICT 2018, Booth	EGM, FHNW	Dec 2018	Vienna, Austria
Cybersecurity	Talk	ICT 2018 Networking on Cybersecurity for SME	Atos	Dec 2018	Vienna, Austria
Industry	Booth	E-World	GridPocket	Feb, 2019	Essen, Germany
Cybersecurity	Conference Talk	NDSS	FORTH	Feb, 2019	San Diego, US
Cybersecurity	Conference Talk	ONTPE (French SME association)	EGM	Mar, 2019	Paris, France
Cybersecurity	Workshop Talk	GHOST's Clustering Workshop	FORTH	Mar, 2019	Athens, Greece
Industry	Exhibition	Koszalin Fair	GridPocket	Mar, 2019	Koszalin, Poland

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	86 of 142
Reference:	D6.3	Dissemination:	PU	Version:	1.0
				Status:	Final

Target	Activity	Event / Channel	Partner	Date	Place
Industry	Workshop Talk	Patras IQ 2019	UOP	April, 2019	Patras, Greece
Cybersecurity	Workshop	Cybersecurity Standards Workshop	EGM, UU	May, 2019	Brussels, Belgium

3.4.1.1 ETSI Security Week



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 standardisation, policies, and solutions.

It offered the opportunity to discuss the underlying cybersecurity challenges and resulting technical and standardisation actions taken or needed to overcome 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 favourably 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 standardisation community.

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

3.4.1.2 (CySeP) Summer School

Cybersecurity and Privacy (CySeP) Summer School, hosted in Stockholm, Sweden from June 11th to 15th, was an event in cybersecurity which gathered students, engineers or practitioners interested in security and privacy, teachers of security courses, and researchers.

It offered the opportunity to discuss how to address real-world security and privacy (S&P) problems. Foundation for Research and Technology – Hellas (FORTH) participated in the CySeP 2018. And “A Large-scale Analysis of Content Modification by Open HTTP Proxies” has been presented as a poster.

For SMESEC, the summer school offered an opportunity to exchange with peer researchers and attract young potentials to the challenge of securing SMEs.

More information: <https://cysep.conf.kth.se/index.html>

3.4.1.3 Swiss SME Association SKV



The Swiss SME Association, SKV, is a Switzerland-wide association fostering good economic and legal conditions for SMEs in Switzerland. As part of the offering, the SKV organises and supports fairs that allow SME to meet, learn from each other, and establish business relations. Roland Rupp, vice president of SKV shared his vision with SMESEC: “to win customers, you need to be present as a person, and this is what we do at our fairs.”

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	87 of 142		
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

SMESEC presented the first prototype of the cybersecurity advisor at the fair and interviewed SME owners about their view of cybersecurity. The SME fair allowed SMESEC to obtain an in-depth understanding of the SME's approach to cybersecurity and received registrations for the SMESEC beta programme. The SMESEC consortium looks forward to joining further fairs!

More information: <http://www.netzwerk-zuerich.ch/30082018.html>

3.4.1.4 RAID 2018



The 21st International Conference on Research in Attacks, Intrusions, and Defences (RAID), co-located with IOSec 2018 and SMESEC Workshop, hosted in Heraklion, Crete, Greece on 10-12 September 2018. RAID provides the possibility for computer and information security researchers and technical staff from the academic community, government, and industry to exchange their ideas and advancements. RAID 2018 was organized by the Foundation for Research and Technology - Hellas (FORTH).

Since RAID conference co-located with the 1st SMESEC Workshop, SMESEC partners also had meetings during the conference and presented and discussed their achievements in two technical and non-technical parts.

More information: <https://www.raid2018.org/>

3.4.1.5 1st SMESEC Workshop



The first SMESEC workshop co-located with the 21st International Symposium on Research in Attack, Intrusions, and Defences (RAID) hosted in Crete, Greece, 14 September 2018. This workshop organized by the Foundation for Research and Technology - Hellas (FORTH) and it provided the possibility for the SMESEC partners to present their advancements in two

technical and non-technical parts.

Although Small and Medium-sized Enterprises (SMEs) have a significant role in European businesses, they are not capable enough of safeguarding themselves against cyber-attacks. SMESEC aims to be a holistic security framework to offer a variety of solution, tools, and training content to SMEs.

More information: <https://www.raid2018.org/smesecworkshop.html>

3.4.1.6 IOSEC-CIPSEC Workshop

The first IOSec Workshop 2018 co-located with the 21st International Symposium on Research in Attack, Intrusions, and Defences (RAID) hosted in Crete, Greece, 13 September 2018. This workshop was supported by Enhancing Critical Infrastructure Protection with innovative SECURITY framework (CIPSEC).

SMESEC partners, including the Univesity of Patras, the Univesity of Utrecht, IBM, and Bitdefender, attended the IOSEC workshop. During the workshop, SMESEC partners' papers with a SMESEC acknowledgment were presented.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	88 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

More information: <https://www.raid2018.org/cipsecworkshop.html>

3.4.1.7 NIS Summer School



5th Network and Information Security Summer School is hosted in Crete, Greece, 24 - 28 September. The theme of the event for this year was "The Challenge of the Changing Risk Landscape" and changing security “ecosystem” can be one of the main challenges of Information Security. The event is managed by ENISA and the Foundation for Research and Technology - Hellas (FORTH) together. And it provides the possibility for the policymakers from the EU Member States and EU Institutions, decision-makers from industry and researchers from the academic community to have dialogue and exchange their ideas and advancements.

FHNW - Fachhochschule Nordwestschweiz presented SMESEC project and a model of the cybersecurity advisor. Received feedback from cybersecurity experts and also SMEs during different meetings may help SMESEC to obtain an in-depth understanding of the challenges and solutions regarding SMEs' cybersecurity problems.

More information: <https://nis-summer-school.enisa.europa.eu/>

3.4.1.8 Cyberwatching.eu first Annual Workshop



The first Annual Workshop of the European observatory of research and innovation in the context of cybersecurity and privacy (Cyberwatching.eu) was organised at CYBERSEC Forum 2018 in Krakow, Poland.

Jose Fran. Ruiz (project coordinator of SMESEC), from Atos, presented the objectives of the SMESEC project and participated in the discussion about how to increase the adoption of results of European research projects by users, focusing on the area of SMEs thanks to the feedback obtained so far from end-users and other SMEs. The roundtable generated a discussion about the barriers for adoption and impact in organizations in Europe and strategies that could facilitate better interaction between end-users and projects at an early stage of the work.

More information: [Cyberwatching.eu first Annual Workshop](#)

3.4.1.9 IoT Solutions World Congress



IoT Solutions World Congress, co-located with Blockchain Solutions World and AI & Cognitive Systems Forum, was hosted in Barcelona, Spain on 16-18 October 2018. During the exhibition, more than 16000 visitors (including SMEs) from 120 countries and 300 exhibitors, sponsors, and partners participated.

On behalf of SMESEC project, EGM (Easy Global Market) and FHNW (Fachhochschule Nordwestschweiz) presented SMESEC, partners, and the objectives of the project. During the event, not only was SMESEC be able to visit some SMEs from different countries, but also had meetings with companies working on topics such as IoT, GDPR compliance, and Cybersecurity to exchange their advancements and ideas.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	89 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

More information: <https://www.iotsworldcongress.com/>

3.4.1.10 Cyberwatching.eu Webinar in Cyber Risk Management from the SME Point of View

On October 17, FHNW participated in the “Cyber risk management from the SME point of view” webinar in Cyberwatching.eu (the European observatory of research and innovation in the context of cybersecurity and privacy). Although cyber threats for SMEs are significant, it seems SMEs are not aware and capable enough to protect themselves and do not consider the risk of cyber-attacks in their business model.

Samuel Fricker (Ph.D., Professor at FHNW University of Applied Sciences and assistant professor at Blekinge Institute of Technology) presented SMESEC project (a framework to provide a variety of cybersecurity tools and training content) and the results of a research report based on this project. Also, he invited SMEs for the SMESEC beta programme.

More information: <https://www.cyberwatching.eu/cyber-risk-management-sme-point-view>

3.4.1.11 Swiss Innovation Forum



The Swiss Innovation Forum is Switzerland’s leading innovation conference. In 2018, the innovation forum was dedicated to surprise as the key to innovation and growth. Associated with the innovation forum was the Future Expo, a unique exhibition that conveys the latest knowledge from a wide range of industries with futuristic prototypes, promising projects, and new technologies. In total, more than 1100

entrepreneurs, CEOs, politicians, researchers, experts, students, and other personalities participate.

SMESEC was selected by “swissuniversities” as one of the top-3 innovation projects run by Swiss universities or universities of applied sciences. For SMESEC, the participation at the Swiss Innovation Forum represented an opportunity to expose cybersecurity for SMEs to the leading innovation community in Switzerland. Several contacts were created with opportunities for strengthening dissemination and enhancing the SMESEC innovation.

More information: <https://www.swiss-innovation.com>

3.4.1.12 European Utility Week



GridPocket joined the European Utility Week 2018 in Vienna and presented the SMESEC Framework to interested SMES and other companies. “The European Utility Week is an environment for all key players in the smart energy ecosystem to come together and discuss European strategy to achieve a smooth transition towards a low carbon energy supply.”

For SMESEC, the talk at SMESEC allowed raising awareness about cybersecurity and inform about the SMESEC framework.

More information: www.european-utility-week.com

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	90 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

3.4.1.13 ICT 2018, Booth



The ICT 2018 conference is a large-scale research and innovation event that took place in Vienna on December 4-6, 2018. The event focused on the European Union’s priorities in the digital transformation of society and industry. ICT 2018 attracted 4800 visitors.

SMESEC was present with a booth. At the booth, the visitors could experience a lightweight do-it-yourself cybersecurity assessment, benefit from a preview of the FHNW cybersecurity coach, and discuss with SMESEC experts from ATOS, FORTH, Easy Global Market, and FHNW. Several contacts were created with opportunities from extending the SMESEC vision, enabled by the

coming H2020 calls.

More information: <https://ec.europa.eu/digital-single-market/en/events/ict-2018-imagine-digital-connect-europe>

3.4.1.14 ICT 2018, Networking on Cybersecurity for SME



The ICT 2018 conference is a large-scale research and innovation event that took place in Vienna on December 4-6, 2018. The event focused on the European Union’s priorities in the digital transformation of society and industry. ICT 2018 attracted 4800 visitors.

SMESEC moderated a networking session on cybersecurity for SMEs. For SMESEC, the participation at ICT 2018 represented an opportunity to expose the SMESEC vision of guided do-it-yourself cybersecurity for SMEs to the European research and innovation community. Several contacts were created with opportunities for strengthening dissemination and enhancing the SMESEC innovation.

More information: <https://ec.europa.eu/digital-single-market/en/events/ict-2018-imagine-digital-connect-europe>

3.4.1.15 E-World



GridPocket joined the E-World 2019 in Essen and presented the SMESEC Framework to interested SMES and other companies. “E-world energy & water is the place where the European energy industry comes together. Serving as an information platform for the energy sector, E-world is gathering international decision makers in Essen each year. More than one fifth of the exhibiting

companies are based abroad. The majority of international exhibitors come from countries of the European Union.”

For SMESEC, the talk at SMESEC allowed raising awareness about cybersecurity and inform about the SMESEC framework as well as the upcoming open call allowing SMEs to join the SMESEC project.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	91 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

More information: <https://www.e-world-essen.com/en/>

3.4.1.16 NDSS



The NDSS symposium fostered information exchange among researchers and practitioners of network and distributed system security. The target audience included those interested in practical aspects of network and distributed system security, with a focus on actual system design and implementation. A major goal was to encourage and enable the Internet community to apply, deploy, and advance the state of available network and distributed systems security technology.

Giorgos Vasiliadis presented "Master of Web Puppets: Abusing Web Browsers for Persistent and Stealthy Computation" paper from FORTH. The paper shows the powerful capabilities which modern browser APIs provide to attackers by presenting MarioNet.

For SMESEC, the conference offered the opportunity to present the cybersecurity expertise of the consortium and obtain feedback and comments from cybersecurity experts.

More information:

<https://www.smesec.eu/publications.html> | <https://www.smesec.eu/publications.html>

3.4.1.17 ONTPE (French SME association)



ONTPE organisation intends to support executives of French companies with fewer than 20 employees. The last event, cybersecurity of TPE conference, took place in Paris on March 14, 2019, and attracted 60 participants.

The conference had 11 speakers, and Philippe Cousin from Easy Global Market presented SMESEC. This event was the first step for the project to work with the French Association of SMEs, and SMESEC is preparing to join further fairs in Lille and Marseille.

More information: <https://www.eventbrite.fr/e/billets-cybersecurite-pour-les-tpe-etes-vous-suffisamment-protége-53779201038>

Link to the video: https://www.youtube.com/watch?v=SLCt_j96NMU

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	92 of 142		
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

3.4.1.18 GHOST's Clustering Workshop



Dr. Sotiris Ioannidis presented the SMESEC project to the participants of the workshop, positioning cybersecurity for SMEs in the broader cybersecurity activities of the H2020 project cluster. For SMESEC, the workshop represented a platform a dissemination and opportunities for future join activities to reinforce the securing of the European economy. For SMESEC, the workshop represented a platform a dissemination and opportunities for future join activities to reinforce the securing of the European economy.

Link: https://docs.wixstatic.com/ugd/1d2842_ea779c8abd0e45e98cf9d8aa25885592.pdf

3.4.1.19 Koszalin Fair



Koszalin Expo 2019 was the 17th job fair event that was organised by Koszalin University of Technology on March 21th, 2019. The exhibition aimed to support students and graduates.

During the exhibition, GridPocket presented SMESEC in a booth and made several contacts with other companies. Moreover, SMESEC was introduced in a conference about cybersecurity threats entitled "Cybersecurity in large datasets and progressive digitisation of life and economy".

More information: <http://targipracy.koszalin.pl/kat/227/program-targow>

3.4.1.20 Patras IQ 2019



Patras Innovation Quest (Patras IQ) was the 6th Technology Transfer Exhibition that took place on April 12-14, 2019. This event has been established as the continuous meeting for interconnecting know-how and innovation with entrepreneurship, maintaining the fruitful research and entrepreneurial human capital of Greece and on the overall development of the local, regional and national economy. This year exhibition includes a variety of events, workshops and exhibitors' booths, while emphasis was placed on the potential that will be provided in the future by the implementation of 5th generation wireless technology (5G).

The University of Patras and the NAM Group of the ECE department of the University of Patras presented SMESEC with a booth and demonstrated how the SMESEC project can enhance SMEs' security against cyber-attacks.

More information: <https://www.patrasiq.gr/>

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	93 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

3.4.1.21 Cybersecurity Standards Workshop



SMESEC project co-organised a workshop on “Cybersecurity Standards: what impacts and gaps for SMEs” with STANDICT.eu project, on the 24th of May 2019, at the CEN-CENELEC Management Center, in Brussel, Belgium. This workshop aimed to identify the state of the art, gaps, and needs for cybersecurity standardization for SMEs. There were 28 participants in the workshop and 12 talks in total.

SMESEC project was also presented to the participants.

SMESEC identified cooperation opportunities with StandICT.eu to push standardisation actions for SMEs (and finance them) over their open calls. SMESEC is planning to push standardisation actions to CEN/CENELEC and ETSI. SMESEC will follow up with ECSO, Digital SME Alliance and SBS for SME involvements and contribution to the revision of key documents.

More information: <https://www.eventbrite.com/e/cybersecurity-standards-what-impacts-and-gaps-for-smes-tickets-60529098162>

3.4.2 Blog with News

In the second year, 10 blog entries related to the project management board meetings, activities, and content-related news were published.

The following subsections report these blogs.

3.4.2.1 CySME (Content-related news)

As part of the SMESEC framework, Utrecht University will provide SMESEC information security maturity model (CySME) adjusted explicitly to SMEs.

At the core of the SMESEC framework are two security assessment models developed from 2011 onward at the Applied Data Science Lab in the Department of Information and Computing Sciences of Utrecht University: ISFAM and CYSFAM.

The Information Security Focus Area Maturity (ISFAM) model and the Cyber Security Focus Area Maturity (CYSFAM) model provide a highly complete security quick-scan for organisations based on both the state-of-the-art in scientific literature and industry standards including ISO27K. The assessment models have been evaluated successfully in various application domains such as telecom, logistics, healthcare, and finance.

The CYSFAM includes focus areas for application security, cybersecurity and network security, and a tentative relationship with internet security. Therefore, it is now becoming possible to attempt to create one harmonised, modular and federative maturity model for security focus areas that enables a complete security quick-scan tailored to specific organisational characteristics.

CySME will be developed by revising and extending the existing maturity models to make them better suitable for SMEs. Even more so, CySME will be designed in a way that SMEs can perform the security assessments themselves, without the help of IT experts. Also, the SMESEC technologies available from

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	94 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

the SMESEC partners will be connected to the models to help implement the SME's desired security capabilities. The SMESEC pilots will be used as case studies to obtain in-depth feedback from end-users and experts. The validation results will be used to tailor the SMESEC assessment and improvement approach to the identified needs of SMEs and ecosystems.

UU's strategic goal is to contribute to establishing cybersecurity standardisation guidelines for organisations in general, and SMEs in particular.

UU's team consists of Bilge Yigit Ozkan, and Marco Spruit.

3.4.2.2 Project Management Board Meeting in Madrid



On May 29-30, the project partners of the SMESEC consortium gathered for the fourth general meeting in Madrid, Spain, in the offices of Atos.

The meeting focused on presenting the advancements done since the last meeting and initial preparation of items for the upcoming first review. So far, the work is in a good pace, having, among others, initial versions of integrations of the framework, preparation of cybersecurity courses and awareness for SMEs, information kit for SMEs, and creation of the first

SMESEC Workshop.

The SMESEC consortium has decided to initiate collaboration with a large number of SMEs already during the second year of the project.

3.4.2.3 Recent Media Coverage in Spain

Several Spanish digital and printed newspapers echo the work and objectives of the project, focusing on how SMESEC will support and help SMEs in building cybersecurity. Among others we can find:

- Computing: Atos lanza el proyecto SMESEC para mejorar la ciberseguridad de las pymes

<http://www.computing.es/seguridad/noticias/1104942002501/atos-lanza-proyecto-smesec-mejorar-ciberseguridad-de-pymes.1.html>

- CSO: Atos presenta el Proyecto SMESEC pensando en la ciberseguridad de las pymes

<https://cso.computerworld.es/social-security/atos-presenta-el-proyecto-smesec-pensando-en-la-ciberseguridad-de-las-pymes>

- Dealerworld: El proyecto SMESEC de Atos aborda la ciberseguridad de la pyme

<https://www.dealerworld.es/actualidad/el-proyecto-smesec-de-atos-aborda-la-ciberseguridad-de-la-pyme>

- Digital affaires: Atos lanza el proyecto SMESEC cofinanciado por la Unión Europea para mejorar la ciber-seguridad de las Pymes

<https://digitalaffaires.es/art/4081/atos-lanza-el-proyecto-smesec-cofinanciado-por-la-union-europea-para-mejorar-la-ciber-seguridad-de-las-pymes>

- EFE empresas: Atos lanza el proyecto SMESEC cofinanciado por la Unión Europea

<https://www.efeempresas.com/noticia/atos-semec-union-europea/>

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	95 of 142		
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

- El Candelero Tecnológico: Atos lanza el proyecto SMESEC cofinanciado por la Unión Europea para mejorar la ciber-seguridad de las Pymes

<https://elcandelerotecnologico.com/tag/proyecto-smesec/>

- Globedia: Atos lanza el proyecto SMESEC cofinanciado por la Unión Europea para mejorar la ciber-seguridad de las Pymes

<http://globedia.com/atos-lanza-proyecto-smesec-cofinanciado-union-europea-mejorar-ciber-seguridad-pymes>

- GPS news: Atos lanza el proyecto SMESEC cofinanciado por la Unión Europea para mejorar la ciber-seguridad de las Pymes

<https://gpsnews.es/art/7778/atos-lanza-el-proyecto-smesec-cofinanciado-por-la-union-europea-para-mejorar-la-ciber-seguridad-de-las-pymes>

- Hispavista: Atos lanza el proyecto SMESEC cofinanciado por la Unión Europea para mejorar la ciber-seguridad de las Pymes

<http://noticias.software.hispavista.com/n20180419152123.atos-lanza-proyecto-smesec-cofinanciado-union-europea-mejorar-ciber-seguridad-pymes>

- IT user: Impulso a la ciberseguridad de las pymes

<https://tecnologiaparatuempresa.ituser.es/seguridad/2018/04/impulso-a-la-ciberseguridad-de-las-pymes>

- TIC PyMEs: La Comisión Europea apoyará a las pymes en la gestión de riesgos

<http://www.ticpymes.es/legislacion/noticias/1104942049204/comision-europea-apoyara-pymes-gestion-de-riesgos.1.html>

Download the SMESEC media kit: <https://smesec.eu/mediakit.html>

3.4.2.4 Security Issues in IoT Devices (Content-related news)

The rapid advent and growth of the Internet of the Things (IoT) technologies are missing, in many cases, the implementation of effective security measures behind. Networks of thousands of devices are connecting critical infrastructures of cities, and devices with highly restricted computational power (normally already overused with the tasks they are specifically designed to perform) have no margin to deploy security procedures that are at best basic or even nonexistent.

Settled this baseline, the attacks to which these devices are exposed to are potentially endless. Here, we present one of the most common: the botnets. A botnet is defined as a logical collection of Internet-connected devices whose security has been breached, and their control is ceded to a third party.

Once those units are compromised, they receive instructions from a central computing system that will coordinate the attacks. The problem that we face here is higher than it might seem at first glance: not only all our devices (including those deployed on clients' premises) will stop working to perform the attackers' tasks, but also our IP addresses will be the only information that the victims will presumably see with consequent damage to our public image. Botnet-based-attacks consequently endanger the reputation of the companies.

IoT solutions should then embrace security from the very beginning conception and design phase to avoid undesired scenarios. Security architects have to be involved in the definition of the project to

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	96 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

identify potential security breaches in the system and then keep the collaboration and the information flowing internally until the end of the development process. Actually, this approach is summarized by the Privacy by Design concept enshrined in the GDPR, and it is considered a best practice that all IoT actors should follow from now on, even if no personal data are processed.

The approach of the security architect at this point must be minimalistic, meaning that this figure will reduce as much as possible the complexity of the system to guarantee a clear view of all the elements and minimize the risk level associated to each of them. On top of this, access control will provide the last layer for a proper hardening. In fact, in-depth analysis to effectively manage the requested accesses to the specific assets, blocking undesired connection attempts, becomes a must. Having a narrow range of permitted connections drastically reduces the attack surface and resources are then properly allocated in the identified inevitable fissures.

SMESEC aims to identify what are the needs from the SME perspective and translate them into requirements for a unified framework, created by the joint of the different solutions and expertise areas of the partners. The products can cover a wide range of security market segments, and it is expected that the unification will bring even higher added value to the products and the Framework.

Olmo Rayón

Cybersecurity Manager at Worldsensing

3.4.2.5 Developing Partnerships to Enhance Security (Content-related news)

IBM and WORLDSENSING

Within this framework, IBM will be the example of how a large company can collaborate with an SME. From WS (Worldsensing) perspective, having the expertise of IBM Research contributes substantially to the development of the products with a more security-concerned approach. On the other hand, IBM has the chance to work with cutting-edge IOT technology, keeping an eye on emerging markets.

In this case, IBM contribution is a hardware-based solution working to protect WS architecture against a big percentage of code-injection attacks. We are referring to ROP techniques (Returned Oriented Programming), which are part of the attack vector for code-injection in more than 90% of the times.

ROP is an exploitation technique that allows an attacker to take control of a program flow by smashing the call stack and execute instruction sequences. The attacker borrows gadgets, or small pieces of code, from the hijacked program to execute malicious code.

WS's effort is focused on integrating this shuffled code within their infrastructure. Actually, the exact location of the solution will be the middle point of our Load-sensing architecture: the gateways. The gateways are connecting the sensors (that are collecting the user data) with the Cloud environment (which is providing with the intelligence on the data and the visualization tools for the end user).

EGM and WORLDSENSING

Easy Global Market (EGM) and WS interaction is another example of the collaborations taking place within the project, but in contrast to the previous case, between two SMEs. EGM is providing services regarding validation and testing of WS's pilots. In this matter, EGM provides advanced tools and methodologies for automated testing systems.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	97 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

MBT (Model-Based Testing) is at the cutting-edge of automated testing; it is a scalable method for complex development systems that offers reliable results by the deployment of a large cover and fast execution testing environment.

On the other hand, WS aims with the insights of their systems to create a tailor-made set testing strategy that will be an enabler to understand the security levels in the present endpoints, the Loadsensing-connected sensors.

Olmo Rayón

Cybersecurity Manager at Worldsensing

3.4.2.6 End Node Security and Trust vulnerabilities in the Smart City Infrastructure (Content-related news)

Many cities around the globe have started becoming “smart cities,” deploying various technologies and digital infrastructures to increase the quality of their services and consequently the quality of life of their citizens. Smart cities offer extensive opportunities by concentrating on urban services and fostering intelligence within networks. A smart city collects various types of electronic data and processes them to a) manage its assets and resources efficiently and b) improve the operations and services provided to its citizens. Data are generally collected from citizens, devices, assets, etc. and are used for the optimization of transportation systems, power plants, water supply networks, waste management, law enforcement, public safety, etc.

A simplified architecture of the smart city is divided into various components fitting in four layers: Sensing and Control Layer, Communication Layer, Processing Layer, Application Layer.

Smart cities are vulnerable to nearly every type of attack in the ICT sector. For the application layer, smart cities applications and services have to deal with injection attacks, cross-site scripting, broken authentication/authorization mechanisms leading to authorized access and sensitive information leaking, social engineering, insecure 3rd party applications/components, etc. For the processing layer, the attacks include DDoS attacks, hacking and intrusion, worms, viruses, and malware, etc. For the communication layer, smart cities are also facing the attacks of existing network infrastructures. Such attacks include jamming, spoofing, wormholes, man-in-the-middle, sinkhole, Sybil, eavesdropping, replay, etc. as those can be manifested in the various layers of the OSI network model. However, most of the above attacks can be mitigated using solutions and products from the Information Technology domain.

A smart city may be seen as a collection of diverse systems forming dynamic applications and services. Thus, complete security cannot be applied in the form of one single framework or product that covers everything. The approach to secure smart cities infrastructures is to a) ensure that its components maintain high levels of security and b) evaluate the vulnerabilities of each new service or application, also examining their security impact on shared systems and resources.

The end node of smart city infrastructure is usually associated with the sensing and control layer of the smart city and partially with the communication layer. Cybersecurity attacks on the end nodes can assume different forms depending on the kind of end node devices (embedded or Personal Computer). While there exist a broad range of attacks targeting PC devices, widely explored, and thwarted by international literature works and products, the embedded system domain is mostly unexplored (and unprotected) regarding cyber-attacks.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	98 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

Recent attacks that exploit cyber-physical systems have triggered interest in cyber-physical/embedded system cybersecurity countermeasures that yet still adopt the same principles as the PC based ones. However, while most high-end software cybersecurity solutions can potentially protect against attacks based on software vulnerabilities, when it comes to hardware vulnerabilities the attackers still have a rich unexplored area to exploit with few countermeasures (if any) to thwart them.

So, end nodes can be attacked in an unconventional way by exploiting hardware vulnerabilities. Thus, a smart city designer and security administrator should be very careful on the choice of deployed end nodes on the smart city urban grid if he is to retain the security level that latest network standards offer him.

Apostolos P. Fournaris, Konstantinos Lampropoulos

University of Patras

3.4.2.7 [Open HTTP proxies an open threat for the SMEs \(Content-related news\)](#)

Open HTTP proxies offer a quick and convenient solution for routing web traffic towards a destination. In contrast to more elaborate relaying systems, such as anonymity networks or VPN services, users can freely connect to an open HTTP proxy without the need to install any special software. Therefore, open HTTP proxies are an attractive option for bypassing IP-based filtering, geo-location restrictions or in-company firewall filtering, circumventing content blocking and censorship and in general, hiding the client's IP address when accessing a web server. Nevertheless, the consequences of routing traffic through an untrusted third party can be severe, especially when such untrusted parties are used within SMEs, as not only they can pose serious threats to individual users, but also to the cybersecurity of the enterprise.

Rogue web proxy operators can monetize their traffic by altering the relayed content to inject ads and affiliate links, prompt users to download spyware and other unwanted software, or mount phishing attacks. Even more deviously, instead of placing additional ads that may annoy users, miscreants can replace existing ads in the page with their own ads. This can be as simple as replacing a website's ad network identifier with the attacker's own affiliate identifier, essentially stealing the revenue of the original website (i.e., publisher).

The proliferation and widespread use of open web proxies necessitate an approach to detect, understand and measure the extent of content modification by such rogue proxies.

To understand and measure the extent of content modification by rogue HTTP proxies, researchers have designed a methodology for detecting and analyzing content alteration and code injection attempts. Specifically, a framework was built that regularly collected publicly available HTTP proxies from several "proxy list" websites and tested them using a novel technique based on decoy websites (dubbed honey-sites) under the researchers' control on a daily basis. The team had also built a content modification detection approach that operated at the level of a page's DOM (Document Object Model) tree, for detecting even slight object modifications, and a clustering technique for grouping together similar cases of content modification.

The results suggest that 5.15% of the tested proxies perform some form of modification that can be clearly considered malicious. The observed modifications included the injection of extra (or the modification of existing) ads, the inclusion of tracking and fingerprinting libraries, and the collection of data from social networking services on which the user is already authenticated. Besides that, the

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	99 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

researchers also discovered more severe and sophisticated instances of malicious behaviour such as SSL (Secure Sockets Layer) stripping. Specifically, 47% of the malicious proxies injected ads, 39% injected code for collecting user information that can be used for tracking and fingerprinting, and 12% attempted to redirect the user to pages that contain malware.

The use of malicious proxies within the IT/OT network of an SME can result into the compromising of key assets of the SME, failures to part or the whole infrastructure, denial of service attacks or user-tracking and even enterprise espionage. As a step towards protecting users and SMEs against unwanted content modification, the researchers built a service that leverages the proposed methodology to collect and probe public proxies automatically and generates a list of safe proxies that do not perform any content modification, on a daily basis. Apart from the whitelisting service provided by the authors and as new security threats both internal and external arise every day, all SMEs must strengthen their day-to-day operation with continuous security training for all employees and use a variety of IT security tools tailored to their specific needs.

Manos Athanatos, based on "A Large-scale Analysis of Content Modification by Open HTTP Proxies." Foundation for Research and Technology - Hellas

3.4.2.8 Aargauer Zeitung reporting about SMESEC



Cybersecurity is about awareness as much as it is about defence. For that reason, the Aargauer Zeitung has cooperated with FHNW to disseminate information about the SMESEC project and reach its 550'000 newspaper readers in Northwestern Switzerland.

The article informs about the cybersecurity challenges of SME, the SMESEC approach, and invites SME to register for the SMESEC beta program. The article may be downloaded here (navigate to "Digitaler Berater für KMU in Kampf gegen Cyber-Risiken").

<https://www.aargauerzeitung.ch/publireportage/woher-das-smartphone-kommt-und-wohin-es-geht-132972550>

3.4.2.9 Project Management Board Meeting in Nice



On January 15-16, the project partners of the SMESEC consortium gathered for the regular general meeting in Nice, France, organized by Easy Global Market.

The meeting focused on presenting the advancements done since the last meeting and preparation of items for the upcoming review. During the meeting, partners discussed different topics such as dissemination and exploitation activities, upcoming events for partners, standardization, framework integration, SMESEC Tools, end-user training and awareness, planning for the open call and framework assessment. Also, CYSEC (Cybersecurity Coach) has been presented, and SMESEC partners provided interesting feedback.

The SMESEC partners have decided to proceed with discussions about framework integration and open call plans.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	100 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

3.4.2.10 Cybersecurity Standards Workshop: impacts and gaps for SMEs



“Cybersecurity Standards Workshop: impacts and gaps for SMEs” is a one-day workshop hosted by CEN & CENELEC Management Center and intends to support SMEs in the relevant cybersecurity policies, rules, and standards. Also, CENELEC on cybersecurity, ETSI TC Cyber, Digital SME Alliance, and European Cybersecurity Organization (ECISO) are participating. The workshop takes place in

Brussels on May 24, 2019, from 10:00 to 16:00.

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

More information and registration: <https://www.eventbrite.com/e/cybersecurity-standards-what-impacts-and-gaps-for-smes-tickets-60529098162>

3.4.3 Social Media Posts using Twitter, Facebook, LinkedIn, and YouTube

SMESEC was publishing news and information about cybersecurity, the consortium, work, and results, including the SMESEC Framework, on Twitter, Facebook, Linked-In, and You Tube. These channels were adapted to the SMESEC visual language. Figure 24 gives a snapshot of these channels.



Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	101 of 142	
Reference:	D6.3	Dissemination:	PU	
	Version:	1.0	Status:	Final

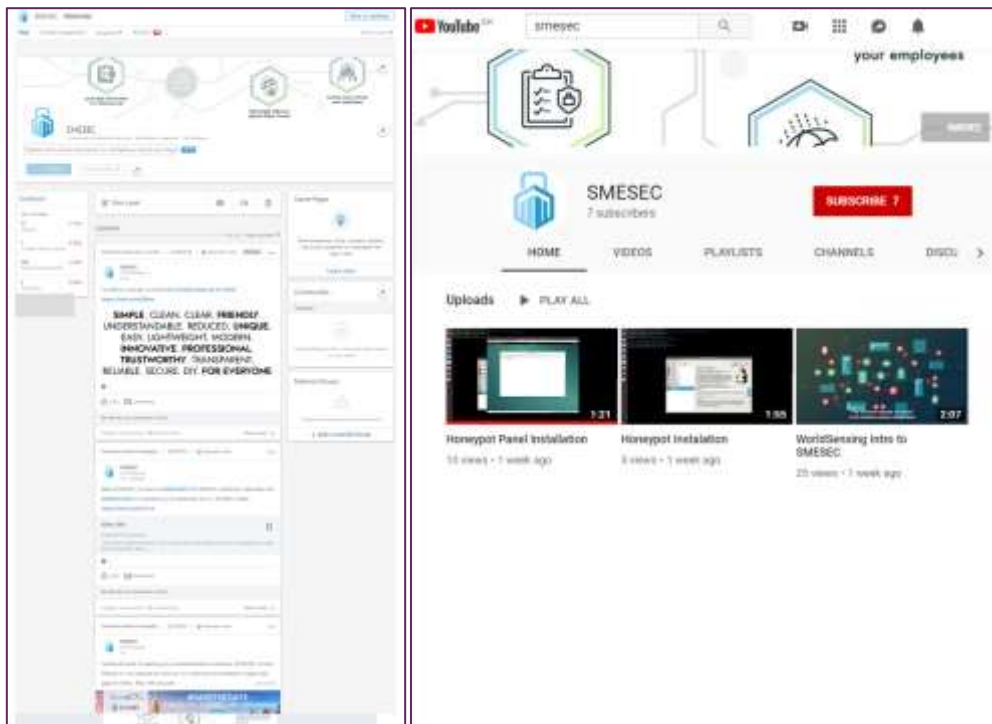


Figure 24: Snapshots of the SMESEC presence on social channels

The following table shows examples of follower categories:

EU Projects	Cybersecurity Experts	IT Professionals
 <p>SOFIE @EU_Sofie The SOFIE project aims to develop a blockchain driven federated platform for enabling information exchange of different IoTs and data silos.</p>	 <p>Marnix Dekker @marnixdekker I work for ENISA, the EU Cybersecurity agency, PhD in Computer security and MSc in Quantum physics. Tweets are personal views.</p>	 <p>John Rotimi Ade @Rotimi_1Adedeji Dad husband #IT Advisory & #Consulting #Change Agent #XaaS #Research #Blockchain #SDGs #GPU #Africa #SDN #HPC #AI #CTO ...</p>
Consortium Member Organizations	European Institutions	SME associations

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	102 of 142	
Reference:	D6.3	Dissemination:	PU	
	Version:	1.0	Status:	Final



At the time of writing, 5 organisations with an SME ecosystem were following the SMESEC Twitter channel: the European Digital SME Alliance, the Employers Group of the EESC, satw, and OPP EU Digital, and EBC.

Also, 10 SMEs followed the Twitter channel:

- The SMESEC use case SMEs Scytl, Worldsensing
- The SMESEC partner SME Easy Global Market
- The third-party SMEs Digiotech, ITML, BiOceanOr, SwitchboardFREE, Medianova, and Geonardo

The following figure shows the sizes of the organisations following the SMESEC LinkedIn channel. In total, we observe 15 SMEs and 3 micro enterprises.

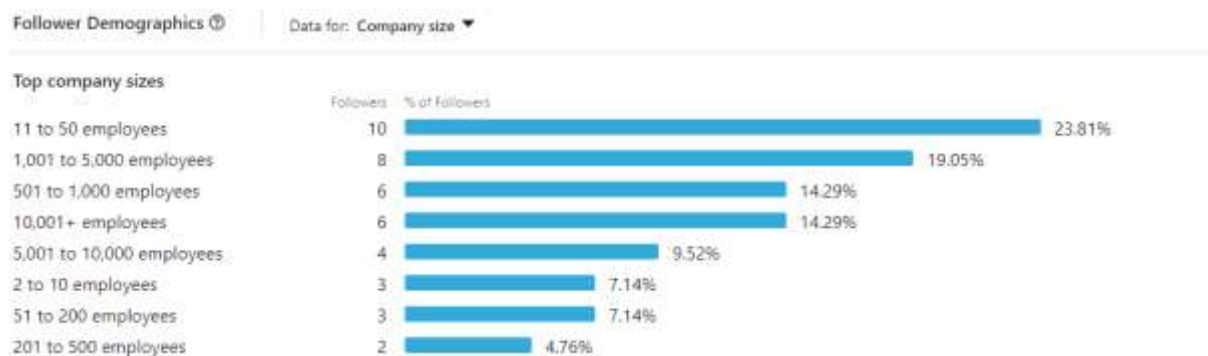


Figure 25: Demography of Linked-In Followers – company sizes.

3.4.4 Publications

Table 17 summarizes the scientific results produced by the SMESEC consortium members.

Table 17: Publications during the year 2.

Type	Title	Authors	Partner	Venue
Conference Proceedings	Please Forget Where I Was Last Summer: The Privacy Risks of Public Location (Meta)Data.	Kostas Drakonakis, Panagiotis Iliia, Sotiris Ioannidis, Jason Polakis	FORTH	NDSS 2019, San Diego, CA, USA

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	103 of 142				
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

Type	Title	Authors	Partner	Venue
Conference Proceedings	REAPER: Real-time App Analysis for Augmenting the Android Permission System	Michalis Diamantaris, Elias P. Papadopoulos, Evangelos P. Markatos, Sotiris Ioannidis, Jason Polakis	FORTH	(CODASPY), 2019, Dallas, TX, USA
Conference Proceedings	Master of Web Puppets: Abusing Web Browsers for Persistent and Stealthy Computation	Panagiotis Papadopoulos, Giorgos Vasiliadis, Panagiotis Iliia, Sotiris Ioannidis, Michalis Polychronakis, Evangelos P. Markatos.	FORTH	NDSS 2019, San Diego, CA, USA
Conference Proceedings	Assessing and Improving Cybersecurity Maturity for SMEs: Standardization aspects.	Yigit Ozkan,B., Spruit,M.	UU	1st SMESEC Workshop, September, 2018
Conference Proceedings	Deep Ahead-of-Threat Virtual Patching.	Fady Copty, Andre Kassis, Sharon Keidar-Barner, Dov Murik	IBM	Springer, Cham, September, 2018
Conference Proceedings	A Questionnaire Model for Cybersecurity Maturity Assessment for Critical Infrastructures	Yigit Ozkan,B., Spruit,M.	UU	1st International Workshop, IOsec 2018, CIPSEC Project. September, Heraklion, Crete, Greece
Conference Proceedings	A Framework for Threats Analysis Using Software-Defined Networking.	Francisco Moldovan, Ciprian Opreša.	Bitdefender	(ICCP). IEEE, September, 2018
Magasine	SMESEC: A Cybersecurity framework to Protect,	Jose Francisco Ruiz, Fady	Atos, IBM, Citrix	ERCIM News online edition, July 2018,

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	104 of 142		
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

Type	Title	Authors	Partner	Venue
	Enhance and Educate SMEs.	Copty, Christos Tselios		
Conference	End Node Security and Trust vulnerabilities in the Smart City Infrastructure.	Apostolos P. Fournaris, Konstantinos Lampropoulos, Odysseas Koufopavlou.	UOP	(ICEAF V), June 2018, Chios Island, Greece
Poster	A Large-scale Analysis of Content Modification by Open HTTP Proxies.	Giorgos Tsirantonakis, Panagiotis Ilia, Sotiris Ioannidis, Elias Athanasopoulos, Michalis Polychronakis	FORTH	Cybersecurity and Privacy (CySeP), June 2018, Stockholm, Sweden

3.4.5 SMESEC Workshop

1st SMESEC Workshop, September 14, 2018



The first SMESEC workshop co-located with the 21st International Symposium on Research in Attack, Intrusions, and Defenses (RAID) hosted in Crete, Greece, 14 September 2018. This workshop organized by the Foundation for Research and Technology - Hellas (FORTH) and it provided the possibility for the SMESEC partners to present their advancements in two technical and non-technical parts.

Although Small and Medium-sized Enterprises (SMEs) have a significant role in European businesses, they are not capable enough of safeguarding themselves against cyber-attacks. SMESEC aims to be a holistic security framework to offer a variety of solution, tools, and training content to SMEs.

More information: <https://www.raid2018.org/smesecworkshop.html>

3.4.6 KPI

The second year of dissemination has focused on providing information about SMESEC activities and outcomes, providing information about the SMESEC framework, and winning participants for the open call. Accordingly, SMESEC has spread information to the target groups about the components of the SMESEC framework as soon as they were available and performed campaigns for making the open call visible to solicit submissions. The third year will focus on disseminating results using the SMESEC framework and enable future exploitation.

The following tables report the objectives and progress of fulfilling for the various dissemination-related KPI for the year 2. The tables state averages if not indicated otherwise.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	105 of 142		
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

Table 18: Visibility monitoring and related objectives.

Channel	Indicators	Objectives Y2	Fulfilment Y2	Objectives Project End
Website	Downloads per year	500	3125	1000
	Unique visitors per month	500	Monthly Average: 3720	1000
	Visits per month	2000	Monthly Average: 5473	4000
	Website news per month	0.5	Monthly Average: 3.1	1.0
Social networks	Social networks posts per month	10	9.4	30
	Twitter followers	125	M24: 237	250*
	Facebook followers	50	M24: 29	100*
	LinkedIn followers	50	M24: 56	100*
	YouTube followers	0	7	30*
Publications / Communication materials / Contributions	Press releases	2	2	4
	Newsletters per quarter	1	0	1
Events	Attended events	33	30	50
	Webinars	2	1	3
	Tutorials	2	0	3

The numbers associated with a “*” were added to manage the dissemination work. No corresponding KPIs were stated in the DoA.

The following table describes the evolution of the social network followers for the year 2 in detail. YouTube was added in May 2019, thus the low number of followers on that channel.

Table 19: Social network followers by month (*: no final figure available at the time of writing).

Network	Jun 2018	Jul 2018	Aug 2018	Sep 2018	Oct 2018	Nov 2018	Dec 2018	Jan 2019	Feb 2019	Mar 2019	Apr 2019	May 2019
Twitter	76	100	120	153	163	174	185	193	205	217	234	237
Facebook	11	11	11	16	16	16	16	19	23	26	29	29
Linked-in	11	14	17	21	23	26	29	35	39	43	54	56

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)				Page:	106 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

YouTube	-	-	-	-	-	-	-	-	-	-	-	7
---------	---	---	---	---	---	---	---	---	---	---	---	---

The following table describes the scientific impact-related KPIs for the year 2.

Table 20: Scientific impact monitoring and related objectives (*: see comment below)

Channel	Indicators	Objectives Y2	Fulfilment Y2	Objectives Project End
Publications / Communication materials / Contributions	Contributions to roadmaps	0	0	2
	Contributions to standards	0	0	2
	Contributions to policy	0	0	2
	Journal Publications	5	1	8
	Conference Talks	13	13	20
Workshops	Number of workshops	1	1	2
Website	Open call registrations	20	12	20
	Registered members (SMESEC framework users)	10	39	10*

The numbers associated with a “*” have been corrected in comparison to the previous deliverable D6.2. They here stated objectives reflect the KPI stated in the DoA.

3.5 Conclusions

In the second year, the SMESEC dissemination aimed at documenting and spreading information about the SMESEC framework. The aim was achieved with several steps. First, significant interaction was performed in workshops and bilateral discussions with the consortium members to understand the capabilities, scope, and value proposition of their tools to be integrated in the framework. Second, many meetings with SMEs were performed in conjunction with SME events, fairs, and webinars that were enabled by the SME associations that SMESEC contacted for cooperation. Third, the SMESEC dissemination material was updated to document the resulting understanding of the SMESEC framework and communicate its attractive value proposition to SMEs and stakeholders.

In the second year, the SMESEC dissemination also aimed at supporting the open call with a suitable campaign. The aim was achieved with directed Twitter and Facebook campaigns, leveraging the dissemination results achieved until M20, and by coordinating the SMESEC partners’ activities for mobilising open call applications.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	107 of 142		
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

SMESEC dissemination also maintained and update the public Web portal, the blog of SMESEC news and events, posting on social media, and to encourage the publication in technical conferences and specialised journals and magazines. Also, the first SMESEC workshop was performed.

During the dissemination work, several observations were made, and lessons were learned. Only few SMEs followed the SMESEC dissemination, the criticality of a sharp SMESEC framework value proposition to raise desire of knowing more about SMESEC, and the still substantial effort to win one SME's interest in trying and use SMESEC. These observations and lessons will be the focal points of the SMESEC dissemination work of the year three.

The third year of SMESEC will aim at enabling the future SMESEC exploitation. Particular themes will be a) awareness workshops and webinars in collaboration with WP3, b) dissemination of the SMESEC value proposition, c) tutorials of how to use SMESEC, and d) testimonials of SMESEC users about the experience and impact generated by SMESEC in the SME. These dissemination activities will be enabled by the full portfolio of actions as described in the DoA and the introduction to this section, as well as in accordance with the security awareness roadmap and its implementation in WP3. The impact will be evaluated with the KPIs presented in the section 3.4.6, in particular the number of members registered for accessing in-depth information about the SMESEC framework and receiving newsletters with updates.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	108 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

4 Standardization Activities

During the second year of the project, we focused our standardisation efforts on two main activities. These activities are shown in Figure 26.

In Activity A, we focused on collaborating with European Standardisation Bodies. In Activity B, we focused on studying existing cybersecurity standards for enhancing SMESEC.

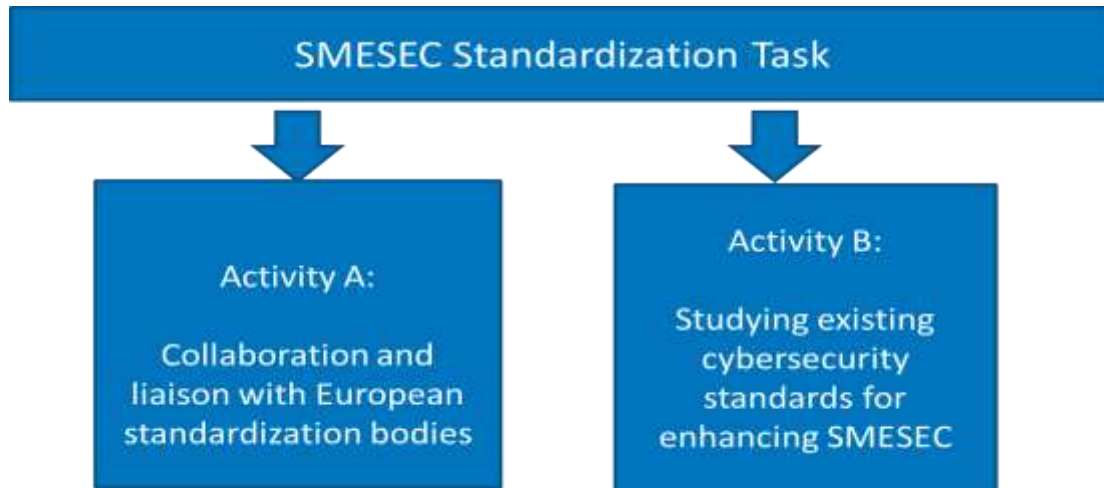


Figure 26: Two main activities for the standardisation task

The following chapters present the work done for these activities. The initial version of the standardisation plan was presented first in the D6.1 Dissemination Plan and Market Analysis document. To reflect the developments and changes, then an updated version of this plan was presented in the D6.2 annual report on exploitation, dissemination and standardization document. Here in Figure 27, we present our revised standardisation plan includes the developments in the second year of the project.

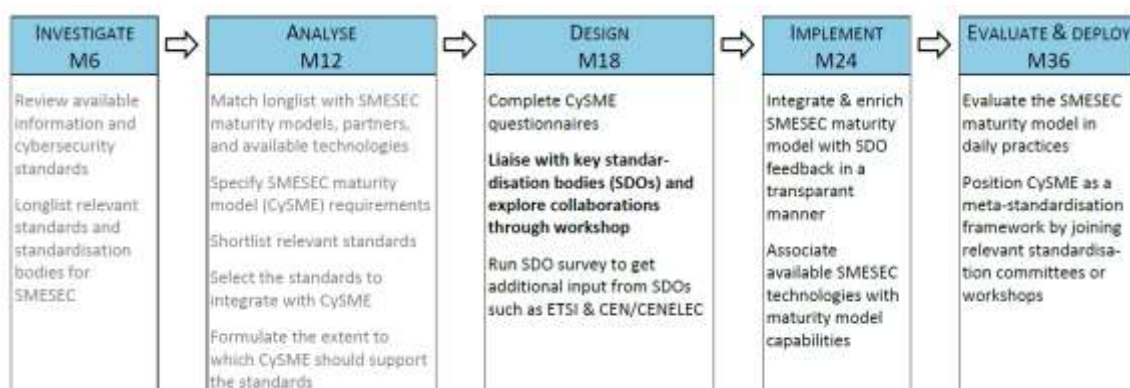


Figure 27: Revised standardisation plan

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	109 of 142	
Reference:	D6.3	Dissemination:	PU	
	Version:	1.0	Status:	Final

The activities listed in this plan are organized according to the timeline of the project. In the following section the work that has been done for these activities are grouped by the two main activities that was mentioned above to improve understandability.

4.1 Collaboration and Liaison with European Standardization Bodies

Following a top-down approach to identify any standardisation gaps SMESEC could contribute, we have followed the process depicted in Figure 28.

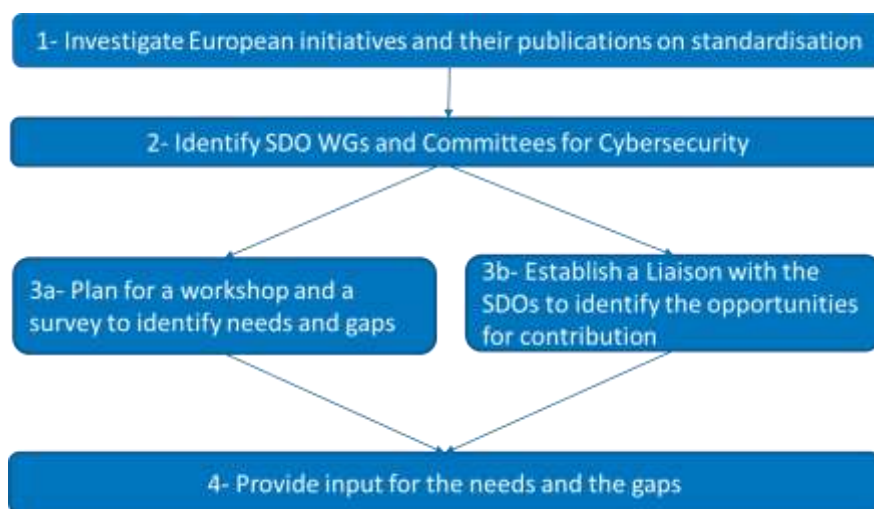


Figure 28: Top-Down Approach Activities

An important accomplishment during the second year of the project was being able to get in touch with the key European standardisation bodies CEN, CENELEC and ETSI. Our first contact was during a conference organised by ENISA, CEN, CENELEC and ETSI. The details for this conference are given below:

Conference “*Cybersecurity Standardization and the Cybersecurity Act: Where are we today?*”
21 January 2019, Brussels

During this conference, the WP6 leader and the standardisation task leader made contacts with the representatives of the standardisation bodies and gave them brief information about the SMESEC project and the standardisation task.

4.1.1 Investigating European Initiatives and Their Publications on Standardization

During the second year, we investigated the European initiatives and their publications on standardisation. We have investigated the standardisation bodies, SME associations and cybersecurity related organisations.

In European level, the standardisation bodies are the following:

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	110 of 142	
Reference:	D6.3	Dissemination:	PU	
	Version:	1.0	Status:	Final

- CEN (European Committee for Standardization)

<https://www.cen.eu/Pages/default.aspx>

- CENELEC (European Committee for Electrotechnical Standardization)

<https://www.cenelec.eu/>

- ETSI (European Telecommunications Standards Institute)

<https://www.etsi.org/>

We have identified the following SME associations:

- European Digital SME Alliance

The European Digital SME Alliance is the largest network of the ICT small and medium sized enterprises in Europe, representing about 20.000 digital SMEs across the EU.

<https://www.digitalsme.eu/>

- Small Business Standards (SBS)

SBS is a European non-profit association co-financed by the European Commission and EFTA Member States. The aim for SBS is to represent and defend SMEs' interests in the standardisation process at European and international levels. They are raising the awareness of SMEs about the benefits of standards and encouraging them to get involved in the standardisation process. SBS works in collaboration with Digital SME Alliance.

<https://www.sbs-sme.eu/>

An important publication of SBS with Digital SME alliance "WG27K" working group is an SME Guide for the implementation of ISO/IEC 27001 on information security management.

We have identified the following cybersecurity related organisations:

- ENISA The European Union Agency for Network and Information Security

The European Union Agency for Network and Information Security (ENISA) is a centre of expertise for cyber security in Europe.

<https://www.enisa.europa.eu/>

ENISA has the following publications related to cybersecurity and SMEs:

- ENISA Network and Information Security Directive
- ENISA Threat Taxonomy
- A simplified approach to Risk Management for SMEs
- Security guide and online tool for SMEs when going Cloud

- European Cyber Security Organisation (ECSO)

ECSO is a fully self-financed non-for-profit organization. ECSO's objective is to support all types of initiatives or projects that aim to develop, promote, and encourage European cybersecurity.

<https://ecs-org.eu/>

ECSO has published State of the Art Syllabus v2 in December 2017, which presents an overview of existing Cybersecurity standards and certification schemes. This document lists standards and

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	111 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

specifications (International and EU) related to Cybersecurity. We have elaborated our findings using this document in the deliverable (D6.2).

Another publication of ECSO is European Cyber Security Certification meta-scheme. This meta-scheme allows combining existing schemes efficiently or to allow creation of new scheme when required.

Since there are any certification schemes in place, each having a different focus (product, systems, solutions, services, organizations ...) and many assessment methodologies (check-list, asset-based vulnerability assessment) this publication is important regarding cybersecurity.

- The Cyber Security Coalition

The Cyber Security Coalition is a unique partnership between players from the academic world, the public authorities and the private sector to join forces in the fight against cybercrime. The Cyber Security Coalition currently have more than 50 key players.

<https://www.cybersecuritycoalition.be/>

The Cyber Security Coalition has published the following regarding cybersecurity and SMEs:

- [Cybersecurity guide for SMEs](#)
- [Cyber Security KIT](#)

European Commission released the 2019 Rolling plan on ICT Standardisation, which identifies ICT standardisation activities in support of EU policies in March. The document can be accessed through this link:

https://ec.europa.eu/growth/content/2019-rolling-plan-ict-standardisation-released_en

In this rolling plan, cybersecurity is referred as a priority area for standardization.

4.1.2 Identifying WGs and Committees for Cybersecurity and SMEs

The European standardisation bodies and organisations have specific workgroups and committees that are related to SMESEC.

- ETSI Technical Committee Cyber

TC CYBER is recognized as a major trusted centre of expertise offering market-driven cyber security standardization solutions, advice and guidance to users, manufacturers, network, infrastructure and service operators and regulators. ETSI TC CYBER works closely with stakeholders to develop standards that increase privacy and security for organizations and citizens across Europe and worldwide.

<https://www.etsi.org/technologies-clusters/technologies/cyber-security>

- CEN_CENELEC Focus Group on Cybersecurity

The Focus Group on Cybersecurity (CSCG) will support CEN and CENELEC to explore ways and means for supporting the growth of the Digital Single market. To this end, the CSCG will analyse technology developments and develop a set of recommendations to its parent bodies for international standards setting ensuring a proper level playing field for businesses and public authorities.

<https://www.cencenelec.eu/standards/sectors/defencesecurityprivacy/security/pages/cybersecurity.aspx>

- CEN/CLC/Joint Technical Committee 13 - Cybersecurity and Data Protection

https://standards.cen.eu/dyn/www/f?p=204:7:0::::FSP_ORG_ID:2307986&cs=1E7D8757573B5975E D287A29293A34D6B

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	112 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

The scope of this joint technical committee is defined as follows: Development of standards for cybersecurity and data protection covering all aspects of the evolving information society.

- ECSO WG1: Standardisation, certification, labelling and supply chain management

<https://ecs-org.eu/working-groups/wg1-standardisation-certification-labelling-and-supply-chain-management>

The working group addresses the following issues:

- EU ICT security certification framework
 - Standards for interoperability
 - EU cybersecurity labelling
 - Increased digital autonomy
 - Testing and validation of the supply / value chain in Europe
- ECSO WG4: Support to SMEs, coordination with countries (in particular East and Central EU) and regions

<https://ecs-org.eu/working-groups/wg4-support-to-smes-coordination-with-countries-and-regions>

The working group focuses on the following issues:

- Support the development of SMEs, start-ups and high growth companies
- Develop coordinated activities between clusters (both business oriented and triple helix), Regions and local bodies (for local implementation of solutions / educations)
- Development of East and Central EU public and private sectors dealing with cybersecurity.

4.1.3 Cybersecurity Standards Workshop and a Survey to Identify Needs and Gaps

Following a top-down approach, we planned to organise a workshop on “Cybersecurity standardisation for SMEs”. Our aim for organising this workshop was to identify any gaps on cybersecurity standardisation for SMEs that SMESEC can contribute.

We organised several tele conference meetings with related parties. As a result of these meetings we had the following parties’ confirmation on organising this workshop collaboratively.

CENCENELEC JTC13, ETSI TC CYBER, ECSO, Digital SME Alliance and the StandICT project.

The parties involved in the workshop are discussed in the previous section. Here, we provide information on StandICT project. StandICT.eu, “Supporting European Experts Presence in International Standardisation Activities in ICT”, addresses the need for ICT Standardisation and defines a pragmatic approach and streamlined process to reinforce EU expert presence in the international ICT standardisation scene. The workshop was announced with the following banner in Figure 29.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	113 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final



Figure 29: Cybersecurity Standardisation Workshop

The workshop is planned to be held at CEN CENELEC headquarters Brussels, Belgium, Date 24th May 2019, between 10:00 – 16:00. The details and the agenda for the workshop is as follows:

Purpose & Scope

We know that within the cybersecurity supply industry, a very substantial part of innovation is driven by SMEs & start-ups. The European Commission has been working on fostering European cybersecurity industry and supporting specifically SMEs towards that direction all along the cybersecurity policy and regulatory initiatives. In that context standardisation is ensuring further cybersecurity which is more at stake with new innovations (e.g.: with use of IoT).

Many reports confirmed that SMEs are more exposed to cybersecurity attacks (eg: Cisco report[1] 53% of small companies who have experienced a breach). To help protect better SMEs on cybersecurity issues, projects such as SMESEC are preparing a framework of solutions for SMEs but SMEs could be already better protected if they follow clear rules as described in cybersecurity standards.

Therefore, two H2020 funded projects SMESEC[2] & StandICT.eu[3] are coming together on a one-day workshop to support the “SME in his/her Cybersecurity ensured by standards” – this is why the workshop is kindly being hosted by CEN & CENELEC with the participation of Cen-Cenelec /TC 13 on cybersecurity, the ETSI TC Cyber, the Digital SME Alliance and the European Cybersecurity Organization (ECSO).

Who should attend?

Innovators, ICT SMEs, SMEs associations, policy makers and funding agencies looking to assess future priorities and challenges in cybersecurity brought by standards and identifying gaps in standardization efforts, Public administrations, larger organisations.

Main Take-aways for the audience

Learn from those Standardization organisations delivering cybersecurity standards which could be important & relevant for SMES;

- *Learn from those Standardization organisations delivering cybersecurity standards which could be important & relevant for SMES;*
- Hear form testimonials who are working on gaps in cybersecurity standardization;
- Contribute to provide SME’s voice on reporting cybersecurity needs in particular which can be supported by standardization;
- Grab the opportunity to apply for an open call currently open in both SMESEC and StandICT.eu Open Call Opportunities;

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	114 of 142
Reference:	D6.3	Dissemination:	PU
	Version:	1.0	Status: Final

- *Gain a whole new understanding of why Cybersecurity is important and should become your priority & how it can be affordable for SMEs;*
- *Become part of our cybersecurity community.*

Agenda Structure- Cybersecurity standards: what impacts and gaps for SMEs?

09:00-09:30 Registration

09:30 -10:00 Networking Coffee

10:00 10:15 – Welcome by the hosts **CEN CENELEC** & a brief intro of who is **SMESEC** by **Philippe COUSIN & StandICT.eu** by **Silvana MUSCELLA**

10:15 – 10:30 – Keynote address by **EC representative** on expectations & future vision in cybersecurity under H2020 & under Horizon Europe - Florent Frederix

10:30 – 11:30 Setting the scene of cybersecurity standardisation impacting SMEs with Key representatives from the Standards Bodies & Organisations on achievements to date & future challenges (Resp from: CEN-CENELEC, ETSI, ECSO).

- 10:30-10:50 Jean Pierre QUEMARD CENCENELEC TC 13
- 10:50-11:10 Jasper Pandza ETSI TC CYBER
- 11:10 – 11:30 Roberto Cascella ECSO Standardisation WG

11:30 – 12:00 Networking Coffee

The panel will open with a brief intro of SMESEC & StandICT.eu but then there will be pitches from SME cybersecurity testimonials or from successful applicants from

12:00- 13:00 - Second Panel Discussion offering a “**A voice to the SMEs**”

- 12:00 -12:15 Mrs Silvana Muscella, H2020 StandICT project
- 12:15 -12:30 Philippe Cousin H2020 SMESEC project
- 12:30 -12:45 Danilo D’Elia ECSO SME Working group
- 12:45-13:00 Q&A

13:00-14:00 Networking Lunch

14:00 15:30 Second panel intervention for **A voice from the SMEs” & an opportunity to report on** cybersecurity standards best practices, gaps and needs.

ECSO SMEs working group, SBS and Digital SMEs Alliance will report on SMEs needs for standardization. SMEs and National SMEs organisations are welcome to present their views. Projects such as the cyberwatching.eu catalogue & marketplace will be invited to attend the event.

- 14:00-14:20 Sebastiano Toffaletti, Secretary General, Digital SMEs alliance
- 14:20-14:40 George Sharkov, Small Business Standards, European Software Institute
- 14:40-14:55 Dr. Stephen Farrell, Research Fellow at Trinity College Dublin (Faculty Computer Science & Statistics) improving security and privacy for people using the Internet
- 14:55-15:10 Javier Tallon, COO and Co-founder at Jtsec Beyond IT security
- 15:10-15:25 Mrs Jacqueline Zoest, Advisor & Consultant at Campbell Millar "Privacy by design for Consumer Goods & Services"

15:30 – 15:45 Q&A & Close

^[1]2018 Cisco Cybersecurity Report: Special Edition SMB <https://www.cisco.com/c/dam/en/us/.../small-mighty-threat.pdf>

^[2] www.smesec.eu This project has received funding from the European Union’s Horizon 2020 R&I programme GA 740787 (SMESEC)

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	115 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

^[3]StandICT.eu has received funding the European Union’s Horizon 2020 research & innovation Programme under GA 7804391

[WD1]Constant

4.1.4 Establishing Liaisons with the SDOs to Identify the Opportunities for Contribution

The interactions with the SDOs is now considered as an ongoing activity for the SMESEC project. We are also investigating the opportunities for establishing formal liaisons with the SDOs.

4.1.5 Providing Input for the Needs and the Gaps

The workshop results and findings will be presented in a report that will be coordinated by the SMESEC project. SMESEC and StandICT projects are planning to organise a webinar to present the results to the related parties. This webinar will be organised probably in October or November 2019.

4.2 Studying Existing Cybersecurity Standards for Enhancing SMESEC

We have followed a bottom-up approach in order to investigate the existing cybersecurity standards for enhancing SMESEC and identify any gaps that SMESEC could contribute. In this section, we present the process we have followed for these activities. The process is depicted in Figure 30.

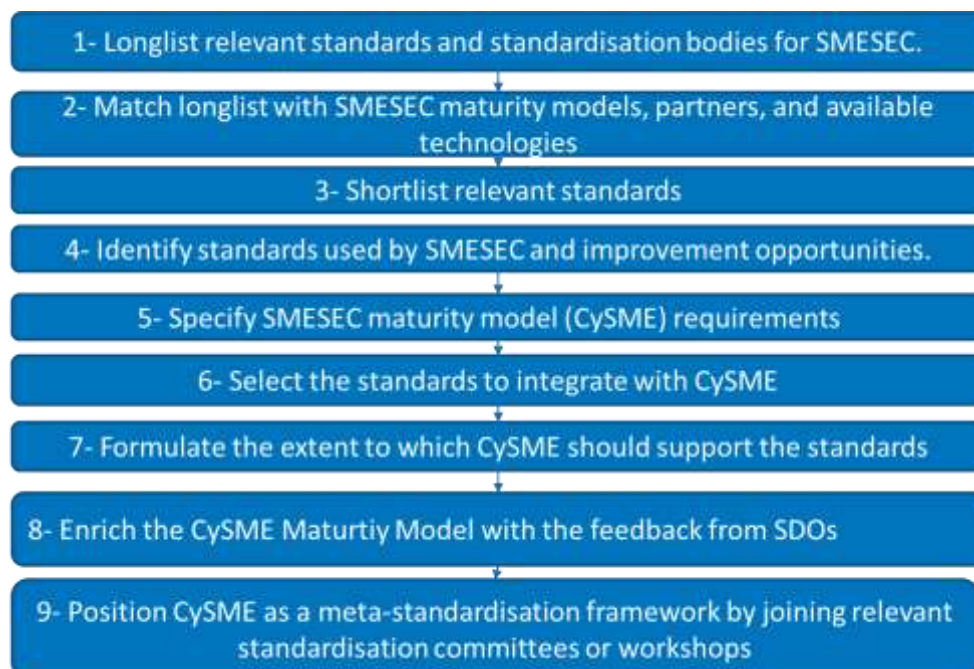


Figure 30: Bottom-up Approach Activities

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	116 of 142
Reference:	D6.3	Dissemination:	PU
	Version:	1.0	Status: Final

The findings for the first two activities were reported in previously submitted deliverables D6.1 and D6.2. Here, we present a summary regarding these results and elaborate more on the following activities. The list of relevant standardisation bodies and organisations for SMESEC are listed in Table 21.

Table 21: Relevant standardisation bodies/organisations for SMESEC

Committee/ Organisation Acronym	Committee/Organisation Name
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
ETSI	The European Telecommunications Standards Institute
oneM2M	Standards for M2M and the Internet of Things
NIS	Network and Information Security Directive
ISF	Standard of Good Practice of the Information Security Forum
ITU	International Telecommunication Union
OMA	Open Mobile Alliance
OASC	Open & Agile Smart Cities
IETF	The Internet Engineering Task Force
W3C	The World Wide Web Consortium
IEEE-SA	The Institute of Electrical and Electronics Engineers Standards Association
FIRST	Forum Of Incident Response and security Teams
MISP Community	Malware Information Sharing Platform Community
OASIS	The Organization for the Advancement of Structured Information Standards (OASIS)
LoRa Alliance	The Long Range Alliance

After having the related standardisation organisations, we investigated the list of possible standards related to SMESEC tools. The findings are presented in Table 22.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	117 of 142		
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

Table 22: Longlist of Possible Standards related to SMESEC Tools

SMESEC Tool	Possible Related Standard
ATOS XL-SIEM - Security Information and Event Management System	ETSI GS ISI 002 V1.2.1 (2015-11) A security event classification model and taxonomy (Group Specification)
	ETSI GS ISI 005 V1.1.1 (2015-11) Information Security Indicators (ISI); Guidelines for security event detection testing and assessment of detection effectiveness
	ETSI GS ISI 004 V1.1.1 (2013-12) Information Security Indicators (ISI); Guidelines for event detection implementation
	ISO/IEC 27043:2015(en) Information technology — Security techniques — Incident investigation principles and processes
	FIRST - Information Exchange Policy (IEP)
Bitdefender GravityZone - Protection against malware.	European Commission Information System Security Policy C(2006) 3602 STANDARD ON CONTROLS AGAINST MALICIOUS CODE
	FIRST - Common Vulnerability Scoring System SIG
Citrix NetScaler - AppFirewall, Unified Gateway, SWG	ISO/IEC 27033-4:2014 Information technology -- Security techniques -- Network security -- Part 4: Securing communications between networks using security gateways
	ICISA Labs Web Application Firewall Certification Criteria
EGM TaaS solution - Security Testing	ETSI TR 101 583 V1.1.1 (2015-03) Methods for Testing and Specification (MTS); Security Testing; Basic Terminology
	ETSI EG 203 251 V1.1.1 (2016-01) Methods for Testing & Specification; Risk-based Security Assessment and Testing Methodologies

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	118 of 142				
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

	Automated Source Code Security Measure™ (ASCSMTM) V1.0
	2011 CWE/SANS Top 25 Most Dangerous Software Errors
	FIRST - Common Vulnerability Scoring System
	ICSA Labs IoT Security Testing Framework
FORTH / Early Warning Intrusion Detection System	ETSI GS ISI 004 V1.1.1 (2013-12) Information Security Indicators (ISI); Guidelines for event detection implementation
	Common Attack Pattern Enumeration and Classification (CAPEC™)
	ETSI GS ISI 003 V1.2.1 (2018-01) Information Security Indicators (ISI); Key Performance Security Indicators (KPSI) to evaluate the maturity of security event detection
	ETSI GS ISI 005 V1.1.1 (2015-11) Information Security Indicators (ISI); Guidelines for security event detection testing and assessment of detection effectiveness
	FIRST - Common Vulnerability Scoring System
IBM AngelEye - Virtual patching	ETSI TR 101 583 V1.1.1 (2015-03) Methods for Testing and Specification (MTS); Security Testing; Basic Terminology
	ETSI EG 203 251 V1.1.1 (2016-01) Methods for Testing & Specification; Risk-based Security Assessment and Testing Methodologies
	Automated Source Code Security Measure™ (ASCSMTM) V1.0
	2011 CWE/SANS Top 25 Most Dangerous Software Errors
IBM Anti-ROP	Evaluating the Effectiveness of Current Anti-ROP Defenses
	Defending against Return-Oriented Programming

After this general investigation regarding the related standardisation organisations and standards, we evaluated our findings with the SMESEC partners who develop the tools for the SMESEC framework.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	119 of 142	
Reference:	D6.3	Dissemination:	PU	
	Version:	1.0	Status:	Final

We have conducted semi-structured interviews for this purpose. We've prepared an interview protocol which is given below in Figure 31.

Semi-Structured Interview for Understanding the Level of Adherence to Standards in SMESEC Cybersecurity Tools

General Information

This questionnaire is prepared by Bilge Yigit Ozkan and Marco Spruit at UU. It is part of the work for the Standardization Task (6.3) in the SMESEC Project.

Research Question

What are the maturity levels of partners' tools regarding adherence to industry standards in their area?

Interview Purpose:

The purpose of this interview is to understand the current level of adherence/support of related standards that the SMESEC tools provide.

Background Questions:

What is your job title?

Your Answer:

What are your main responsibilities in the company?

Your Answer:

How long have you been working in the company?

Your Answer:

Section 1: Understanding the Field and Current Level of Adherence to Standards

What is your company's cybersecurity tool's field of application?

Your Answer:

Which standards/recommendations/guidelines relevant to your tools' field of study are you/your company aware of? Does your tool adhere to any of these standards/recommendations/guidelines? If so, which ones? Please answer by filling in the table.

Your Answer:

Standards/recommendations/guidelines	Status of Implementation/adherence	Comments

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	120 of 142
Reference:	D6.3	Dissemination:	PU
	Version:	1.0	Status:
			Final

Section 2: Understanding the level of agreement with UU findings and willingness to adhere.

Please find standards/recommendations/guidelines identified for ATOS XL-SIEM - Security Information and Event Management system by UU.

Which of the standards/recommendations/guidelines that are identified by UU were you aware of?

Which of these standards/recommendations/guidelines do you consider to be relevant to adhere to in your tool and you are willing to adhere? Please answer by filling in the table.

Your Answer:

Standard/ Recommendation/ Guideline	Were you aware of? (yes/no)	Is it relevant? (yes/no)	Are you willing to adhere? (yes/no)	Comments
<standards related to the tool are listed here>				

Closing

Thank you for your time.

These are all the questions we have for you. Is there anything else you would like to add?

Figure 31: Semi-structured Interview Protocol

4.2.1 Shortlist Relevant Standardisation Bodies/Organisations for SMESEC

The interviews were held with the representatives of the partners. Using the information provided by the partners, we have prepared a shortlist of standardisation bodies and organisations related to SMESEC in the point of view of the partners. Table 23 presents the related technology, corresponding SMESEC tool and the related standardisation organisation or the community that was identified.

Table 23: Relevant Standardisation bodies/organisations for SMESEC (after the interviews)

Area/ Technology	SMESEC Tool	Standardisation Organisation/ Community
Governance, Risk Management and Compliance	FHNW CYSEC	ISO
Security Information and Event Management	ATOS XL-SIEM	OASIS

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	121 of 142	
Reference:	D6.3	Dissemination:	PU	
	Version:	1.0	Status:	Final

Unified Threat Management	The unified SMESEC Framework	MISP Community
Secure Web Gateways (SWG)	Bitdefender GravityZone	FIRST
Endpoint Protection Platforms	Bitdefender GravityZone	FIRST
Application Security Testing	EGM TaaS	OneM2M, LoRa Alliance, FIRST
Endpoint Detection and Response	Bitdefender GravityZone	FIRST

4.2.2 List of Standards Used by SMESEC Tools

In addition to the related standardisation organisation or the community, the standards that are used by the tools were also identified during the interviews. Table 24 presents the list of standards used by the SMESEC tools that are identified.

Table 24: List of Standards used by SMESEC Tools

Area/ Technology	SMESEC Tool	Related Standards
Governance, Risk Management and Compliance	FHNW CYSEC	ISO 27002
Security Information and Event Management	ATOS XL-SIEM	TAXII, STIX
Unified Threat Management	The unified SMESEC Framework	MISP
Secure Web Gateways (SWG)	Bitdefender GravityZone	FIRST Common Vulnerability Scoring System
Endpoint Protection Platforms	Bitdefender GravityZone	FIRST Common Vulnerability Scoring System
Application Security Testing	EGM TaaS	OneM2M standards, LoRa security, FIRST Common

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	122 of 142	
Reference:	D6.3	Dissemination:	PU	
	Version:	1.0	Status:	Final

		Vulnerability System	Scoring
Endpoint Detection and Response	Bitdefender GravityZone	FIRST Vulnerability System	Common Scoring

4.2.3 Identified Opportunities to Contribute Standardisation

4.2.3.1 Opportunity 1:

During the interviews we asked the SMESEC partners for any opportunities they see to improve the standards that they use for their tools. There is one opportunity that was identified this way.

The unified SMESEC framework is using MISP (Malware Information Sharing Platform) as a standard for alert communications. The information regarding this platform is available through the following website. MISP data models – MISP core format, MISP taxonomies, <https://www.misp-project.org/datamodels>.

According to the experts utilising this standard there could be some missing alerts like training alerts, user behaviour alerts, and security management alerts. Adding these types of alerts can enable providing a great added value for SMESEC towards creating a solid differentiation from similar products in the market.

4.2.3.2 Opportunity 2:

The other opportunity that was identified to contribute to standardization is developing a procedure/model to connect different kinds of security products in one framework which is one of the activities accomplished in the SMESEC project. This opportunity was identified during an ETSI TC CYBER meeting in October 2018. University of Patras attended this meeting in regard to another project. During the meeting, this opportunity was identified as a result of the discussions.

4.2.4 CySME Maturity Model and Standardisation

Utrecht University is developing information security assessment models specifically adjusted to SMEs. During the last decade, UU has developed a family of information security assessment tools for SMEs (e.g. [16]; [17]). Most notably, the ISFAM and CYSFAM maturity models have been evaluated successfully in daily operations. The CYSFAM includes focus areas for application security, cyber-security and network-security, and a tentative relationship with internet-security. Therefore, it is now becoming possible to attempt to create one harmonized, modular and federative security focus area maturity model that enables a complete security quick-scan tailored to specific organizational characteristics.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	123 of 142		
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

For the development of the CySME maturity model we first developed a questionnaire model that can be used to facilitate the self-assessment and improvement requirements for the SMEs. The findings were presented in SMESEC and CIPSEC workshops in October 2018, Crete. Here we present how CySME will support standardization of the cybersecurity practices of the SMEs. Figure 32 presents general concepts regarding the CySME.

CySME has the following attributes:

- enables the assessment of cybersecurity capabilities,
- is situational aware (assessment questions are customized according to the characteristics of the SMEs)
- supports standardization (questions are derived from well-known, widely-applied industry standards, i.e. ISO 27k)
- incorporates good practices and tools for implementing the capabilities.



Figure 32: CySME Maturity Model

By the help of CySME, SMEs will be able to assess their cybersecurity maturity and by implementing the capabilities that are being assessed, they will be able to adhere to the underlying standards used in the maturity model.

4.2.4.1 CySME Cybersecurity Maturity Model Focus Areas

The following focus areas are used in the CySME maturity model. These focus areas were identified in the deliverable D2.3 Security Awareness Plan Report.

Table 25: CySME Cybersecurity Maturity Model Focus Areas

CySME Cybersecurity Maturity Model Focus Areas			
Fast Ramp-up			

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	124 of 142	
Reference:	D6.3	Dissemination:	PU	
	Version:	1.0	Status:	Final

Access Control and Audit
Code Inspection
Malware Scans
Patch Management
User Training
Capability Building
Absorption Networks
Application Change Management
Credential Management
Intrusion Prevention
Network Controls
Second Opinion Defence
Security Engineering
Standards and Compliance
Ability to Manage
Asset Management
Cybersecurity Coach
Security Baseline
SIEM
Vulnerability Scans
Ability to Manage(Medium Enterprises)
Budgeting and Funding
CIRT Team and Process
Governance

4.2.4.2 The Requirements for the CySME Maturity Model

The following requirements were identified for the CySME Maturity Model:

- Easy to use, self-assessment, do-it-yourself
- Situational awareness
- Standards-transparency

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	125 of 142				
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

- Provide cybersecurity awareness
- Maintainability by design

These requirements are elaborated in our paper presented during the 1st SMESEC workshop.

Yigit Ozkan,B., & Spruit,M. (2018). Assessing and Improving Cybersecurity Maturity for SMEs: Standardization aspects. *1st SMESEC Workshop*, September 14, 2018

4.2.4.3 Implementation of the CySME Maturity Model

CySME maturity model is currently being implemented by the CYSEC tool of FHNW. Figure 33 shows the main components of the CYSEC tool. In this figure, the part that is in red includes the CySME maturity model.

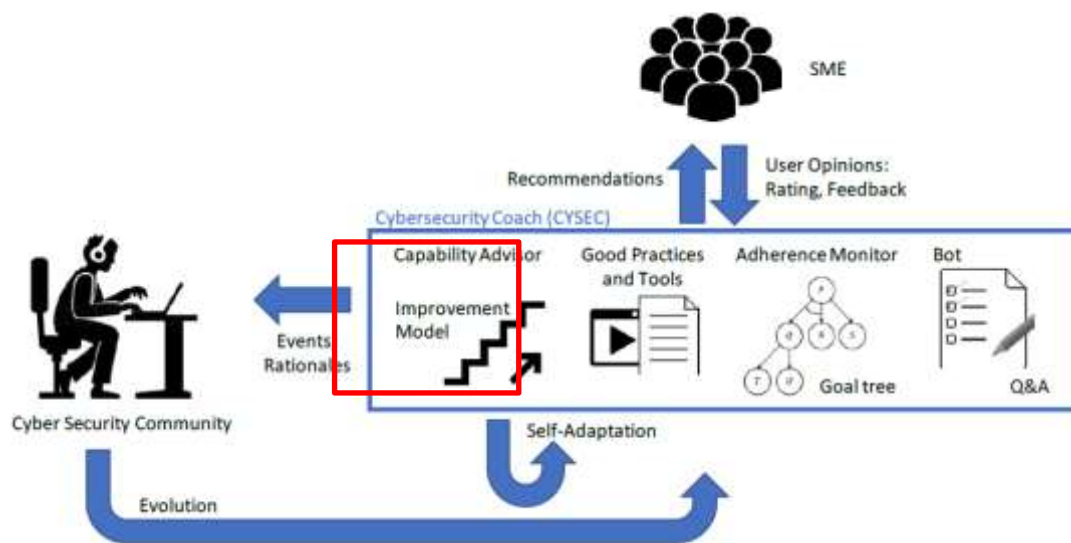


Figure 33: CYSEC Tool (from deliverable D 2.3)

The following list shows the contributions of the CySME maturity model to the CYSEC tool that is developed by FHNW.

- The capabilities and the assessment questions. (derived from the standards and frameworks)
- The flow of the assessment questions.
- The scoring mechanism for the assessment.
- The situational questions and their possible effect on the assessment questions.
- Capability levels for the capabilities.

The Figure 34 shows the relationships between the CySME maturity model components. As can be seen from this figure, the capability assessment questions depend on standards.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	126 of 142	
Reference:	D6.3	Dissemination:	PU	
	Version:	1.0	Status:	Final

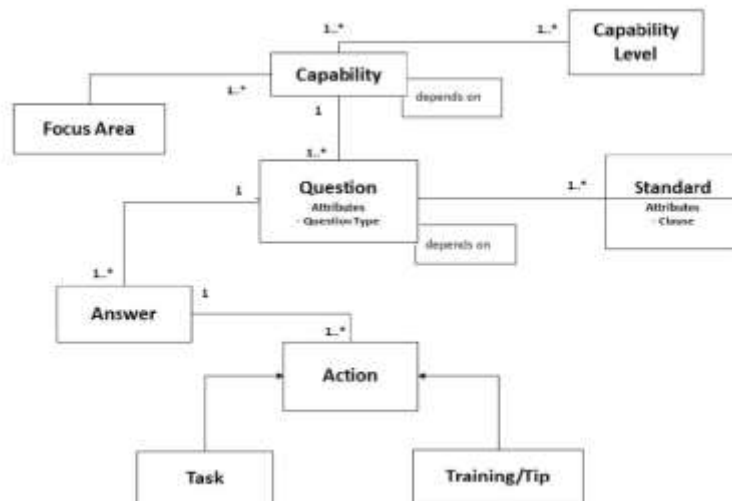


Figure 34: Relationships between the model components

With the help of the CySME maturity model and its implementation in CYSEC tool the mechanism shown in Figure 35 shows how by performing self-assessments, SMEs will be able to improve their capabilities as well as be aware and adhere to the underlying information security standards.



Figure 35: Assessment - Improvement - Standardisation Mechanism

4.2.4.4 The Process of selecting standards for the assessment questions

For the focus areas presented Table 25, we have investigated the applicable standards to identify the capabilities and the assessment questions. Figure 36 summarises the process of selecting standards for the assessment questions. ECSO published the State of The Art Syllabus, Overview of existing Cybersecurity standards and certification schemes [15] . This document includes a comprehensive list

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	127 of 142	
Reference:	D6.3	Dissemination:	PU	
	Version:	1.0	Status:	Final

of standards and specifications (International and EU) related to cybersecurity. For every focus area we searched the focus area in this publication. Then, we performed key word searches on the ETSI, CEN and CENELEC standards databases. Using the found standards, we identify a capability that is represented in the focus area. Finally, we formulate a question that can be used to assess the identified capability. An exemplary process is described in detail in the following paragraphs.

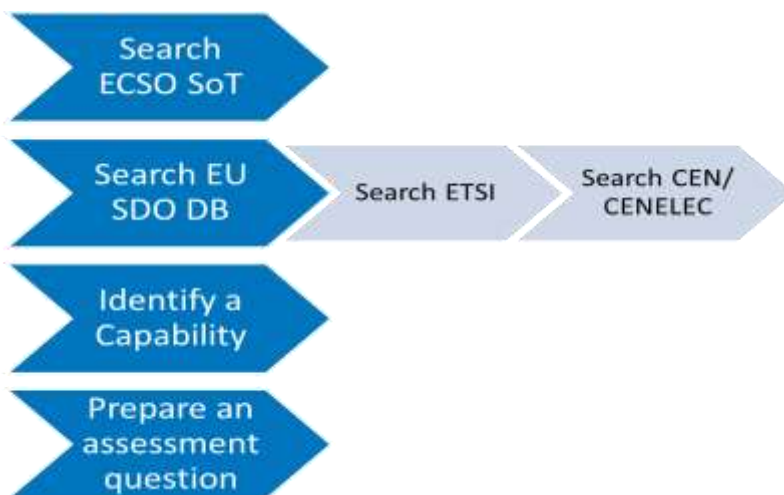


Figure 36: The process of selecting standards for the assessment questions

4.2.4.5 Exemplar Implementation for the Access Control and Audit Focus Area Capability

- Results of ECSO SoTA Search

The following standards in Table 26 were identified in the ECSO SoTA related to the focus area (Access Control and Audit).

Table 26: The results of ECSO SoTA Search

Standard	Description
ISO/IEC 27002:2013	Information technology -- Security techniques -- Code of practice for information security controls
Center for Internet Security (CIS) Critical Security Controls.	Critical Security Controls.
Cyber Essentials	10 Steps to Cyber Security

- Results of EU SDO Search

The following standards in Table 27 were identified in the ETSI, CEN and CENELEC database search related to the focus area (Access Control and Audit).

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)	Page:	128 of 142				
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

Table 27: ETSI, CEN and CENELEC database search results

Standard	Description
ETSI TS 103 532	CYBER; Attribute Based Encryption for Attribute Based Access Control
ETSI TR 118 516 V2.0.0 (2016-09)	oneM2M; Study of Authorization Architecture for Supporting Heterogeneous Access Control Policies (oneM2M TR-0016 version 2.0.0)
ETSI TS 103 458 V1.1.1 (2018-06)	CYBER; Application of Attribute Based Encryption (ABE) for PII and personal data protection on IoT devices, WLAN, cloud and mobile services - High level requirements
ETSI TS 103 645 V1.1.1 (2019-02)	CYBER; Cyber Security for Consumer Internet of Things
ETSI TR 103 305 V1.1.1 (2015-05)	CYBER; Critical Security Controls for Effective Cyber Defence

- Identifying a Capability

The following capability was identified as a result of the review of the standards:

Default vendor passwords are changed following installation of systems or software.

In order to assess this capability, the following assessment question was prepared:

Do you change default passwords for all applications, operating systems, routers, firewalls, wireless access points, printer/scanners, and other devices when adding them to the network?

We elaborated our findings in Table 28 showing the related standards, the related clause and the sub-clauses regarding the identified capability.

Table 28: Capability Identified in Different Standards

Standard	Name	Clause	Sub-Clause
INTERNATIONAL STANDARD ISO/IEC 27002	Information technology — Security techniques — Code of practice for information security controls	9.2.4 Management of secret authentication information of users	g) default vendor secret authentication information should be altered following installation of systems or software.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	129 of 142		
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

ETSI TS 103 645 V1.1.1	Cyber Security for Consumer Internet of Things	4.1 No universal default passwords	<p>Many IoT devices are being sold with universal default usernames and passwords (such as "admin, admin") for user interfaces through to network protocols. This has been the source of many security issues in IoT and the practice needs to be discontinued. Following best practice on passwords and other authentication methods is encouraged. Device security can further be strengthened by having unique and immutable identities.</p>
CIS	Center for Internet Security - Critical Security Controls	Control 4: Controlled Use of Administrative Privileges	Change Default Passwords Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts

As presented here, the identified capability is derived from several standards. By assessing this capability with the assessment question an SME will be aware of this requirement of several standards and by implementing this capability as advised by the CySME maturity model, SMEs will also improve their adherence to the standards.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	130 of 142		
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

5 Conclusions

For the period of this report, all WP6 activities made major progress:

On task T6.1 “exploitation”: as we progressed the SMESEC tools integration we had a more detailed proposals on what could be the commercial SMESEC offers.

On task T6.2 “dissemination”, we carried out many dissemination activities along the three-dissemination axis we have identified in our strategy. SMESEC got a lot of attention and what well known in particular when we launched the open call for helping further in validation.

On task T6.3 “standardisation”, we had a major move in revisiting the strategic with a more pragmatic approach mixing bottom-up and top-down ones; We had major interactions with key organisations and standardisation bodies and we held a key workshop to help SMESEC addressing key topics for SMEs.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	131 of 142		
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

6 References

- [1] Osterwalder, Alexander, and Yves Pigneur. Business Model Generation: A Handbook For Visionaries, Game Changers, And Challengers. Wiley, 2010, <https://www.strategyzer.com/canvas>;
- [2] D6.2 Annual report on exploitation, dissemination and standardization (Year 1), Mendelow (1991), Power interest matrix
- [3] D6.1 Dissemination plan and market analysis
- [4] D2.1 SMESEC security characteristics description, security and market analysis report
- [5] Grant Agreement-740787-SMESEC
- [6] Allied market research, <https://www.alliedmarketresearch.com/press-release/cyber-security-market.html>
- [7] <https://www.cyberbit.com/solutions/security-operations-automation-orchestration/>
- [8] <https://www.cyberbit.com/blog/security-operations/incident-response-save-gdpr-fines/>
- [9] <https://gcatoolkit.org/smallbusiness/>
- [10] <https://chronicle.security/>
- [11] <https://www.accenture.com/us-en/insights/security/cost-cybercrime-study>
- [12] <https://www.channelfutures.com/mssp-insider/smb-cybersecurity-budgets-rise-14>
- [13] <https://451research.com/>
- [14] EiQ Networks survey, <https://www.esecurityplanet.com/network-security/86-percent-of-smes-are-underfunding-cyber-security.html>
- [15] ECSO. (2017), “ECSO State of the Art Syllabus v2”, available at: <http://www.ecs-org.eu/documents/uploads/updated-sota.pdf>.
- [16] Spruit, M. and Röling, M. (2014), “ISFAM: THE INFORMATION SECURITY FOCUS AREA MATURITY MODEL”, ECIS 2014 Proceedings, available at: <https://aisel.aisnet.org/ecis2014/proceedings/track14/6>.
- [17] Mijnhardt, F., Baars, T. and Spruit, M. (2016), “Organizational Characteristics Influencing SME Information Security Maturity”, Journal of Computer Information Systems, Vol. 56 No. 2, pp. 106–115.
- [18] Mendelow (1991), Power interest matrix
- [19] H2020 project Fortika, <https://fortika-project.eu/>

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	132 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

7 Annex

7.1 Annex I IPR Agreement

IPR AGREEMENT

BETWEEN:

Description of partners detailed in the Consortium Agreement

1. **ATOS SPAIN SA (ATOS)**, established in CALLE DE ALBARRACIN 25, MADRID 28037,
Spain, VAT number: ESA28240752, represented for the purposes of signing the Agreement by Alicia GARCÍA
2. **WORLDSENSING S.L.N.E (WoS)**, established in C ARAGO 383, PLANTA 4, BARCELONA 08013, Spain, VAT number: ESB64902208,
3. **PANEPISTIMIO PATRON (UoP)**, established in UNIVERSITY CAMPUS RIO PATRAS, RIO PATRAS 265 04, Greece, VAT number: EL998219694,
4. **FOUNDATION FOR RESEARCH AND TECHNOLOGY HELLAS (FORTH)**, established in N PLASTIRA STR 100, HERAKLION 70013, Greece, VAT number: EL090101655,
5. **EASY GLOBAL MARKET SAS (EGM)**, established in ROUTE DES LUCIOLES 2000 CS 90029 LES ALGORTIHMES BATIMENT A, BIOT 06410, France, VAT number: FR10524029469,
6. **SCYTL SECURE ELECTRONIC VOTING SA (SCY)**, established in PLACA GAL LA PLACIDIA 1-3, 1A PLANTA, BARCELONA 08006, Spain, VAT number: ESA62604087,
7. **GRIDPOCKET SAS (GRIDP)**, established in ROUTE DE CRETES 300, VALBONNE SOPHIA ANTIPOLIS 06560, France, VAT number: FR06518639695,
8. **FACHHOCHSCHULE NORDWESTSCHWEIZ (FHNW)**, established in BAHNHOFSTRASSE 6, WINDISCH 5210, Switzerland, VAT number: CHE116216865MWST,
9. **BYTEMOBILE EUROPEAN DEVELOPMENT CENTER MEPE (ByteMobile)**, established in EO KATO-ANO KASTRITSIOU 4, KATO KASTRITSI PATRAS 26504, Greece, VAT number: EL099730753,

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	133 of 142		
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

10. **IBM ISRAEL - SCIENCE AND TECHNOLOGY LTD (IBM)**, established in 94 DERECH EM-HAMOSHAVOT, PETACH TIKVA 49527, Israel, VAT number: IL95432408,
11. **BITDEFENDER SRL (BD)**, established in 15A ORHIDEELOR STREET, ORHIDEEA TOWERS, 6TH DISTRICT, BUCHAREST, Romania, VAT number: RO18189442,
12. **UNIVERSITEIT UTRECHT (UU)**, established in HEIDELBERGLAAN 8, UTRECHT 3584 CS, Netherlands, VAT number: NL001798650B01,

hereinafter, jointly or individually, referred to as "Parties" or "Party" relating to the Action entitled

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

in short

SMESEC

hereinafter referred to as "Project" or "Action"

WHEREAS:

The Parties, having considerable experience in the field concerned, have submitted a proposal for the Project to the Funding Authority as part of the Horizon 2020 – the Framework Programme for Research and Innovation (2014-2020).

The Parties wish to specify or supplement binding commitments regarding intellectual property rights (IPR) handling among themselves in addition to the provisions of the specific Grant Agreement and Consortium Agreement.

NOW, THEREFORE, IT IS HEREBY AGREED AS FOLLOWS:

1. Purpose

1.1 The purpose of this IPR Agreement is to specify with respect to the Project the IPR ownership of all software components developed within the Project.

1.2 The "SMESEC" Grant Agreement (Attachment 1) and the "SMESEC" Consortium Agreement (Attachment 2) are attached to this IPR Agreement. The referred attachments are integral parts of this agreement. Should this agreement contain clauses contradicting Attachment 1 or Attachment 2, then all clauses in Attachment 1 and Attachment 2 overrule the clauses in this agreement.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	134 of 142		
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

1.3 The agreements made herein settle only the purpose defined in section 1.1 and not any future contracts or contracts, which are currently negotiated between some Parties.

2. IPR Ownership

Section X.0 and X.1 of the “SMESEC” Consortium Agreement (Attachment 2) settle the ownership of results.

In addition to the Consortium Agreement, this document settles that “*generation of results*” means that an owner has developed through substantial effort, research, time, and expense specific software components.

Basically, results are owned by the Party that generates them. However, if results are jointly generated and if it is not possible to establish the respective contribution of each Party; or separate them for the purpose of applying for, obtaining or maintaining their protection, a joint ownership is the case.

The following table lists all resulting components generated in the project SMESEC and indicates whether

- the component is owned by a single Party or
- in case of joint ownership
 - the component is owned by multiple Parties and contributions are separable or
 - if the component cannot be separated the degree (%) of a Party’s ownership

If a listed component uses (binary) code from another listed component, this code IS NOT covered by the corresponding IPR assignment.

Name of component	Subtask	Lead developer	Contributing parties	IPR %
AngelEye				
		IBM		100%
Risk Assessment Engine (RAE)				
		ATOS		100%

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	135 of 142
Reference:	D6.3	Dissemination:	PU	Version:	1.0
				Status:	Final

Name of component	Subtask	Lead developer	Contributing parties	IPR %
EGM-TaaS				
		EGM		100%
Anti-Rop				
		IBM		100%
Testing Platform (ExpliSAT)				
		IBM		100%
NetScaler AppFirewall				
		CITRIX		100
Cross-layer SIEM (XL-SIEM)				
		ATOS		100%
End Point Protection Platform				
		BD		100%
EWIS (Early Warning Intrusion Detection)				
		FORTH		100%
Cloud-based IDS (Intrusion Detection System)				
		FORTH		100%
CYSEC				
CYSEC Framework		FHNW	-	100%
CYSEC Content		FHNW		50%
			UU	50%

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	136 of 142
Reference:	D6.3	Dissemination:	PU	Version:	1.0
				Status:	Final

Name of component	Subtask	Lead developer	Contributing parties	IPR %
Maturity Model		UU		100%
Trainig platform				
		UoP		100%
Framework				
		ATOS		45%
		WOS		0%
		UOP		1%
		FORTH		5%
		EGM		1%
Integrated Front-End (Interface)		FHNW		37%
		CITRIX		0%
		IBM		1%
		BD		10%

3. Other provisions

3.1 This agreement becomes only operative if, and only if, it is signed by all parties.

Date: DD.MM.YYYY

Name:

Function:

Representing the following body:

full official address, and if any, VAT/registration number

Signature:

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	137 of 142
Reference:	D6.3	Dissemination:	PU	Version:	1.0
				Status:	Final

7.2 Annex II Commercial Agreement

Commercial agreement and compensation scheme strategy

1. Definitions

In this Agreement, the following words shall have the meaning determined hereunder:

- ✓ **Assets:** any project result designated as such by the project partners, such as Methods, Algorithms, Reference Architectures, Software Platforms and Components as well as their instantiations into a number of Industrial Trials experimentations.
- ✓ **Product:** any product or service which could be commercialized on the basis of the Assets.
- ✓ **Lead:** the potential final customer contact information and in some cases, more detailed information of a potential customer (e.g. budget).
- ✓ **Commercial Business Opportunities:** or shortly Business Opportunity (BO) means that one of the Parties has the opportunity to sell Assets or Product to a final customer on the market, which is not any of the Party that signed this agreement.
- ✓ **Internal Use Opportunity:** that one of the Parties (or an entity that belongs to the same Group of the Party) is the final customer for the Assets or Products or intends to apply Assets or Products for its own activities.
- ✓ **Lead generator:** the Party that has initial contacts with a potential customer and that answers initial enquiry into Assets or Products defined in this agreement.
- ✓ **Business Opportunity Proposing Party:** or shortly Proposing Party means the Party that carries out activities related to the preparation of Commercial Business Offering based on Assets, including the preparation of business opportunity dossier.
- ✓ **Contractor:** the Party that actually signs contract with the final customer and takes the responsibility of compensation sharing as agreed in this agreement.
- ✓ **Intellectual Property Owner:** (IP Owner) is the Party that owns IP over an Asset as listed in the Annex 1 of this Agreement
- ✓ **Service Provider:** is the Party or an external organization that provides specific services (e.g. training, consulting, integration, deployment, maintenance) related to the Assets and described in Business Opportunity Dossier.
- ✓ **Business Opportunity Dossier:** a document prepared by the Proposing Party describing as many details as possible related to the specific Business Opportunity, including proposed offering with related Assets and Services, draft financial conditions, list of Concerned Parties and any other that Proposing Party considers important to realize the opportunity.
- ✓ **Concerned Parties:** all Parties that have been identified by the Proposing Party in the Business Opportunity Dossier as IP Owners or Service Providers.
- ✓ **Implementation Arrangements:** any further agreements, contracts or similar that are used after the preparation of the Final Business Opportunity Dossier in order to realise this opportunity.

2. Scope

In the context of the Project, the Parties have produced Results in the form of a **range of separately exploitable components**. Some of components have been produced by one sole Party, while others have been produced based on the joint collaboration of several Parties.

The purpose of this compensation scheme is to establish the compensation terms under which the Parties will exploit Commercial Business or Internal Use Opportunities which may derive from or be based on the identified Assets, once the EU co-financed Project is finalised.

3. Duration

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	138 of 142		
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

This yearly Agreement shall take effect on the date hereof and remain valid until the expiration of a period of twelve (12) months from the date on which the Grant Agreement is terminated (the “Final Date”), and shall be thereafter renewed for one (1) year periods, each Party being entitled to terminate its participation, after the Final Date, at any moment by sending to the other Parties a termination notice in this respect, which shall take effect at least sixty (60) days after the date of the termination notice.

Notwithstanding anything to the contrary, in case of termination, the rights and obligations deriving from this Agreement will be maintained until finalisation of all Business Opportunities carried out by one or more of its Parties in accordance with the conditions provided therein. Although a withdrawal from the contract is possible, the contract provisions related to BOs that started before the termination notice apply in such a way, that the withdrawing party is obliged to fulfil the obligations already assumed (orders, etc.).

4. Results of the Project

The Parties agree that the list of project results designated as Assets, as well as intellectual property (IP) ownership of the Assets shall be ascribed as detailed in **Annex 1**.

5. Commercial Setting for the Use of Assets owned by the other Parties

Following the end of the Project, the Parties intend to engage in commercial activities towards selling or using Products.

a. Definition of Asset Business Model and Price List

Any Party is entitled to define a Business model (such as fixed annual licence fee, pay per use or free licence with obligatory expert service fee) and the according Price List guidance for each of its Assets owned accordingly and listed in Annex 1. This Price List might be discounted to other Parties for specific Commercial Business Opportunities or Internal Use Opportunities. If the Party considers that prices of its product or service shall be defined case by case, such Party is entitled not to include in the Annex 1 its prices or to include estimated price framework subject to future negotiations. For the avoidance of doubt this agreement does not limit the Parties to negotiate case by case the prices of their products or services.

b. Roles and responsibilities

The party that identifies a possible Lead (see definitions in the chapter 1) is called Lead Generator while the party that starts Business Opportunity and intends to exploit Product or Assets jointly under this Agreement will be called the “**Proposing Party**”.

Nothing in this Agreement limits the Party to exploit independently and out of this Agreement any of its own Intellectual property Rights related to the Assets or to exploit independently and out of this Agreement other solutions/products present in the market and in competition with Assets.

- the **Proposing Party** shall identify Assets relevant to Business Opportunity (BO) and will inform Asset IP owners, together with a detailed dossier including an estimation of BO Value, with financial projections and assumptions (which for the avoidance of doubt shall be based on guiding price list proposed by the Parties in the Annex 1 of this Agreement), together with a description of the activities in which the involvement of the other Parties could be necessary (such as professional services or similar activities with financial conditions at which such involvement is expected by the

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	139 of 142		
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

Proposing Party). The “**BO Dossier**” should therefore also identify list of services related to Business Opportunity and Assets (such as installation, deployment, configuration, consulting, training, maintenance and technical support). If IP owners listed their guiding price for specific expert or technical services such as training, deployment, maintenance etc (price in euros per manday) they can also have the role of Service Provider and can be included by the Proposing Party in BO Dossier. Separated Implementation arrangements can be negotiated between the Proposing Party and Service Providers, including the amount of service fee, independently from IP ownership or licensing fee.

- In case one or several Parties shall be involved in a **Business Opportunity**, they shall, together with the Proposing Party (and any third party, if need be), enter into Implementation arrangements to implement the concerned Business Opportunity. These Implementation arrangements might include purchase orders, contracts or special agreements between Concerned parties. For the reason of transparency these arrangements should be available on request to the Concerned parties.
- The **BO Value** is the sum of affected Assets prices and sum of prices of all additional professional services or external products included in the BO, (to be negotiated directly with the Concerned Parties based on guiding price list), but it refers the value before taxes.

Any Business Opportunity shall be presented by the Proposing Party to Concerned Parties and should be reviewed and discussed among them.

Before the celebration of the Business Opportunity agreement, the Concerned Parties:

- Can, if the Proposing Party agrees to, modify the conditions of the BO Dossier (the “**Modified BO Dossier**”);
- Can benefit from a right of refusal to participate to the Business Opportunity at the conditions presented in the BO Dossier or as agreed in the Modified BO Dossier, as the case may be, only during the first presentation of the BO (hereinafter referred as First Refusal).

In the case Concerned Parties accept the business conditions defined in the BO dossier, then the proposing party will release a **Final Approved BO Dossier**, which constitutes pre-commercial partners agreement.

Nothing in this Agreement shall be understood as an obligation of the Parties to participate in any Business Opportunity or to somehow contribute in it, except expressly agreed under any written Agreement.

Each Party obligates itself vis-à-vis each and every other Party to use reasonable endeavours to perform and fulfil, promptly, actively and on time, all of its obligations under this Agreement.

Each Party hereby undertakes to use reasonable endeavours to supply promptly to the parties involved in BO all such information or documents as the Party may need to carry out its responsibilities.

Each Party shall ensure the accuracy of any information or materials it supplies for the purpose of commercial activities and prompt corrections of any error therein of which it is notified. The recipient Party shall be entirely responsible for the use that such information and materials are given.

In addition, any Party hereby agrees to make available (under the conditions defined in the Implementing Arrangements) any of its Assets (including, but not limited to, any right it may have on Background or

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	140 of 142		
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final

the results) which is needed for use for the purpose of carrying out a Business Opportunity with other Parties.

The Parties undertake to respect and implement any standard of use of the Assets, in particular in the marketing of the Products.

Each Party has the right to carry out all the Business Opportunities in any part of the world, but in any event within, if any, the geographical scope agreed in the corresponding Implementation Arrangements. Each Party can delegate or sub-contract to other persons the performance of a Business Opportunity, as further specified in the Implementation Arrangements.

c. Compensation scheme framework

The compensation distribution scheme to be determined for each Business Opportunity shall recognise for each Concerned Party:

- (i) sales efforts, and therefore the related commission for such investments;
- (ii) the value of the IPRs made available by a Concerned Party for the concerned business opportunity;
- (iii) the service provision costs / investments:

It is specified that the values assigned to these items with respect to one Party in the Implementation Arrangements (e.g. contracts or specific agreements) regarding one Business Opportunity, shall also, unless otherwise agreed by the Concerned Parties, be applicable for any further Business Opportunity for which such Party participates.

Unless otherwise negotiated and agreed in the Implementation Arrangements,

- (i) Only in the case of a Commercial Business Opportunity and if the Lead Generator is different from Business Opportunity Proposing Party, a percentage of (**X%**) of the total value of the Total Contract Value (TCV) will be paid to the Lead Generator.
- (ii) Only in the case of a Commercial Business Opportunity a percentage of (**X%**) of the Total Contract Value will be paid to the Party(ies) who has(ve) generated the Business Opportunity (the proposing party), and
- (iii) the remaining compensation generated by the same Business Opportunity will be distributed among the Parties that participate in the Business Opportunity (Asset IP owners and Service Providers) depending on the selected business model and according to the list of Assets and Services outlined in the Final Approved BO dossier. This distribution will be negotiated for each Business Opportunity in the Implementation Arrangements and might refer to fixed amounts (e.g. licence fee, expert man-day fee) and variable amounts (e.g. pay per use) in relation to the value initially reported by BO dossier.
- (iv) In case of an Internal Use Opportunity, any percentage will be recognized to proposing Party(ies) who has(ve) generated the Business Opportunity,
- (v) If, during the exploitation period of a specific Business Opportunity, there is a change in the operation or exploitation which causes a participating Party to receive a level of income which is no longer in line with the income taken into account in the Implementation Arrangements, all

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)			Page:	141 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status: Final

Concerned Parties shall agree in good faith to any modification or adaptation necessary to allow the concerned Party to continue participating in the Business Opportunity on the same basis as originally contemplated in the initial Implementation Arrangements, except as otherwise agreed as between the Concerned Parties.

Document name:	D6.3 Annual report on exploitation, dissemination and standardisation (Year 2)				Page:	142 of 142	
Reference:	D6.3	Dissemination:	PU	Version:	1.0	Status:	Final