



# SMESEC

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

## D6.2 Annual report on exploitation, dissemination and standardization (Year 1)

Document Identification			
Status	Final version	Due Date	31/05/2018
Version	1.2	Submission Date	18/06/2018

Related WP	WP6	Document Reference	D6.2
Related Deliverable(s)		Dissemination Level (*)	PU
Lead Organization	EGM	Lead Author	Philippe COUSIN, EGM
Contributors	FHNW UU ATOS	Reviewers	Christos Tselios, CITRIX Francisco Hernández-Ramírez, WoS

### Keywords:

Dissemination, market analysis, cybersecurity, 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
Cousin Philippe, Giunta Nicolas	EGM
Fricker Samuel	FHNW
Yigit Ozkan Bilge, Spruit Marco	UU
Ruiz José Francisco, Miranda Garcia Alberto	ATOS
Christos Tselios	CITRIX
Francisco Hernández-Ramírez	WORLDSENSING

Document History			
Version	Date	Change editors	Changes
0.1	23/04/2018	EGM	Table of contents
0.2	04/05/2018	FHNW	Dissemination report M1-M12 in Section 3
0.3	07/05/2018	ATOS	Integration of UU Standardization part ToC, Integration of ATOS Exploitation part, Update in dissemination part
0.4	15/05/2018	FHNW	Inputs in the exploitation part, update of dissemination figures and addition of conference reports
0.5	16/05/2018	UU	Integration of UU standardization inputs
0.6	16/05/2018	EGM	Update in dissemination roadmap, global reading and minor corrections
0.7	17/05/2018	EGM	Final draft version ready for review
0.8	23/05/2018	CITRIX	Review
0.8.1	24/05/2018	EGM	Corrections and information update next to review 1 comments
0.8.2	25/05/2018	UU	Standardization section update
0.8.3	28/05/2018	FHNW	Dissemination section update: KPI updated, news items added
0.8.4	29/05/2018	ATOS	Exploitation section update
0.8.5	29/05/2018	EGM	FHNW content v0.8.3 integration, final

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)	<b>Page:</b>	2 of 126
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2
		<b>Status:</b>	Final version

			reading – Version ready for review 2
0.8.6	31/05/2018	WOS	Review 2
0.8.7	05/06/2018	UU	Update in standardization part, latest information
0.8.8	05/06/2018	EGM	Overall reading and minor corrections
0.9	06/06/2018	ATOS	Quality control
1.0	06/06/2018	EGM	Final refinements (references and figures)
1.1	12/06/2018	FHNW	Finalization of Dissemination KPI
1.2	18/06/2018	ATOS	Submission to EC

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)	<b>Page:</b>	3 of 126
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2
		<b>Status:</b>	Final version

# Table of Contents

Document Information .....	2
Table of Contents .....	4
List of Tables.....	10
List of Figures .....	11
List of Acronyms.....	12
Executive Summary .....	14
Introduction .....	15
1.1 Purpose of the document .....	15
1.2 Relation to other project work.....	15
1.3 Structure of the document .....	15
2 Business Plan and Exploitation strategy .....	16
2.1 Exploitation strategy.....	16
2.1.1 Exploitable items .....	16
2.1.2 Joint exploitation plan .....	23
2.1.3 Individual exploitation plans .....	24
3 Business Plan .....	27
3.1 Market analysis.....	27
3.1.1 Initial segmentation .....	28
3.1.2 PEST analysis.....	33
3.1.3 Competitors .....	35
3.1.4 Stakeholders analysis .....	39
3.2 Business Model .....	40
3.2.1 SMESEC Framework Business Model Canvas.....	40
3.2.2 Value proposition .....	42
3.2.3 Customer Segment .....	42
3.2.4 Channels .....	43
3.2.5 Customer Relationships.....	43
3.2.6 Revenue streams.....	43
3.2.7 Key activities .....	44
3.2.8 Key Resources .....	44

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)			<b>Page:</b>	4 of 126
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version

3.2.9	Key Partners .....	44
3.2.10	Cost Structure .....	45
4	Project dissemination .....	46
4.1	Dissemination strategy .....	46
4.1.1	Global approach and phasing .....	46
4.1.2	Objectives .....	47
4.1.3	Targets .....	48
4.1.4	Dissemination Messages .....	49
4.1.5	Project branding .....	51
4.2	Dissemination tools .....	55
4.2.1	Public Website.....	55
4.2.2	Printed materials.....	57
4.2.3	Other materials .....	60
4.2.4	Social networks .....	60
4.3	External events .....	61
4.3.1	Cyberstorm 2017 .....	62
4.3.2	AVAR 2017 Conference .....	63
4.3.3	34C3 - tuwat!.....	63
4.3.4	Industry 2025 R&D Conference.....	63
4.3.5	NDSS Symposium.....	64
4.3.6	REFSQ Working Conference .....	65
4.3.1	SAINT Project Workshop .....	65
4.3.2	Software Product Summit.....	65
4.3.3	Cyberwatching.eu Concertation Meeting .....	66
4.4	News / Blog Entries.....	66
4.4.1	SMESEC Project Launched .....	67
4.4.2	Project Management Board Meeting in Patras .....	67
4.4.3	Project Management Board Meeting in Haifa.....	67
4.4.4	Atos presents SMESEC in a national press note .....	68
4.4.5	Don't fail with EFAIL and stop panicking.....	68
4.5	Publications .....	69
4.6	Dissemination results .....	69

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)			<b>Page:</b>	5 of 126
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version

4.7	Dissemination plan update .....	71
5	Standardization activities .....	74
5.1	Standardization plan .....	74
5.1.1	Standardization approach and phasing .....	74
5.1.2	Objectives .....	75
5.1.3	Target standards developing organizations (SDOs) .....	76
5.2	Activities conducted during the Investigate Phase (M1-M6) .....	77
5.3	Activities conducted during the Analyse Phase (M7-M12) .....	78
5.4	Conclusions .....	84
6	Conclusions .....	85
	Annexes .....	86
1	Anti-Rop exploitation fiche .....	87
1.1	Component fiche 1 .....	87
1.2	Commercial Assessment of the component .....	87
1.2.1	Value proposition .....	87
1.2.2	Target users .....	87
1.3	Competition .....	87
1.4	Distribution model .....	88
1.5	Delivery model .....	88
1.6	Customer relationships .....	88
1.7	Financial Model .....	88
2	ExpliSAT exploitation fiche .....	89
2.1	Component fiche 2 .....	89
2.2	Commercial Assessment of the component .....	89
2.2.1	Value proposition .....	89
2.2.2	Target users .....	89
2.2.3	Competition .....	89
2.2.4	Distribution model .....	90
2.2.5	Delivery model .....	90
2.2.6	Customer relationships .....	90
2.3	Financial Model .....	90
3.1	Component fiche 3 .....	90
3.2	Commercial Assessment of the component .....	91

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)			<b>Page:</b>	6 of 126
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version

3.2.1	Value proposition .....	91
3.2.2	Target users .....	91
3.2.3	Competition .....	91
3.2.4	Distribution model.....	91
3.2.5	Delivery model.....	92
3.2.6	Customer relationships .....	92
3.2.7	Financial Model.....	92
4.1	Component fiche 4 .....	92
4.2	Commercial Assessment of EWIS .....	92
4.2.1	Value proposition .....	92
4.2.2	Target users .....	93
4.2.3	Competition .....	93
4.2.4	Distribution model.....	93
4.2.5	Delivery model.....	94
4.2.6	Customer relationships .....	94
4.2.7	Financial Model.....	94
4.3	Commercial Assessment of DDOS solution .....	94
4.3.1	Value proposition .....	94
4.3.2	Target users .....	94
4.3.3	Competition .....	94
4.3.4	Distribution model.....	95
4.3.5	Delivery model.....	95
4.3.6	Customer relationships .....	95
4.3.7	Financial Model.....	95
5.1	Component fiche 5 .....	95
5.2	Commercial Assessment of the component .....	97
5.2.1	Value proposition .....	97
5.2.2	Target users .....	97
5.2.3	Competition .....	97
5.2.4	Distribution model.....	98
5.2.5	Delivery model.....	98
5.2.6	Customer relationships .....	98

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)			<b>Page:</b>	7 of 126
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version

5.2.7	Financial Model.....	99
6.1	Component fiche 6 .....	99
6.2	Commercial Assessment of the component .....	100
6.2.1	Value proposition .....	100
6.2.2	Target users .....	101
6.2.3	Competition .....	101
6.2.4	Distribution model.....	102
6.2.5	Delivery model .....	103
6.2.6	Customer relationships .....	103
6.2.7	Financial Model.....	103
7.1	Component fiche 7 .....	103
7.2	Commercial Assessment of the component .....	104
7.2.1	Value proposition .....	104
7.2.2	Target users .....	104
7.2.3	Competition .....	104
7.2.4	Distribution model.....	106
7.2.5	Delivery model.....	106
7.2.6	Customer relationships .....	106
7.2.7	Financial Model.....	106
8.1	Component fiche 8 .....	107
8.2	Commercial Assessment of the component .....	108
8.2.1	Value proposition .....	108
8.2.2	Target users .....	109
8.2.3	Competition .....	109
8.2.4	Distribution model.....	110
8.2.5	Delivery model .....	110
8.2.6	Customer relationships .....	110
9.1	Component fiche 9 .....	111
9.2	Commercial Assessment of the component .....	114
9.2.1	Value proposition .....	115
9.2.2	Target users .....	116
9.2.3	Competition .....	116

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)			<b>Page:</b>	8 of 126
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version



9.2.4	Distribution model.....	116
9.2.5	Delivery model.....	117
9.2.6	Customer relationships.....	117
10.1	Component fiche 10.....	117
10.2	Commercial Assessment of the component.....	118
10.2.1	Value proposition.....	118
10.2.2	Target users.....	118
10.2.3	Competition.....	119
10.2.4	Distribution model.....	119
10.2.5	Delivery model.....	119
10.2.6	Customer relationships.....	119
10.2.7	Financial Model.....	120
11.1	Component fiche 11.....	120
11.2	Commercial Assessment of the component.....	120
11.2.1	Value proposition.....	120
11.2.2	Target users.....	120
11.2.3	Competition.....	121
11.2.4	Distribution model.....	121
11.2.5	Delivery model.....	121
11.2.6	Customer relationships.....	121
11.2.7	Financial Model.....	121
12	TaaS platform exploitation fiche.....	123
12.1	Component fiche 12.....	123
12.2	Commercial Assessment of the component.....	123
12.2.1	Value proposition.....	123
12.2.2	Target users.....	124
12.2.3	Competition.....	124
12.2.4	Distribution model.....	124
12.2.5	Delivery model.....	124
12.2.6	Customer relationships.....	124
12.2.7	Financial Model.....	125
	References.....	126

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)			<b>Page:</b>	9 of 126
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version

## List of Tables

<i>Table 1: Commercial vs non commercial exploitable items</i>	16
<i>Table 2: Commercial exploitable items (Components)</i>	21
<i>Table 3: Commercial exploitable items (Services)</i>	22
<i>Table 4: Non-commercial exploitable items</i>	22
<i>Table 5: Consortium partners individual exploitation plans</i>	26
<i>Table 6 : P.E.S.T Analysis of SMESEC framework [14]</i>	34
<i>Table 7: Competition matrix</i>	38
<i>Table 8 : Business Model Canvas for SMESEC framework</i>	41
<i>Table 9: Dissemination target groups</i>	49
<i>Table 10: Dissemination message</i>	50
<i>Table 11: Social network followers by month (*: no final figure available at the time of writing)</i>	60
<i>Table 12: Event participation of SMESEC consortium members during Year 1.</i>	62
<i>Table 13: Dissemination activities of SMESEC consortium members during Year 1.</i>	69
<i>Table 14: Visibility monitoring and related objectives (*: no objective defined in DOA)</i>	70
<i>Table 15: Scientific impact monitoring and related objectives (*: c.f. also previous table)</i>	71
<i>Table 16 : Targeted coming events</i>	72
<i>Table 17 : SMESEC Partners' Involvement with Standardization Bodies</i>	77
<i>Table 18 : Standards related to ATOS XL-SIEM</i>	78
<i>Table 19 : Standards related to Bitdefender GravityZone</i>	78
<i>Table 20 : Standards related to Citrix NetScaler</i>	78
<i>Table 21 : Standards related to EGM TaaS Solution</i>	79
<i>Table 22 : Standards related to FORTH / Early Warning Intrusion Detection System</i>	79
<i>Table 23 : Standards related to IBM AngelEye - Virtual patching</i>	80
<i>Table 24 : Standards/Literature related to IBM Anti-ROP</i>	80
<i>Table 25 : Standards related to E-voting Domain</i>	80
<i>Table 26 : Standards related to IOT Domain</i>	81
<i>Table 27 : Standards related to Smart Grid Domain</i>	81
<i>Table 28 : Standards related to Smart Cities Domain</i>	81
<i>Table 29 : Standardization Bodies/Organizations and SMESEC Domains</i>	82
<i>Table 30 : ETSI Clusters and SMESEC Relevance</i>	82
<i>Table 31 : ITU Workgroups and SMESEC Relevance</i>	83

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)			<b>Page:</b>	10 of 126
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version

## List of Figures

<i>Figure 1: Overview of SMESEC market analysis approach</i>	27
<i>Figure 2: Europe's SMEs by sector [2]</i>	28
<i>Figure 3: Europe IoT Data Management Market – Key Segments</i>	28
<i>Figure 4: SMEs landscape in Europe by activity – Source: Own creation/ Eurostats data</i>	32
<i>Figure 5: Best practices approach for security development – Source Eurosmart report</i>	32
<i>Figure 6: Identification of SMESEC stakeholders[8]</i>	39
<i>Figure 7: Stakeholders distribution</i>	39
<i>Figure 8: Business Model Generation, Alexander Osterwalder</i>	40
<i>Figure 9: Overview of SMESEC dissemination approach</i>	46
<i>Figure 10: Dissemination plan</i>	47
<i>Figure 11: Overview of SMESEC dissemination objectives</i>	47
<i>Figure 12: SMESEC business model (thick blue frames: priorities for dissemination).</i>	48
<i>Figure 13: SMESEC logo</i>	51
<i>Figure 14: SMESEC colour palette</i>	51
<i>Figure 15: SMESEC design elements and visual language.</i>	52
<i>Figure 16: SMESEC icons.</i>	53
<i>Figure 17: SMESEC infographics.</i>	54
<i>Figure 18: SMESEC webpage (main landing page).</i>	56
<i>Figure 19: SMESEC information architecture.</i>	57
<i>Figure 20: SMESEC flyer</i>	57
<i>Figure 21: SMESEC poster.</i>	58
<i>Figure 22: SMESEC poster.</i>	59
<i>Figure 23: Snapshots of the SMESEC presence on social channels</i>	60
<i>Figure 24: Overview of the SMESEC Standardization plan with five main phases, each consisting of several steps.</i>	74
<i>Figure 25: SMESEC related SDOs landscape</i>	76

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)			<b>Page:</b>	11 of 126
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version

## List of Acronyms

Abbreviation / acronym	Description
AI	Artificial Intelligence
AST	Application Security Testing
CAGR	Compound Annual Growth Rate
CASB	Cloud Access Security Brokers
CBOR	Concise Binary Object Representation
DAST	Dynamic Application Security Testing
DDoS	Distributed Denial-of-Service
DLTS	Datagram Transport Layer Security
EC	European Commission
EDR	Endpoint Detection and Response
EGRC	Enterprise Governance, Risk and Compliance
EI3PA	Experian's Independent 3rd Party Assessment
EPP	Endpoint Protection Platform
EU	European Union
FISMA	Federal Information Security Management Act
GDPR	General Data Protection Regulation
GLBA	Gramm-Leach-Bliley Act
GRC	Governance, Risk Management and Compliance
HIPAA	Health Insurance Portability and Accountability Act
HTTP	Hypertext Transfer Protocol
IAM	Identity and Access Management
IAST	Interactive Application Security Testing
ICO	Information Commissioner's Office
ICT	Information and Communication Technology
IDS	Intrusion Detection Systems
IoT	Internet of Things

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)	<b>Page:</b>	12 of 126
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2
		<b>Status:</b>	Final version

<b>Abbreviation / acronym</b>	<b>Description</b>
IPS	Intrusion Prevention Systems
ISO	International Organization for Standardization
IT	Information Technology
IPR	Intellectual Property Right
JVM	Java Virtual Machine
KPI	Key Performance Indicators
NGO	Non-Governmental Organization
OSS	Open source software and their communities
PCI DSS	Payment Card Industry Data Security Standard
PEST	Political, Economic, Socio-cultural and Technological
RASP	Run-time Application Security Protection
R&I	Research and Innovation
SAST	Static Application Security Testing
SDO	Standards Developing Organization
SIEM	Security Information and Event Management
SME	Small or medium-sized enterprise
SOX	Sarbanes-Oxley Act
SQL	Search and Query Language
SSL	Secure Sockets Layer
SWG	Secure Web Gateway
UEBA	User Entity Behaviour Analytics
UK	United Kingdom
URL	Uniform Resource Locator
USD	United States Dollar
UTM	Unified Threat Management
VPN	Virtual Private Network
WAF	Web Application Firewall
WP	Work Package
XSS	Cross-Site Scripting

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)	<b>Page:</b>	13 of 126
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2
		<b>Status:</b>	Final version

---

## 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 an overall strategy to maximize the project audience, prepare the final framework exploitation and efficiently contribute in the related standards. In the same time, SMESEC will improve the overall awareness of the SMEs in the cybersecurity domain through a carefully designed and meticulously executed plan, fully integrated into the Project's dissemination activities.

Core target of the project, SMEs will be associated in all SMESEC steps from framework definition, experimentation and validation within a continuous exchange within SMEs organization, H2020 sister projects, partners existing networks, survey and other events participation. This strategy will be implemented at the European level, with a dedicated role of each partner in their respective country and expertise area. This deliverable describes the dissemination, exploitation and standardization activities carried out during the first 12 months of SMESEC project, including an overview of the exploitation roadmap and all communication and standardization actions set to enhance the project impacts with an update of the initial strategy defined at M6.

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)	<b>Page:</b>	14 of 126		
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version

---

# Introduction

---

## 1.1 Purpose of the document

---

---

This document presents the overall first-year results of the SMESEC project in the areas of dissemination, exploitation and standardization. It gives an overview of the performed work from all consortium partners and provides a more accurate view of the project roadmap with an update of the initial plan presented in the previous deliverable D6.1 at M6.

The global strategy of the consortium is maintained for the coming months, however as the technical part progressed, SMESEC integrated into its approach feedbacks from reached SMEs or representatives, as well as input derived from other work packages aiming to further enhance the project impact on several domains.

## 1.2 Relation to other project work

---

---

This work is based on all WPs and especially on WP2 and WP3 bringing inputs for technical understanding and use cases definition, in the creation of the security awareness plan, presented in the deliverable D2.3 at M6.

## 1.3 Structure of the document

---

---

This document is structured in four major chapters:

**Chapter 1** presents the SMESEC business plan and exploitation strategy.

**Chapter 2** presents the communication activity, the tools that were developed for the period M1-M12, as well as an update of the initial dissemination plan.

**Chapter 3** presents the conducted work in the two first phases (Investigation, Analysis) in the period M10 – M12, along with further details in the standardization strategy plan.

**Chapter 4** presents the standardization strategy plan, and the related activity for the period M1-M12.

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)	<b>Page:</b>	15 of 126		
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version

## 2 Business Plan and Exploitation strategy

### 2.1 Exploitation strategy

#### 2.1.1 Exploitable items

The following section broadly describes various exploitation items carried out during the first year of the project, based on results that will be more mature in the forthcoming periods. Table 1 categorizes the results in commercial and non-commercial exploitation activities. All these items have been widely detailed on individual fiches generated by each partner (see Annex I).

SMESEC will deliver the following project results based on their distinct characteristics categorised into:

- *Software/developments.* This category refers to tangible outcomes, namely the SMESEC framework, toolkits,
- *Services.* The word “Service” refers to the traditional meaning of IT services. These are future services offered around SMESEC, which aim at improving customers' effective use of SMESEC solutions and to provide in-depth customized assistance to SMEs.
- *Knowledge.* This category comprises the project know-how (mainly contained in deliverables and papers), methodologies, architecture, and primitives.

Commercial Exploitation	Non-commercial Exploitation
<ul style="list-style-type: none"> <li>• <b>Software/Developments</b> SMESEC framework SMESEC components</li> <li>• <b>Services built around the SMESEC framework</b></li> </ul>	<ul style="list-style-type: none"> <li>• <b>Training</b></li> <li>• <b>Knowledge (Know-How, papers)</b></li> <li>• <b>Collaboration with standardization bodies</b></li> <li>• <b>Use the developments for academic purposes</b></li> </ul>

**Table 1: Commercial vs non commercial exploitable items**

The SMESEC offering distinguishes between the aforementioned exploitation options to clearly categorise all the items identified at this stage of the project.

Each one has distinct and appropriate ways of exploitation, aligned with its technological maturity level and the ability to transfer the added value generated by the project to the market. The consortium aims to effectively transfer the results to the market and to ensure the economic sustainability of the solutions.

SMESEC exploitation strategy proposes several actions which pave the way for the adoption of the project's results.

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)	<b>Page:</b>	16 of 126
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2
		<b>Status:</b>	Final version



These strategies focus on following a sales lifecycle with strong emphasis on prospecting potential customers by contacting them and promoting the key features of SMESEC. This can be summarized as *“To support SMEs on to protect their business from cyber-security threats”*. The exploitation activities will receive feedback from the project pilots and the interaction with the SME’s associations and the companies participating in the open call (planned at month 24).

It is important to mention that this initial exploitation plan is based on the current status of the technical developments of the project. Most of the SMESEC components are still under development, and corrective technical decisions must be taken in the following months, with a significant impact on the current exploitation plan. This explains why this deliverable focuses mainly on the value proposition, while other business factors, such as the distribution strategy, are just tentative ideas to be modified in the future. Others, such as the business models, pricing structures or cost/benefit analysis are not totally defined yet.

These questions will be solved in the future deliverables due by M24 and M36, which are expected to contain the updated version of the exploitation plan progressing in parallel with the project.

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)	<b>Page:</b>	17 of 126		
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version

### 2.1.1.1 Software/Developments

This category comprises all project tangible outcomes/developments, listed in the following sections that SMESEC generates. As mentioned above, all project components as categorized according to their commercial and non-commercial exploitation eligibility.

Each component includes a resume description of the exploitation fiches detailed in the document Annex1.

Component name	Benefits	Target user
<b>Early Working Intrusion System(EWIS)</b>	<ul style="list-style-type: none"> <li>Lively reporting of attacks happening in the network</li> <li>Network decoys that appear more “appealing” to the attacker, thus diverting them from attacking the real infrastructure.</li> <li>Detect attack prior to happening to the real system</li> <li>Emulation of real services that we want to protect</li> </ul>	All SMEs offering services over the internet using protocols like HTTP, SMB, MSSQL, MySQL etc.
<b>Cloud-based IDS (Intrusion Detection System)</b>	<ul style="list-style-type: none"> <li>Reporting of DoS attacks happening in the network</li> <li>Standalone solution can be deployed to the same network we want to protect</li> <li>Based on the detection of amplification DoS attack no need for extensive network monitoring.</li> </ul>	All SMEs offering services over the internet
<b>Secure wireless monitoring and data acquisition system</b>	<ul style="list-style-type: none"> <li>Quality of service for the target users improved: the system is not easily hacked, and the service continuity is achieved (resilience improvement).</li> <li>Data protection: data are acquired, processed and stored with secure protocols to guarantee their integrity in their whole lifecycle.</li> </ul>	The intended users of the “evolved” solution of Worldsensing are basically the same than those from the already-commercial product LoadSensing. By adding new features to this new release of LoadSensing, Worldsensing aims to improve the market penetration offering a differentiating factor regarding the competence. Right now, LoadSensing is addressed worldwide to city and infrastructure operators, construction companies and mines operators mainly.
<b>Risk Assessment Engine (RAE)</b>	The tool allows a real-time evaluation of the systems by executing qualitative and quantitative models. The assessment is done together with the business profile of the organization, allowing having specific information about how the risks affect them from a management and financial point of view.	Main target is the cybersecurity experts of the organizations. They are the ones that work in defining the models for assessment and analysing the results of the tool. Together with this role it is important also the management level, as, together with the cybersecurity expert, works in defining the impact of the threats at management and financial level.

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)	<b>Page:</b>	18 of 126
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2
		<b>Status:</b>	Final version

Component name	Benefits	Target user
		The output will be used by both the cybersecurity expert (for identifying threats and vulnerabilities) and the management role for taking decisions at high-level
<b>XL-SIEM</b>	The tool improves other existing open source solutions in different ways. Among other characteristics, one of the more interesting is the enhancement of the performance and scalability, allowing processing of big amounts of data and having the possibility of performing event correlation at different layers with more complex rules. Additionally, one key objective of the XL-SIEM is to increase the awareness of cybersecurity for the users, which is supported with an interface for visualization that includes high-level charts and diagrams in different dashboards, including decision-support ones	Cybersecurity experts of organizations, ranging from SMEs to large organization. Refining the information of the cybersecurity status and provide it to other layers of the organization for decision support (e.g. management). Any type of domain, the main target is information technology companies, which either support or work with data (e.g. personal, of organisations, etc.) or provide digital services. In that sense, organizations working with IoT devices, big data, cloud systems or services, etc. would be the ones that take more advantage of our tool.
<b>NetScaler App Firewall</b>	This tool is a comprehensive web application firewall that analyses all bi-directional traffic, including SSL-encrypted communication, to protect against a broad range of security threats.	<ul style="list-style-type: none"> <li>• Networking vendors / large enterprises</li> <li>• Key networking industry players</li> <li>• SME, SMB, large companies</li> </ul>
<b>NetScaler Gateway</b>	This tool provides users with one access point and single sign-on (SSO) to business applications and data deployed in a datacentre, the cloud, or delivered as SaaS across a range of devices.	<ul style="list-style-type: none"> <li>• Networking Vendors / Large Enterprises</li> <li>• Key Networking Industry players</li> <li>• SME, SMB, Large companies</li> </ul>
<b>NetScaler Secure Web Gateway</b>	This tool addresses main security challenges through advanced traffic inspection, intrusion blocking, malware elimination, and application control	<ul style="list-style-type: none"> <li>• Networking Vendors / Large Enterprises</li> <li>• Key Networking Industry players</li> <li>• SME, SMB, Large companies</li> </ul>
<b>EGM-TaaS</b>	<ul style="list-style-type: none"> <li>• Benefits for the target users               <ul style="list-style-type: none"> <li>○ Flexibility – Lightweight offer without integration or maintenance phases</li> <li>○ Modularity – Modular and flexible infrastructure</li> <li>○ Reactivity and quality – MBT powered tool enabling fast integration of new security standards or customer test suites,</li> </ul> </li> </ul>	Describe which is the intended user(s) of your solution, considering: <ul style="list-style-type: none"> <li>• Market addressed: ICT companies</li> <li>• Specific industry more suited for the component: IT related SMEs especially in IoT such as system integrators</li> <li>• Specific size of organization being targeted:</li> </ul>

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)	<b>Page:</b>	19 of 126
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2
		<b>Status:</b>	Final version

Component name	Benefits	Target user
	<p>full test coverage and traceability</p> <ul style="list-style-type: none"> <li>• Added value for the target users               <ul style="list-style-type: none"> <li>○ Cost efficient – No maintenance cost, efficiency in software development with non-regression testing, continuous testing during the development phase.</li> <li>○ Quality oriented – User-friendly interface, full details testing reports, fully customizable</li> </ul> </li> </ul>	<p>SME</p> <ul style="list-style-type: none"> <li>• Geographical area: Europe</li> </ul> <p>Role in the organization: Test engineer, Security analyst</p> <ul style="list-style-type: none"> <li>• Market addressed: Testing laboratories</li> <li>• Specific industry more suited for the component: IT Certification centres</li> <li>• Specific size of organization being targeted: SME, Large company)</li> <li>• Geographical area: Europe</li> </ul> <p>Role in the organization: Test engineer, Security analyst</p>
<b>Information security assessment model</b>	<ul style="list-style-type: none"> <li>• SMEs will be able to conduct self-assessments on their information security capabilities.</li> <li>• SMEs will be able to better understand information security requirements, their dependencies and associate these requirements with the standards.</li> <li>• SMEs will be able to formulate their personalized improvement plans for their desired improvement path.</li> <li>• SMEs will be able to compare their information security capabilities with another SME's.</li> </ul>	<p>Regardless of the industry, information security maturity model could be used by any SME.</p> <p>The usage of the maturity model requires basic knowledge on information security and information technology concepts.</p>
<b>AngelEye (Virtual Patching)</b>	<ul style="list-style-type: none"> <li>• Create a virtual patch of C/C++ application</li> <li>• The virtual patch can predict an input that may trigger a vulnerability before the vulnerability is found by testing technique</li> </ul>	<ul style="list-style-type: none"> <li>• Developers that want to create polymorphism in their code to obtain better resiliency to ROP attacks</li> <li>• Developers of IoT platforms that want to harden their gateways/endpoints and break the scalability of cyber-attacks on their platform</li> </ul>
<b>Anti-ROP</b>	<ul style="list-style-type: none"> <li>• Create various unique executable copies of a C/C++ application</li> <li>• Break the attackers' ability to scale-up their knowledge of one device to attack another.</li> </ul>	<ul style="list-style-type: none"> <li>• The target users are the developers of new software that need to protect their software against vulnerability exploitation.</li> <li>• Additional usage is to protect binaries against vulnerability exploitation.</li> </ul>

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)	<b>Page:</b>	20 of 126
<b>Dissemination:</b>	PU	<b>Version:</b> 1.2	<b>Status:</b> Final version

Component name	Benefits	Target user
<b>ExpliSAT</b>	<ul style="list-style-type: none"> <li>Identifying security vulnerabilities early in the development process</li> <li>Releasing more secure code which increase the software resiliency to cyber attack</li> </ul>	<ul style="list-style-type: none"> <li>The target users are the developers of new software that need to amend vulnerable code before they release their products.</li> <li>Additional usage is to locate the vulnerability after an exploit to provide a timely patch with the right fix.</li> </ul>
<b>Endpoint Protection Platform</b>	GravityZone delivers multiple layers of security for endpoints and for Microsoft Exchange mail servers: antimalware with behavioural monitoring, zero-day threat protection, application control and sandboxing, firewall, device control, content control, anti-phishing and antispam.	Bitdefender is already addressing the global market, encompassing start-ups, SMEs and large corporations, usually seeking contact with the CIO or the cybersecurity responsible of the targeted organisation.
<b>FHNW-CYSEC CyberSecurity Coach</b>	This tool will provide end users with the ability to assess and improve the cybersecurity capabilities of their SME incrementally in a low-cost do-it-yourself manner. For the cybersecurity community, the tool will offer feedback regarding the SME priorities and fitness of cybersecurity advice/trainings/technology.	<ul style="list-style-type: none"> <li>SME</li> <li>Cybersecurity community</li> </ul>

**Table 2: Commercial exploitable items (Components)**

### 2.1.1.2 Services

This section includes main services provided by project partners. Alongside to these services, additional ones (consulting, system integration and deployment, training and maintenance) can be provided by one or several partners once the exploitation strategy is defined at a later stage of the project.

Component name	Benefits	Target user
<b>SMESEC components integration/deployment</b>	Process outsourcing, cost	All customers that request support after buying any SMESEC component
<b>Consulting / Training Services</b>	Process outsourcing, cost	All customers that request support after buying any SMESEC component
<b>Maintenance</b>	Process outsourcing, cost	All customers that request support after buying any SMESEC component

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)	<b>Page:</b>	21 of 126
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2
		<b>Status:</b>	Final version

**Table 3: Commercial exploitable items (Services)**

2.1.1.3 Other outcomes

This section lists all non-commercial exploitable items identified by consortium partners, spanning from knowledge transfer to standardization activities.

<b>Component name</b>	<b>Benefits</b>	<b>Target user</b>
<b>Papers in academic conferences/journals</b>	Advance of the state of the art in the topics of the project. This also improves the branding of the project.	Academic and applied research community.
<b>Master thesis</b>	Advanced training in cybersecurity for some talented students enrolled in MSc programs related with the academic partners of SMESEC	Students of different universities
<b>PhD thesis</b>	Generation of high-quality academic results with practical impact within the context of the project	Academic community
<b>Courses</b>	Training in cybersecurity topics related to the project	Students enrolled in MSc programs of different universities.
<b>Talks</b>	Invited presentations about SMESEC and the technology being developed in the project.	Industry and academia

**Table 4: Non-commercial exploitable items**

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)			<b>Page:</b>	22 of 126
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version

### 2.1.2 Joint exploitation plan

One of the key objectives of the project itself is to extend the lifespan of the SMESEC framework beyond the actual duration of the project per se. To make it possible, sustainability is the keyword to be used. This can be only achieved if enough number of consortium partners are committed to support the forthcoming phases in a joint approach. This commitment has strong dependencies on the strategic decisions of the partners' organizations.

It is key to have an open discussion and check each partner's interest and try to preserve the engagement or to look for alternatives that could fill a potential gap.

The main topics to discuss and agree will be:

- Licencing approach to be used (for the whole SMESEC Framework, covering the licencing restrictions/needs of each partner of the project) with the different components developed;
- IPR (Intellectual Property Rights) / Partner compensation scheme;
- New legal structure/consortium agreement to extend the project activities beyond its lifespan;
- Bilateral/multilateral agreements between partners to exploit the SMESEC individual components.

Several scenarios can be envisaged at the end of the project:

- 1 All consortium partners commit to a joint exploitation of SMESEC.
- 2 Not all partners commit to the joint SMESEC solution. Multilateral agreements can be reached between the partners to exploit individual components or groups of them that can provide a service or cover a market segment need.
- 3 Each partner wants to exploit individually their components.
- 4 Bilateral (multilateral) partners' agreement can be reached to exploit a group of components that can offer one or several functionalities to the market.

All these topics will be initiated during the second year of the project once the technology developments are defined and remain on track.

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)	<b>Page:</b>	23 of 126
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2
		<b>Status:</b>	Final version

### 2.1.3 Individual exploitation plans

The present section provides the SMESEC partners' individual exploitation plans based on the original plans presented on the Grant agreement[1]. As a living document those plans will be updated once the results of the project are more mature Each plan describes in a summarized way a description of the relevance of the project SMESEC for the organization and a short description of the individual exploitation plan along the project execution. Taking into account that consortium partners come from the three major organization roles (industrial partners, academic and research partners) these plans cover a multi-angle perspective of the exploitation strategy:

Consortium partner	Description
<p style="text-align: center;"><b>ATOS</b></p>	<p>The ATOS portfolio brings together all ATOS capabilities in the sector, delivering a 360-degree security and full spectrum control and combining relevant experience and knowhow from all ATOS Service Lines. SMESEC advances in information security, safety and trust in the SMEs domain fits quite nicely in the ATOS Identity, Security and Risk Management portfolio of solutions. Particularly the Governance, Risk and Compliance (GRC) offerings where the ATOS High Performance Security (AHPS) services helps managing controls efficiently, consistently and reliably across the enterprise, ensuring an ideal balance amongst compliance requirements, IT security issues and operational expenses. Moreover, ATOS will exploit SMESEC results through strategic R&amp;D&amp;I consulting and Technology Watch, applying the latest research results to opportunities where clients need solutions that go beyond markets. Increased possibilities to undertake research and innovation projects, outreaching to key players in the innovation sector (research institutes, universities, etc.).</p>
<p style="text-align: center;"><b>Worldsensing</b></p>	<p>A very active SME in innovation activities. Its core expertise is in providing sensing and machine-to-machine technologies and services to specific industry verticals. It has two mains product portfolios: one being smart traffic solutions for smart cities; and the other being heavy-industry monitoring solutions. Taking into account Worldsensing clients and targets, such company will exploit the security framework capabilities and skills acquired in this project to push its core business. Their typical clients are city councils and companies' owner and manager of big infrastructures. SMESEC will provide to Worldsensing a fundamental knowledge for increasing the quality of the provided services in this context. After SMESEC this SME will be able to provide "reliable" Internet of Things applications where security threats are analyzed and minimized. These benefits will open the door to many more business cases and thus to novel opportunities for increasing the number of clients and products sales.</p>
<p style="text-align: center;"><b>IBM</b></p>	<p>The role on this project is to support the development of the SMESEC security framework and to enable business growth for SMEs involved in this initiative. IBM is constantly looking for the synthesis of security into the business requirements. Its deep industry and business understanding enables them to tailor their products to facilitate specific business requirements. With specialists in</p>

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)	<b>Page:</b>	24 of 126
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2
<b>Status:</b>	Final version		



<b>Consortium partner</b>	<b>Description</b>
	<p>application, infrastructure, organizational and cyber security, IBM aims to maintain its outstanding reputation for delivering value and excellence to all their clients. This includes the identification of new key data groups mapping the related security threats and possible attack platform, business processes and the core assets that they need to protect. The SMESEC project will give to IBM the opportunity to develop and then exploit agnostic security solutions within the SMEs environment as well as extend the company products and services in the security and digital sector.</p>
<b>CITRIX</b>	<p>Long-time experience in highly security-critical IT markets, and successfully develops products and solutions to make SW-based solution safer and more user-friendly. With its platform and their concepts, CITRIX guarantees an optimal IT-network management by adjusting their solutions to user demand and expectation. With its expertise on service offering, CITRIX is an important member of SMESEC project since they will support this initiative by organizing and securing the end-point devices and sensitive IT-networks components of SMEs and by offering continuous support to the project's pilots and real-life experimentations. CITRIX will exploit SMESEC by contacting with novel clients from both Public Administrations and private companies and by improving the actual security solutions for specific verticals as Smart Grid and/or Smart Industry (e.g. IoT). Such opportunity will create a great chance for CITRIX in order to further exploit the security and digital EU market for the next decade.</p>
<b>GridPocket</b>	<p>An innovative company devoted on the 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 behavioral experts' systems for electricity, water and gas utilities. GridPocket distributes its applications through partnerships with energy distributors, ESCOs (energy saving companies), equipment manufacturers and utilities worldwide. GridPocket's applications enable end-users to take full control over their energy spending and reduce their CO2 emissions. Moreover, the complete analysis and an oversight over a customer behavior are proposed to energy utilities as a mean to match electricity consumption following peak times and real time electric demands. The participation of GridPocket within SMESEC is a great opportunity for this SME. Indeed, GridPocket will be able to integrate the last cyber-security solutions in their applications, increasing the overall level of system reliability while adopting privacy-preserving methods to protect their clients' data. GridPocket is focusing on citizens' engagement solutions to empower their platform with more users and data. SMESEC will contribute on this direction since the project's participation will facilitate the creation of relevant material to increase the awareness of secure solutions in the context of Smart Grid.</p>
<b>Bitdefender</b>	<p>BD provides several security products that include anti-virus and anti-spyware capabilities against internet security threats such as viruses, Trojans, rootkits, rogues, aggressive adware, spam and others. Bitdefender applications include web protection, cloud anti-spam, firewall, vulnerability scanner, parental controls, document encryption and device antitheft as well as backup for corporate and home users. Bitdefender will use SMESEC as a catapult to enter in the cyber-security market for SMEs and innovative digital solutions; the SMESEC use cases will be composed from innovative multi-technology solutions that will provide an incredible test</p>

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)	<b>Page:</b>	25 of 126
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2
<b>Status:</b>	Final version		

<b>Consortium partner</b>	<b>Description</b>
	board to evaluate the most interesting configuration about cyber-security for novel technology as IIoT, Smart City, etc. On one side, the great experience on cyber-security of Bitdefender will provide a transversal value for SMESEC and, on the other side, the great network of contacts of SMESEC will propose a long list of possible novel clients for Bitdefender. Bitdefender aims to approach innovative solutions market by exploiting its experience on internet security. This will allow to potentially increase their sales even at short-term.
<b>SCYTL</b>	The worldwide leader in secure electronic voting, election management and election modernization solutions. Their solutions incorporate unique cryptographic protocols that ensure maximum security, transparency and auditability in all types of elections. Scytl's groundbreaking electoral security technology is protected by international patents and 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. Within SMESEC, Scytl will be able to update the implemented security solutions with more efficient mechanisms. Indeed, 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.
<b>Easy Global Market</b>	EGM provides solutions and services to develop market confidence for the adoption of innovative technologies. Moreover, Easy Global Market is making the global market "easy" for companies looking for globalization. This company is strongly active in the major technology clusters and innovation networks, enhanced by the experience gained by their directors working in +30 research projects and designing +10 worldwide label or certification programs. Easy Global Market is funding member of IoT Forum and is member of key European clusters, standard bodies and alliances such as ETSI, OneM2M, AIOTI, SCS cluster, etc. Within SMESEC, Easy Global Market, on one hand, will help project's SMEs regarding the achievement of novel business opportunity with its experience on internationalization and business model, and on the other hand, it will increase their knowledge on cyber-security and digital solutions as well as will contact novel potential clients in project's verticals.
<b>FHNW</b>	FHNW will develop and utilize the SMESEC exploitable items consisting in educational offerings in cybersecurity for BSc and MSc students as well as industry-courses within the Swiss CAS/MAS educational frameworks (12'000 FHNW active students). In the meantime FHNW intends to bring the FHNW-CYSEC tool to market readiness for commercial offering in cooperation with industrial and academic partners. FHNW runs more than 1000 such applied research projects with industry, help EGM to establish an industrial certification programme following the experience of FHNW members in establishing the successful ireb.org and ispma.org industrial certification programmes but also contribute in advancing scientific knowledge and industrial practice in cybersecurity engineering with one PhD thesis and two MSc theses, papers and talks in industry, academic conferences and journals.

**Table 5: Consortium partners individual exploitation plans**

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)	<b>Page:</b>	26 of 126
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2
<b>Status:</b>	Final version		

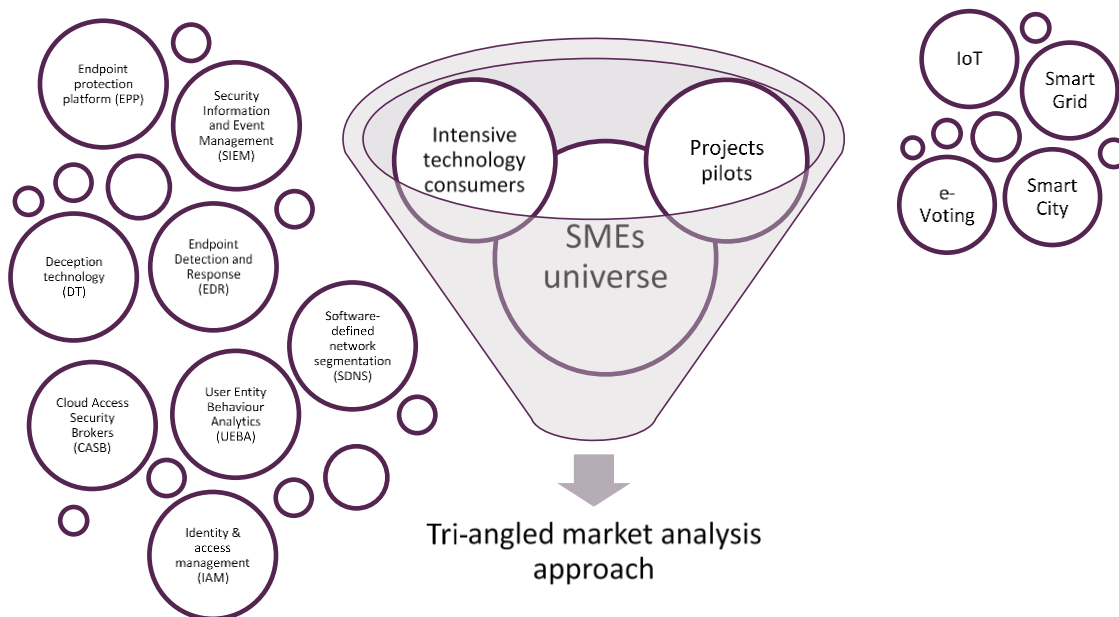
## 3 Business Plan

### 3.1 Market analysis

As part of market analysis (a quantitative and qualitative assessment of a market), SMESEC project has initiated a first approach to the key drivers to create a basis for the design and development of the objectives of the project (an extended version of the market analysis can be found in D6.1 [2] ). SMEs represent in Europe about 99% of the total number of established companies and contribute in about 60% in the value-added production[13]. Usually early adopters and first players in emerging markets, SMEs are facing today cybersecurity threats that may seriously hinder the company’s development. Larger enterprises can afford costly security solutions and own expertise resources to prevent alert and react to cyberattacks and cybercrime threats.

The objectives of this task are to better understand the market to increase the SMESEC potentialities with a tri-angled approach as illustrated in the Figure 1: Overview of SMESEC market analysis approach by:

- Analyzing current trends, performing market segmentation and investigating market barriers.
- Surveying the existing technologies, (described in D2.1)[3].
- Assessing selected business and technology transfer models in different EU countries.



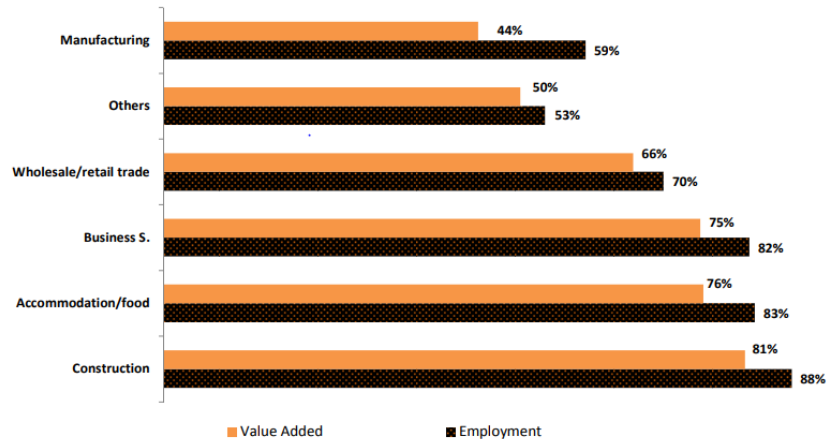
**Figure 1: Overview of SMESEC market analysis approach**

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)	<b>Page:</b>	27 of 126
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2
		<b>Status:</b>	Final version

A top-down market analysis approach will include the generic SMEs’ market domain up to the use case pilots’ market domains alongside with new emerging markets where SMEs have a specific weight. As a living document, the market will be monitored throughout the project’s lifetime and any major impact on the analysis would be reported in the forthcoming exploitation documents.

### 3.1.1 Initial segmentation

SMESEC aims to become a “ready-to-market solution with an immediate market impact. With international and European links, the project will provide a harmonized solution with high quality and affordable cybersecurity tools validated in multiple SMEs environment. Increasing SMEs protection will also be ensured by focusing on increasing awareness and training among these organizations.



The key driver of the SMESEC project orbits around SME’s in Europe (primary target), therefore the direct market target should include all SME’s (In 2015, just under 23 million SMEs generated €3.9 trillion in value added and employed 90 million people as illustrated in Figure 2) [2].

Figure 2: Europe's SMEs by sector [2]

A more specific target (secondary target) will place the focus on the main SME’s areas where cybersecurity developments can generate a greater added value to the organization which implements those enhancements:

- Data management

According to the “Europe IoT Data Management Market Report (2017 – 2023)”[5], published by KBV research, the Europe Internet of Things (IoT) Data Management SMEs Market would witness a market growth of 16.1% CAGR during the forecast period (2017 – 2023). Other studies [4] value globally this market in **USD 23.8 Billion in 2016 and are projected to reach USD 66.44 Billion by 2022**, at a Compound Annual Growth Rate (CAGR) of 19.3%.

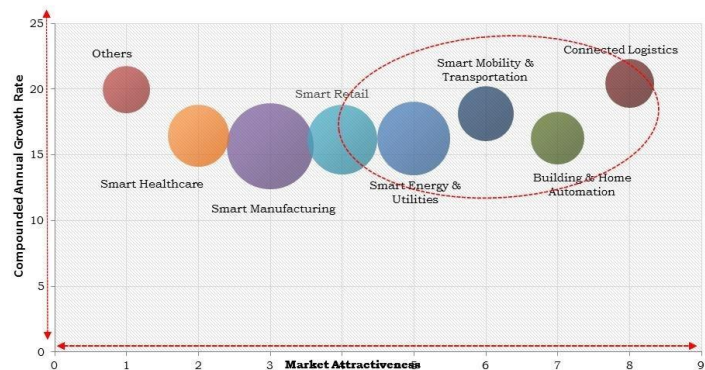


Figure 3: Europe IoT Data Management Market – Key Segments

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)	<b>Page:</b>	28 of 126
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2
		<b>Status:</b>	Final version

Finally, an indirect approach to the market segmentation with a fine-grained domain selection can specifically target the main beneficiaries of SMESEC development. This approach can be done from both vertical and horizontal perspective to create precise market segmentation both in market domains and technology areas:

### 3.1.1.1 Vertical segmentation

The **vertical segmentation** offers goods and services to a specific industry, business, or a group of customers with similar needs. On the other hand, **horizontal segmentation** offers a broad range of goods and services to a wider group of customers with a wide range of needs.

On the **vertical axis** for this project, there are 4 main markets targeted which correspond to the 4 project pilots, as it is essential to provide proven results that our solution enhances different types of SMEs operating in a range of market sectors and offering diverse products and services, against threats and risks introduced by the recently adopted ICT advances:

- Smart-City.
- Industrial Internet of Things (IIoT).
- e-Voting.
- Smart Grids.

#### 3.1.1.1.1 (Industrial) IoT



INTERNET OF THINGS - IIoT. Image source: www.unsplash.com

Market size in 2022 :  
561.04 USD Billion

Growth rate : 26.9%

Estimated number EU  
SMEs : 2 074 010

Estimated EU SMEs  
market share : 35%  
(64.83 USD Billion)

Type of SMEs :  
Consulting, System  
integrators,  
Application providers

*“Solutions aim to detect and prevent possible risks to structures and infrastructures by monitoring their operations and status in real time. These solutions are essential for ensuring that the assets’ operations are maximally optimal, safe and cost competitive”<sup>1</sup>.*

<sup>1</sup> Grant Agreement-740787-SMESEC

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)	<b>Page:</b>	29 of 126
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2
		<b>Status:</b>	Final version



### 3.1.1.1.2 Smart city



SMART CITY. Image source: www.unsplash.com

Market size in 2022 : 1.201 USD Billion

Growth rate : 23.1%

Estimated number of EU SMEs : 708 971

Estimated EU SMEs market share : 50% (285 USD Billion)

Type of SMEs : Start ups, Hardware manufacturers, Application developers

*“Provides the tools that activate citizen's creativity, imagination and communication, engages urban thinking and improves the relationship between citizens, the city municipality and city's public services. With their own communication devices (mobile phones) or via an application, citizens can post in real time issues and problems for something that happens in their city and inform their fellow citizens as well as the municipality for problems and incidents that occur every moment”<sup>2</sup>.*

### Smartgrid



SMART GRID. Image source: www.unsplash.com

Market size in 2022 : 50.65 USD Billion

Growth rate : 19.4%

Estimated number EU SMEs : 14 739

Estimated EU SMEs market share : 46% (5.56 USD Billion)

Type of SMEs : Consulting, System integrators, Application providers

Similar fields : Water, Gas, Oil

*“Energy networks that can automatically monitor energy flows and adjust to changes in energy supply and demand accordingly. When coupled with smart metering systems, smart grids reach consumers and suppliers by providing information on real-time consumption”.*

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)	<b>Page:</b>	30 of 126
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2
		<b>Status:</b>	Final version

*“They can also help to better integrate renewable energy and also open up the possibility for consumers who produce their own energy to respond to prices and sell excess to the grid”[6]*

### 3.1.1.1.3 E-Voting



E-VOTING. Image source: [www.unsplash.com](http://www.unsplash.com)

Estimated number EU SMEs : around 34

Type of SMEs : Consulting, System integrators, Application providers

One of the most critical environments from the point of view of security is the electoral processes. To ensure privacy and integrity of the votes, electronic voting systems usually implement advanced cryptographic protocols at application level by implementing end-to-end encryption and verifiability of the election results, which detects if there have been any attacks. However, these measures do not prevent possible attacks<sup>3</sup>.

As a niche market, there is no accurate and updated information about the market size. Based in Austria, E-Voting.CC provides a long list of key players. This is not an exhaustive list but the evoting activity seems to count about 50 companies [7]

In addition, with legal and political constraints, for a real development, the security aspects remain the first barrier. Trust and acceptance cannot be gathered without a strong guarantee in security, privacy and transparency in the voting process. The needed security level is such that the end to end security is a must to ensure reliability of voting activities. This implies security measures for data, system, transactions, VPN and associated networks.

### 3.1.1.1.4 Other fields

To extend these vertical axis, other areas can also be mentioned as part of the initial segmentation to keep them on the radar as emerging markets. Apart from the four pilots, SMESEC will organize an **Open Call** in the final year of the project to invite more SMEs operating in diverse contexts, offering various kinds of services and products. This open call will allow SMESEC to collect additional evaluation results and make the necessary adjustments towards a robust and flexible security framework capable of supporting companies and organizations with a limited budget. This first focus on pilots aims to start

<sup>3</sup> Grant Agreement-740787-SMESEC

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)		<b>Page:</b>	31 of 126
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b> Final version

the SMESEC awareness, approaching market players with a vertical validated framework. That is a first step and the consortium will progressively extend to other fields. The following Figure 4 gives the number of SMEs in Europe depending on their activity sector.

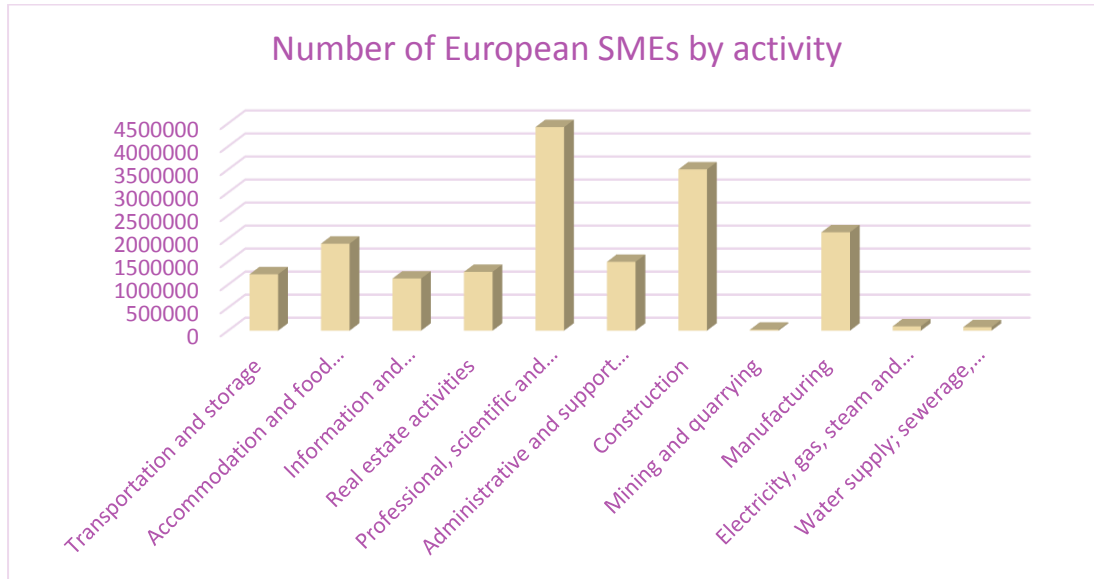


Figure 4: SMEs landscape in Europe by activity – Source: Own creation/ Eurostats data

This combined approach (vertical and horizontal) try to investigate the wider SMEs audience and also refers to the way the SMESEC identified solutions for market needs. This is confirmed by the latest Eurosmart report on IoT security where some best practices are disseminated. Figure 5 shows the preconized action canvas.

**Per sector/application perform:**

- Architecture model
- Policies & procedures
- Risk assessment
- Privacy impact assessment

**Security requirements**

**Security functions:**

- Technical requirements
- Security level

**Major vertical common needs:**

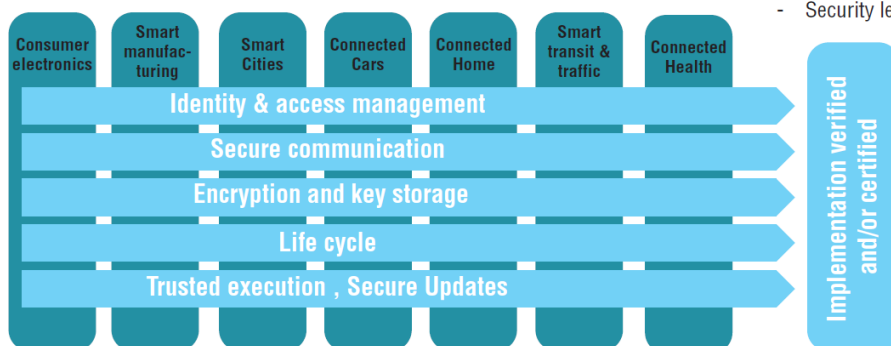


Figure 5: Best practices approach for security development – Source Eurosmart report

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)	<b>Page:</b>	32 of 126
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2
		<b>Status:</b>	Final version



### 3.1.1.2 Horizontal segmentation

The **horizontal axis** will include all main security product areas SMESEC aims to provide a service as part of the project scope:

- User Entity Behaviour Analytics (UEBA).
- Cloud Access Security Brokers (CASB).
- Endpoint Detection and Response (EDR).
- Deception technology.
- Secure Web Gateway.
- Application security testing.
- Endpoint Protection Platform (EPP).
- Web application platform.
- Distributed DDoS.
- Intrusion detection and prevention systems.
- Security Information and Event Management (SIEM).
- Unified threat management.
- Governance, risk management and compliance.
- Other.

An extensive analysis on these traditional and emerging markets has been carried out in another project deliverables (**D2.1** SME security characteristics description, security and market analysis and **D6.1** Dissemination plan and market analysis)

Those areas are susceptible to be reviewed and modified (add or remove) along the project's lifetime as the impact for targeted SME's could vary or even the obtained results could show there is not a viable transfer to market with a significant economic impact.

### 3.1.2 PEST analysis

An initial P.E.S.T analysis has been carried out around the SMESEC framework adoption (see Table 6). As result of this analysis, several barriers and obstacles have been identified with a direct impact on the project's achievement (as initially mentioned in the grant agreement document<sup>4</sup>).

The first barrier is the **traditional working method**, which still exists in many SMEs. It is not only an issue of technological support but a socio-economical challenge. Such barrier can be smoothed with a set of measures mentioned below that will be supported through the SMESEC results.

<sup>4</sup> Grant Agreement number: 740787 — SMESEC — H2020-DS-2016-2017/H2020-DS-SC7-2016

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)		<b>Page:</b>	33 of 126
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b> Final version

	Description
<b>Political</b>	New requirements through regulations could have an impact on the technical solutions developed in the SMESEC project e.g. EU policies for privacy, data protection (as direct impacts on the materialization of benefits for industrial partners). There are no known regulations or standards at this time that restrict/limit or prohibit the use of the proposed technology in Europe.
<b>Economical</b>	<p>SMESEC puts a considerable emphasis on all inputs to be collected from businesses and markets in order to orient the implementation. This will drive the project to focus the implementation into the more important requirements which represent the specific market's needs. Since security solutions are most of the time seen as an added cost without providing new business opportunities, SMESEC will study this barrier in two levels:</p> <ul style="list-style-type: none"> <li>• Costs for the provided security products/services.</li> <li>• Provide necessary examples and proofs of the negative economic impacts that potential cyber-attacks have on businesses.</li> </ul>
<b>Social</b>	Reluctance to new technology acceptance (from awareness to economic concerns) would have a significant impact on SMESEC adoption. On the other hand, concerns on security, specifically in terms of access to sensitive information, may represent an important obstacle for proper adoption of SMESEC solutions. Since security is not only a technological issue but also involves several organizational and procedural issues, SMESEC also plans to provide security guidelines addressing this purpose. The collaborative approach proposed by SMESEC naturally faces one of the most basic pre-conditions for any collaborative work: the <b>trust building</b> . Another societal barrier is human understanding of what SMESEC is building, and how to ensure this project has a common understanding, especially given the number of disciplines involved.
<b>Technological</b>	<p>SMESEC pays extreme attention to the interoperation of all kind of modules playing a role within the cyber-security environment. Support of existing and proposed standards is mandatory in order to guarantee the full integration and features of all relevant components and interaction with external systems. Non-adoption of these standards would frustrate or prevent connections to some devices or external software and systems, or loss of features, thus impacting business potential and revenue. Following, we summarize technological barrier in a list of important issues:</p> <p><b>1-Replicability of proposed solutions for different domains:</b> SMESEC solutions will be tested in the pilot activities but also in the exploitation activities that will engage potential early adopters and stakeholders across Europe as soon as possible (moving from pilot solutions to additional local/regional testing-SMESEC has an open call in scope to extend the framework adoption).</p> <p><b>2-Complexity for the technicians:</b> The proposed solutions will have to be managed by technician staffs of generic SMEs, which are not security experts. SMESEC will define user-friendly tools in order to facilitate their use and understanding.</p> <p><b>3-Interoperability and standard solutions:</b> SMESEC will cope with a large diversity of components/subsystems developed using different technologies; the adoption of interoperable mechanisms is expected to lower this obstacle, which nevertheless cannot be underestimated.</p>

**Table 6 : P.E.S.T Analysis of SMESEC framework [14]**

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)	<b>Page:</b>	34 of 126
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2
		<b>Status:</b>	Final version

### 3.1.3 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. Inputs of this analysis are detailed in FireCompass.com [8] and include the main strengths and weaknesses of each of the tool identified providing valuable information on the internal analysis of the market.

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 behavior-based anomaly detection; Not flexible alerting
	LogRhythm	LogRhythm	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	It doesn't include support for custom meta-data fields, log normalization, support for statistical-based and heuristic

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)	<b>Page:</b>	35 of 126
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2
		<b>Status:</b>	Final version

Market	Name of competitor solution	Company	Strengths	Weaknesses
				correlation. Additionally, it doesn't include 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
	Symantec	Symantec	Very good detection	Botnet detection; Restricted investigation;
Application Security Testing	Fortify	HPE	Excellent static and dynamic analysis; Excellent mobile 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	It doesn't include 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

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)	<b>Page:</b>	36 of 126
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2
		<b>Status:</b>	Final version

Market	Name of competitor solution	Company	Strengths	Weaknesses
				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 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 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,	No ticketing system integration and contract management; No

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)	<b>Page:</b>	37 of 126
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2
		<b>Status:</b>	Final version

Market	Name of competitor solution	Company	Strengths	Weaknesses
			Incident management;	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;
	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 defense; No shadow IT discovery
	Web Security Appliance	Cisco	Malware protection; Integrations; Deployment options;	No Botnet defense; No compliance reporting templates; No hybrid (on-prem, cloud) offering
	Web Security	McAfee	Web Traffic control; DLP; Deployment options	Botnet defense; Mobility support for Web Traffic Control
	Web Security	Symantec	Botnet and malware defense; deployment options	Fewer integrations; no cloud-based sandboxing
	SWG	TrustWave	Malware protection; Web Traffic Control; DLP;	No Botnet defense; No shadow IT discovery; No Cloud or Hybrid deployment support

**Table 7: Competition matrix**

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)	<b>Page:</b>	38 of 126
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2
		<b>Status:</b>	Final version

### 3.1.4 Stakeholders analysis

One of the standard analysis to be carried out in a market analysis is the stakeholder one. The key activities to perform on this subject include:

- Identify the stakeholders.
- Get a deeper understanding of the various identified stakeholders 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, it would be beneficial to directly interact with stakeholders and to reevaluate the analysis and potentially consider a more mature Stakeholder Model. As part of this initial approach during year 1, a strong dissemination activity plan has been prepared which include workshops and presentation in the main project-related events.

The methodology proposed for this stakeholder mapping is based on the Mendelow's matrix (Power / Interest Matrix)[9]

At this initial stage the SMESEC project has identified three main stakeholders' groups:

- **Active 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.).
- **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-).
- **Internal stakeholders** involved in the development and establishment of SMESEC (consortium partners).

At this initial stage of the project, this is the first approach to the distribution of the stakeholder the consortium is considering, as illustrated in the Figure 6, however, as a living document this matrix could be updated with the feedback obtained from the dissemination activities carried out during the forthcoming months.

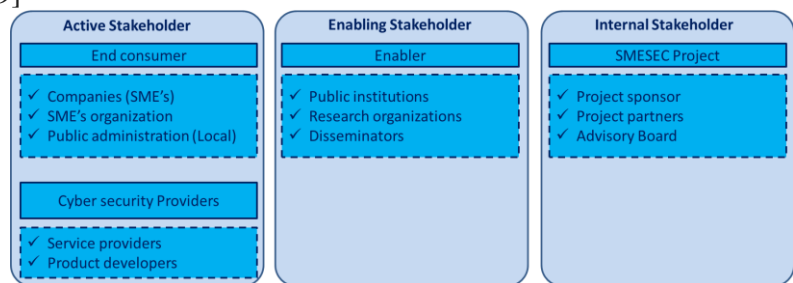


Figure 6: Identification of SMESEC stakeholders[8]

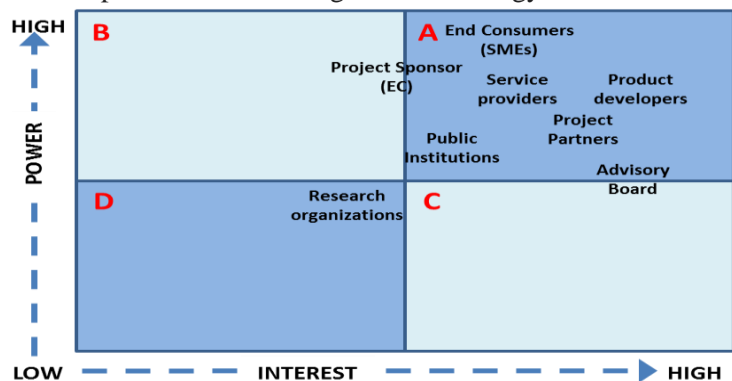


Figure 7: Stakeholders distribution

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)	<b>Page:</b>	39 of 126
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2
		<b>Status:</b>	Final version



## 3.2 Business Model

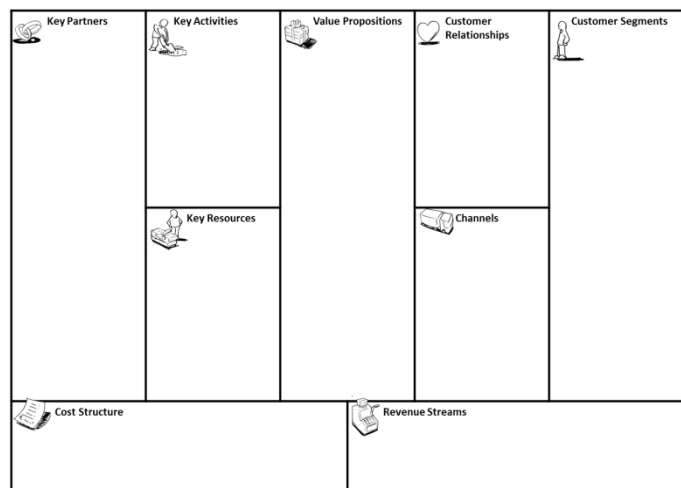
### 3.2.1 SMESEC Framework Business Model Canvas

This section in deliverable D6.2 is a preliminary version of the prospective business plan, therefore the business model presented below takes on a more general and theoretical perspective.

However, in the final version of this deliverable, due at the end of the project, it is planned to present an overview of exploitable items and to decide upon the most relevant to present potential business plans for them. Further, each pilot would also produce a business plan and present it in the final deliverable.

“A business model describes the rationale of how an organization creates, delivers, and captures value”<sup>5</sup>

As part of the SMESEC overall business plan, the Consortium has prepared 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 help



transform the innovation of SMESEC into tangible market uptake prospects in targeted market segments.

**Figure 8: Business Model Generation, Alexander Osterwalder**

As a living document, the business plan will act as a continuous reference to ensure that the technical dimension, as it evolves, will fully focus on short and mid-term market needs and to prepare an effective products and services launch once the project is finished. In this sense, we aim to follow an effective innovation roadmap that takes the initial ideas generation towards market positioning for business creation that addresses needs of SMEs.

As part of this initial approach, an initial draft version of the SMESEC framework is under discussion.

At a later stage of the project and in order to better accommodate to the specific market needs, **BMC per component could be developed.**

<sup>5</sup> Business Model Generation, Alexander Osterwalder, Yves Pigneur, Alan Smith, and 470 practitioners from 45 countries, self published, 2010

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)	<b>Page:</b>	40 of 126
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2
		<b>Status:</b>	Final version





<b>Key Partners 8)</b>  1 ATOS 2 WOLDSENSING 3 UoP (Patras) 4 FORTH 5 EGM 6 SCYTL 7 GRIDPOCKET 8 FHNW 9 CITRIX 10 IBM 11 BITDEFENDER 12 UU (Utrecht)	<b>Key Resources 7)</b>  ➤ Persons ➤ Knowledge ➤ Software/Hardware ➤ Sales force	<b>Value proposition 1)</b>  ➤ Encryption ➤ Governance, Risk Management and Compliance (GRC) ➤ Data Loss Prevention ➤ Unified Threat Management (UTM) ➤ Security Information and Event Management (SIEM) ➤ Intrusion Detection and Prevention System (IDS/IPS) ➤ Distributed Denial-of-Service mitigation (DDoS) ➤ Business Continuity / Disaster Recovery ➤ Web Application Firewall (WAF) ➤ Secure Web Gateway (SWG) ➤ Application Security Testing ➤ Security Awareness and Training ➤ Endpoint protection platform (EPP) ➤ Deception technology ➤ Endpoint Detection and Response (EDR) ➤ Cloud Access Security Brokers (CASB) ➤ User Entity Behaviour Analytics (UEBA) ➤ Identity & access management (IAM)	<b>Customer relationship 4)</b>  ➤ Personal assistance ➤ Self-service ➤ Automated services ➤ Communities ➤ Co-creation	<b>Customer segment 2)</b>  <b>1-Vertical approach</b>  ➤ Smart-City ➤ Internet of Things (IoT) ➤ e-Voting ➤ Smart Grids  <b>2-Horizontal approach</b>  ➤ Technology providers ➤ Services providers ➤ Direct end users
<b>Cost structure 9)</b>  Fix Variable		<b>Revenue Streams 5)</b>  One-Time Recurring		

**Table 8 : Business Model Canvas for SMESEC framework**

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization (Year 1)	<b>Page:</b>	41 of 126
<b>Dissemination:</b>	PU	<b>Version:</b>	1.2
		<b>Status:</b>	Final version



### 3.2.2 Value proposition

The Value Proposition describes the group of products/services that create an added value for a specific Customer Segment. The Value Proposition is the reason why customers are **willing to pay for a specific product**. It solves a customer problem or satisfies a customer need.

In the specific case of SMESEC “Protecting Small and Medium-sized Enterprises digital technology through an innovative cyber-SECurity framework” which includes the following components:

- Encryption
- Governance, Risk Management and Compliance (GRC)
- Data Loss Prevention
- Unified Threat Management (UTM)
- Security Information and Event Management (SIEM)
- Intrusion Detection and Prevention System (IDS/IPS)
- Distributed Denial-of-Service mitigation (DDoS)
- Business Continuity / Disaster Recovery
- Web Application Firewall (WAF)
- Secure Web Gateway (SWG)
- Application Security Testing
- Security Awareness and Training
- Endpoint protection platform (EPP)
- Deception technology
- Endpoint Detection and Response (EDR)
- Cloud Access Security Brokers (CASB)
- User Entity Behaviour Analytics (UEBA)
- Identity & access management (IAM)

### 3.2.3 Customer Segment

This building block defines the **different groups** of people or organizations that are our **target** market in order to provide SMESEC as a product/service? For whom are we creating value? Who are our most important customers?

In order to better satisfy customers, this building block groups them into different segments with common needs, common behaviours, or other attributes.

Vertical approach

In this market segmentation, the offer of goods and services are specific to an industry or group of customers with specific needs. In SMESEC particular case, this is related to the project pilots industries:

- Smart-City
- Internet of Things (IoT)
- e-Voting
- Smart Grids

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization			<b>Page:</b>	42 of 126	
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b> Final version

## Horizontal approach

In this market segmentation, the products or services meet the need of a wide range of customers across different sectors. In SMESEC particular case, this is related to:

- Technology providers
- Services providers
- Direct end users

### 3.2.4 Channels

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

- Own (from a web site to company's own sales force).
- Partner (from stores-retail or wholesale- to partner's web sites).
  - Direct. Where the consortium distributes SMESEC product or services directly to the customers.
  - Indirect. The distribution of products or services is partially or totally carried out by an external partner.

### 3.2.5 Customer Relationships

Types of relationships we establish with the specific Customer Segments. What type of relationship does each of our Customer Segments expect from us? Are they cheap or expensive?

- Personal assistance. There is a direct interaction between customer and the company
- Self-service / Automated services. The customer has at his disposal all means to help himself.
- Communities. Which allow knowledge and experience exchange between users.
- Co-creation. Enhancing the product functionalities via feedback from customer/users.

### 3.2.6 Revenue streams

How will we be **generating cash** from each customer segment defined. Are they all willing to pay the same? What value has each product or service? What is the value proposition that customers are willing to pay?

One-time

- Asset selling
- Components selling

Recurring

- Fee structure (subscription, usage, broker,)
- Licensing
- Advertising

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization			<b>Page:</b>	43 of 126		
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version

### 3.2.7 Key activities

Which are the most important things we have to do to make this business model work? What is required to make our Value Propositions available to our customer segments/distribution channels/customer relationships/revenue streams?

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

### 3.2.8 Key Resources

Which are the most important **assets required** (by our Value Propositions, Distribution Channels, Customer Relationships, Revenue Streams,...) to make a **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...)

### 3.2.9 Key Partners

- Public/Semipublic sector
  - EC (European Commission)
  - FORTH
- Private sector
  - ATOS
  - EGM
  - WOLDSENSING
  - IBM
  - CITRIX
  - BITDEFENDER
  - BYTEMOBILE
  - SCYTL
- Academic sector
  - UoP
  - UU
  - FHNW

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization			<b>Page:</b>	44 of 126	
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b> Final version

### 3.2.10 Cost Structure

The Cost Structure describes all costs incurred to operate business activities. What are the most important costs inherent in our business model? Which Key Resources are most expensive? Which Key Activities are most expensive?

Fix (Remain the same regardless of the volume produced)

- Salaries (administration, outsourcing,)
- Utilities (electricity, gas, water, phone, internet,)
- Rents (premises, offices,)
- Transport
- Communication
- Maintenance
- Amortizations, Fees (Local, State)
- Other

Variable (Heavily dependent on the volume of output generated).

- Salaries (Direct)
- Sales Fees
- Taxes
- Others

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization			<b>Page:</b>	45 of 126		
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version

## 4 Project dissemination

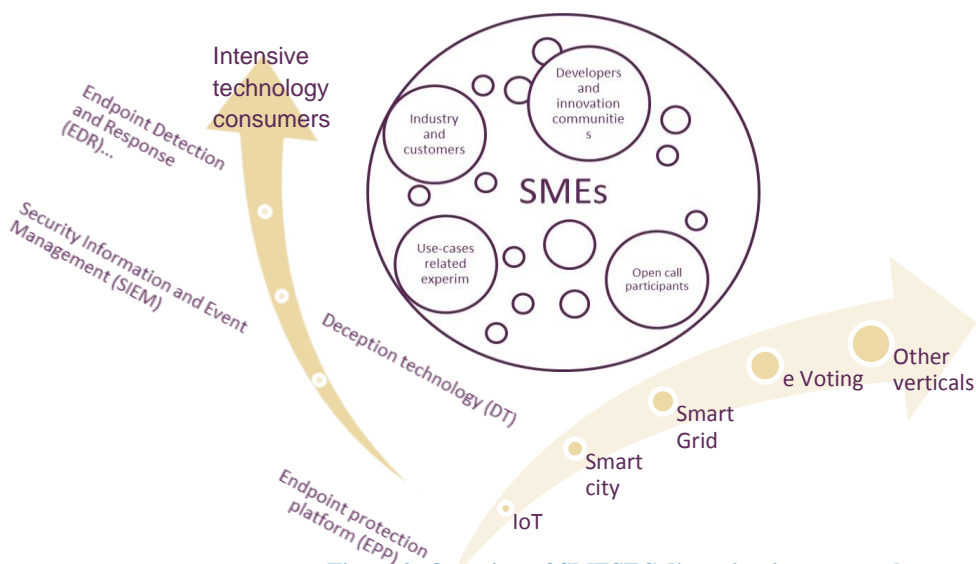
The SMESEC scope implies, as a cybersecurity project, a wide range of actors and stakeholders that the consortium will involve in its dissemination activities. Targeting primarily SMEs, the project will reach a wide range of satellite stakeholders such as SMEs organizations, sister H2020 projects, local and cybersecurity specialists representatives. Developed in the previous deliverable D6.1, released at month 6, the consortium validated the initial dissemination plan and fine tune in this deliverable its strategy adding complementary information and details of actions developed in the task T6.2, animating the network of contacts of each entity to reach end-user communities (including SMEs), the public sector, and the wider public.

The section here describes the project dissemination performed during M1-M12 according to the overall strategy as depicted in Figure 9, the channels used for dissemination, the dissemination kits and artefacts, and the dissemination process and monitoring for Year 1. The remaining years will be described in the deliverables D6.3 at M24 and D6.4 at M36.

### 4.1 Dissemination strategy

#### 4.1.1 Global approach and phasing

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.

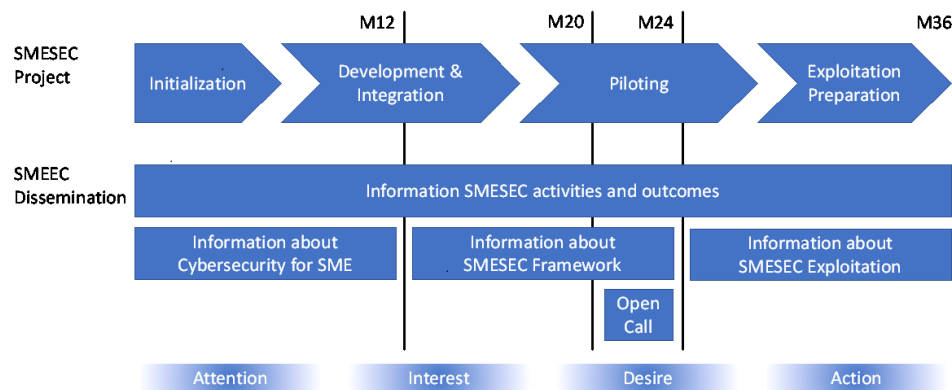


**Figure 9: Overview of SMESEC dissemination approach**

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	46 of 126
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU
		<b>Version:</b>	1.2
		<b>Status:</b>	Final version

As presented in Figure 9: Overview of SMESEC dissemination approach, 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.

Figure 10: 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.



**Figure 10: Dissemination plan**

#### 4.1.2 Objectives

The dissemination objectives are shown in Figure 11. From a short-term view, dissemination firstly intends to ensure a proper communication of all project outcomes and generates project awareness and attractiveness towards future users, SMEs, etc. From a mid-term view, these actions will support standardisation and exploitation activities and trigger the adoption and implementation of SMESEC security framework while ensuring the wider project audience.

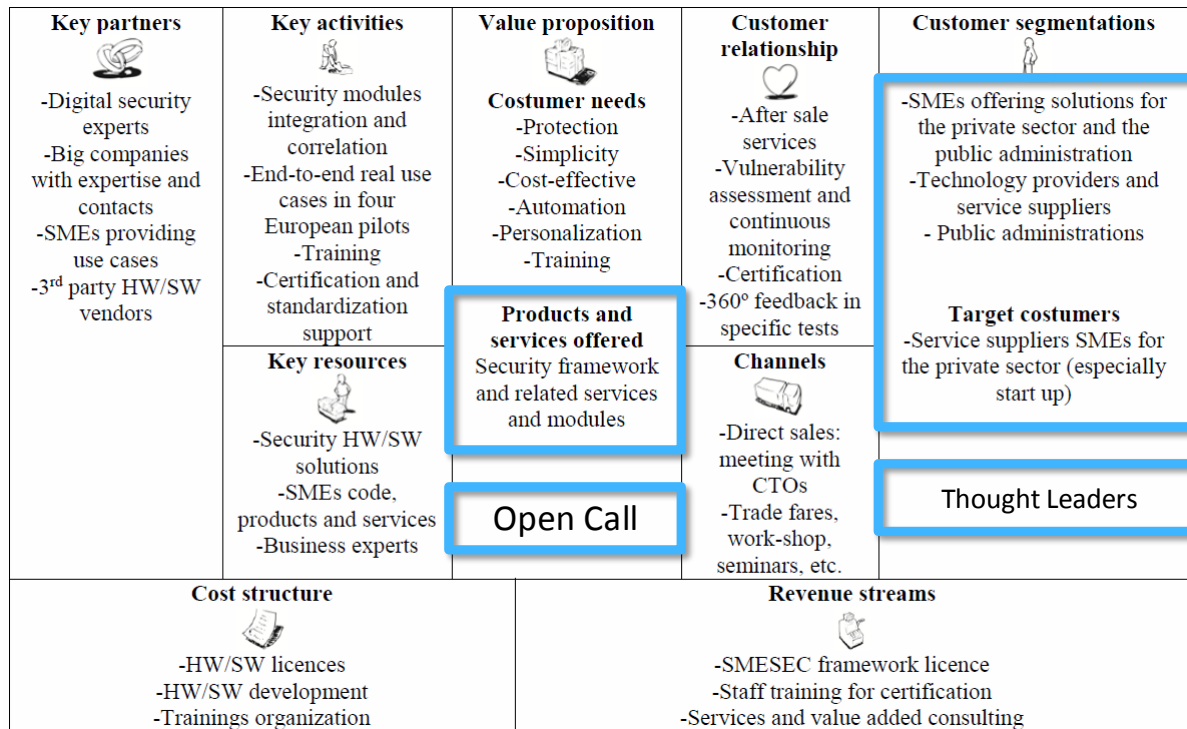


**Figure 11: Overview of SMESEC dissemination objectives**

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	47 of 126	
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	
	<b>Version:</b>	1.2	<b>Status:</b>	Final version

### 4.1.3 Targets

The dissemination performed by the SMESEC project is primarily intended to support the validation and exploitation of the SMESEC framework according to the SMESEC business model. For dissemination, a particularly important validation activity will be the open call. Figure 12 gives an overview of the SMESEC business model.



**Figure 12: SMESEC business model (thick blue frames: priorities for dissemination).**

Table 9 shows the target audiences that the SMESEC dissemination is trying to reach. The target audiences will be addressed with refined messages based on the market and stakeholder segmentation described earlier in this document. The focus of SMESEC dissemination is small and medium-sized enterprises. That target is prioritised over the other target.

Target	Dimension	Segments	Information needs	Desired outcomes
SME	Size	Small	Goal-Oriented Hardening of a Digital Offering	Use and endorse SMESEC Framework
		Medium-sized	Goal-Oriented Cybersecurity in the Organization	
	Maturity	Start-up	Top-10 Hardening of a Digital Offering	

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization			<b>Page:</b>	48 of 126
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2
				<b>Status:</b>	Final version



Target	Dimension	Segments	Information needs	Desired outcomes
	Domain	Established	Sustaining Cybersecurity for whole Digital Portfolio	
		IoT	IoT-Specific Chapters	
		Smart Cities	Smart City-Specific Chapters	
		Other	Other Domains	
OSS	Product	Cybersecurity	How to bring OSS to SMEs	Integrate SMESEC Framework
		Other	Top-10 Hardening of a Digital Offering	Integrate SMESEC Framework
Academia	Discipline	Cybersecurity	Cybersecurity innovations	Papers and citations
		Technology	Technology-oriented communities	
		Engineering	Security engineering for SMEs	
Policy	Region	EU, CH, Israel	Policy recommendations	Encourage SMESEC cybersecurity practice.
R&I	Region	EU, CH, Israel	Recommendations for economic development	Calls allowing SMESEC to mature and grow.
Individuals	Specialization	Opinion Leaders	Business-enablement with SMESEC.	Inform about SMESEC Framework
		Employees	SME protection and safety with SMESEC.	Use and endorse SMESEC Framework
		Public	Trust in protected SMEs.	Positive attitude towards SMESEC
Standardization	Body	ETSI, IETF		Use SMESEC Results in Standards

**Table 9: Dissemination target groups**

#### 4.1.4 Dissemination Messages

SMESEC started to implement the dissemination with a series of contents or stories that are kept consistent across channels. For the year 1, they include Cybersecurity problems for SMEs, SMESEC framework vision, and interviews with stakeholders.

The dissemination messages have been stable with just small modifications during year 1. Table 10: Dissemination message shows the message to be communicated by SMESEC dissemination.

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization			<b>Page:</b>	49 of 126
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2
				<b>Status:</b>	Final version

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"> <tr> <td>DoS and DDoS Vulnerable Software Broken Authentication Misconfigurations Injection</td> <td>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		
SMESEC Framework	SMESEC offers a lightweight cybersecurity framework for thorough protection, including.... ...Awareness & Training Tutorials ...Vulnerability Discovery & Resolution Tools ...Definition & Recommendation Tools ...Threat Protection & Response Tools ...Lessons from Testing & Validation		
SMESEC Methodology	Framework Tested on Real-World SMEs in... ...IoT ...Smart City ...Smart Grid ...e-Voting ...Digital Start-ups		
Advantages of SMESEC	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 the company instead of complicated formal policies and procedures		

**Table 10: Dissemination message**

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.

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	50 of 126				
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version

### 4.1.5 Project branding

The dedicated logo was slightly adapted to fit the visual language (Figure 13).



Figure 13: SMESEC logo

#### Logo

The logo-icon associates a padlock symbolizing security concept with urban building profiles. Both elements refer to smart cities and IoT use cases.

The icon should be used in combination with the logotype, and positioning as well as proportions of the two items shouldn't be modified. The logo should always be placed on light backgrounds leaving sufficient whitespace (approx. the width of diameter of the hexagon on all sides).

A black & white version as well as an inverted version are available for monochrome application of the logo.

The color palette was slightly adapted, and color gradients introduced (Figure 14).

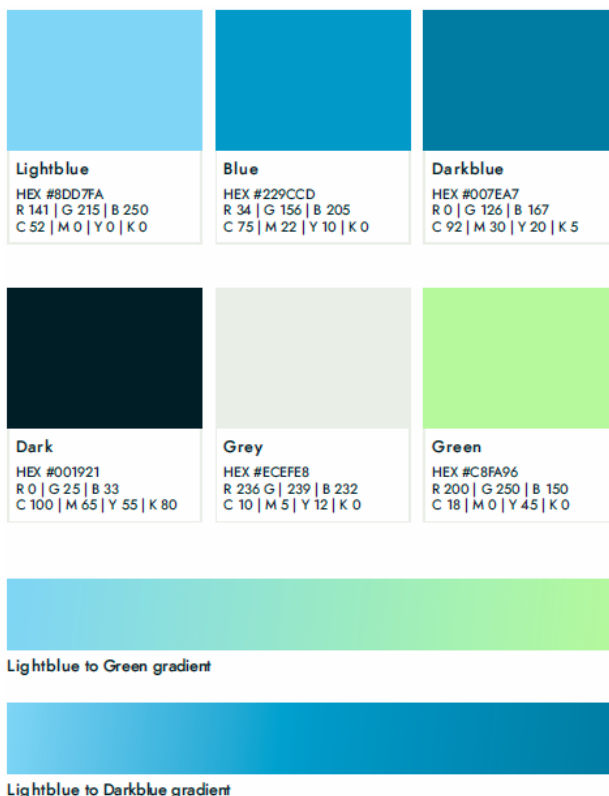


Figure 14: SMESEC colour palette

#### Colors & Gradients

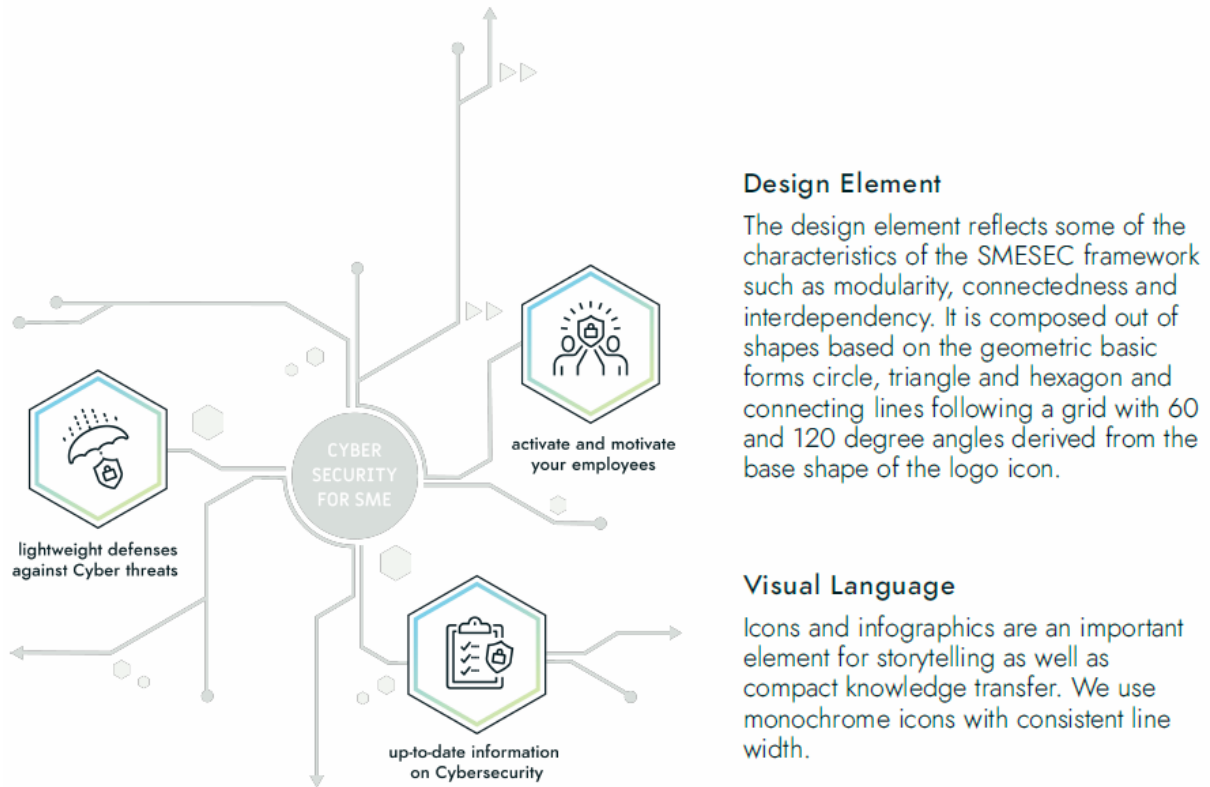
SMESECs goal is to deliver lightweight Cybersecurity for thorough protection. In order to convey this mission also through its visual identity, the use of much white space and some light grey tones is highly recommended.

The main colors are bluetones which represent attributes such as trust, confidence, integrity and responsibility.

The green accent colour standing for change, health and growth should exclusively and purposefully be applied to put greater emphasis on matters of highest importance. The use of gradients serve this purpose.

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	51 of 126	
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	
	<b>Version:</b>	1.2	<b>Status:</b>	Final version

New design elements and a visual language for the SMESEC storyline were introduced (Figure 15). This design is intended to be used by SMESEC tools, providing continuity from the awareness-generating webpage and dissemination kits to the SMESEC framework.



**Figure 15: SMESEC design elements and visual language.**

A consistent, extensible set of icons was created to communicate the SMESEC ideas and concepts intuitively. These icons may be combined into infographics that reflect the digital, connected domain that is affected by cybersecurity, pointing to the hotspots/buttons that allows the visitor to benefit from the SMESEC value propositions.

### Cybersecurity for SME



<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	52 of 126	
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	
	<b>Version:</b>	1.2	<b>Status:</b>	Final version

### The SMESEC Framework



### Benefits from using the SMESEC Framework



### Cyber threats to SMEs

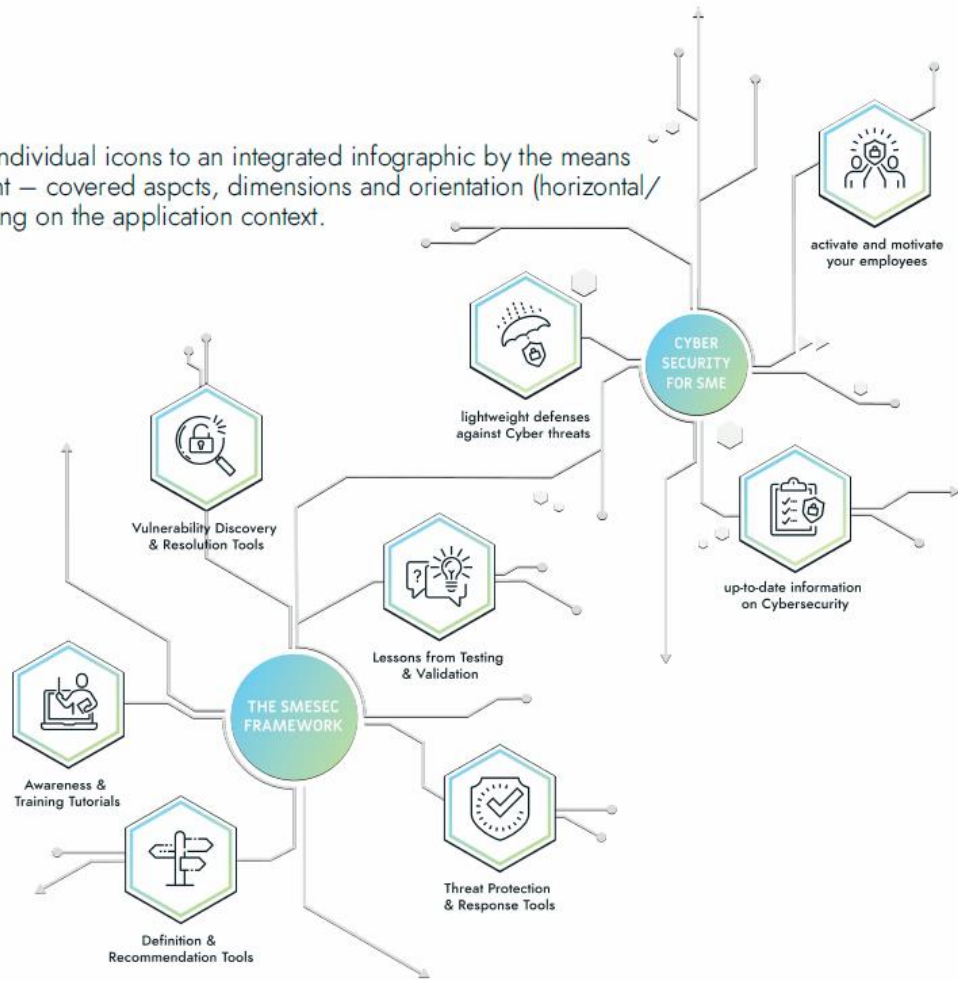


Figure 16: SMESEC icons.

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	53 of 126	
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	
	<b>Version:</b>	1.2	<b>Status:</b>	Final version

### Infographics

Combination of the individual icons to an integrated infographic by the means of the design element – covered aspects, dimensions and orientation (horizontal/vertical) are depending on the application context.



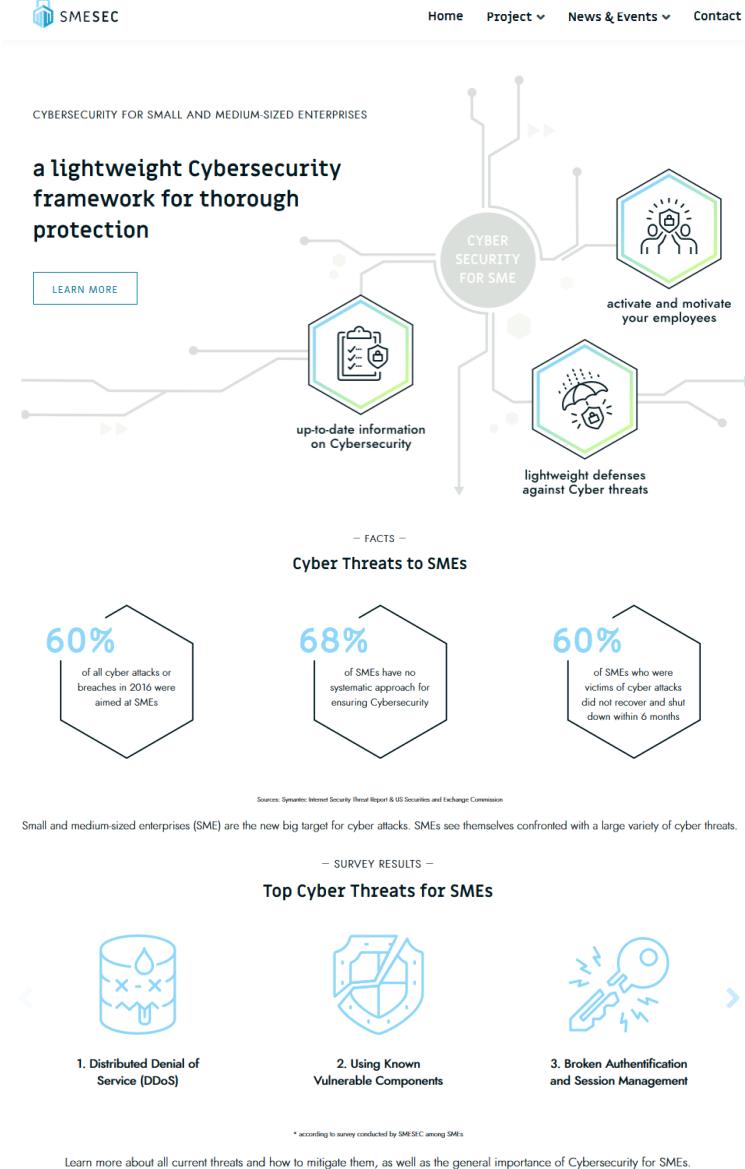
**Figure 17: SMESEC infographics.**

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	54 of 126	
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	
	<b>Version:</b>	1.2	<b>Status:</b>	Final version

## 4.2 Dissemination tools

### 4.2.1 Public Website

The SMESEC message was placed on the public web [www.smesec.eu](http://www.smesec.eu) by following the visual language:



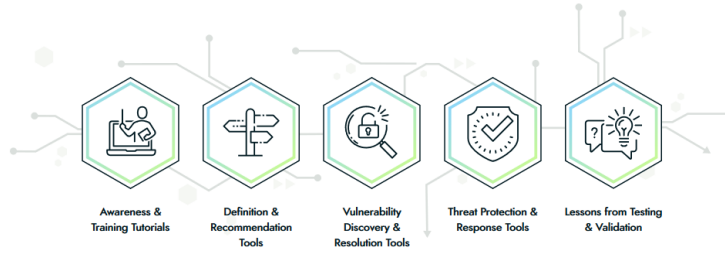
The screenshot displays the SMESEC website layout. At the top, there is a navigation bar with the SMESEC logo and links for Home, Project, News & Events, and Contact. The main content area features a central graphic titled "CYBER SECURITY FOR SME" with three key components: "up-to-date information on Cybersecurity", "activate and motivate your employees", and "lightweight defenses against Cyber threats". Below this, a "FACTS" section highlights three statistics: 60% of all cyber attacks or breaches in 2016 were aimed at SMEs; 68% of SMEs have no systematic approach for ensuring Cybersecurity; and 60% of SMEs who were victims of cyber attacks did not recover and shut down within 6 months. A source is cited as "Sources: Symantec Internet Security Threat Report & US Securities and Exchange Commission". A paragraph states: "Small and medium-sized enterprises (SME) are the new big target for cyber attacks. SMEs see themselves confronted with a large variety of cyber threats." Below this, a "SURVEY RESULTS" section lists the "Top Cyber Threats for SMEs": 1. Distributed Denial of Service (DDoS), 2. Using Known Vulnerable Components, and 3. Broken Authentication and Session Management. A footnote indicates: "\* according to survey conducted by SMESEC among SMEs". A final line of text reads: "Learn more about all current threats and how to mitigate them, as well as the general importance of Cybersecurity for SMEs."

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	55 of 126	
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	
	<b>Version:</b>	1.2	<b>Status:</b>	Final version



– SOLUTION –

### The SMESEC framework



SMESEC is a lightweight Cybersecurity framework for protecting small and medium-sized enterprises (SME) against Cyber threats. As an SME, you find vulnerabilities and address them with simple tutorials, tools, and lessons-learned – all by yourself.

– RATIONALE –

### Benefits from using the SMESEC framework



#### 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

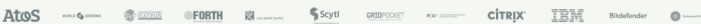



#### Keep it simple

Practices adapted to your company instead of complicated formal policies and procedures

The SMESEC consortium understands the SMEs environment, which may be busy, hectic, and diverse. SMESEC will offer a framework that is based on up-to-date information about Cybersecurity facts and events and makes Cybersecurity available to all employees. The SMESEC framework will allow an SME to build Cybersecurity itself, require just little investment, and avoid complicated formal policy and procedures. The use of the SMESEC framework will make Cybersecurity accessible for SME and help to prevent and mitigate cyber risks of a large part of the European economy.

#### Consortium Members






The project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 440191 (SMESEC). This work is supported by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 13.00009. The opinions expressed and arguments employed herein do not necessarily reflect the official views of these funding bodies.

© 2017 SMESEC Consortium | Design | hosted by HYBM

#### FOLLOW US



#### LATEST NEWS

Atos promotes SMESEC

University of Patras presents SMESEC project at the 1st Workshop of SAINT project in Athens

Project Management Board Meeting in Haifa

[News Archive](#)

**Figure 18: SMESEC webpage (main landing page).**

The website offers the following information architecture, outlining the sub-webpages. Preference was given to simplicity, hence communicating the lightweight nature of SMESEC cybersecurity.

<b>Home</b>	<b>The Framework</b> > Cyber Security (explain why Cybersecurity is important for SME (expert view), infos about threats, in particular those relevant for IoT & Smart city, interviews with partner SMEs and link to solutions) > SMESEC Framework (explain the Components, Capability improvement, Value/Benefits...)	<b>The Project</b> > About SMESEC > Consortium > Publications > Deliverables	<b>News &amp; Events</b> > News > Upcoming Events > Subscribe (Newsletter/RSS) > Beta Tester Signup > Media Kit	<b>Contact</b>
-------------	---	--	--	----------------

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	56 of 126
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU
	<b>Version:</b>	1.2	<b>Status:</b> Final version



Figure 19: SMESEC information architecture.

### 4.2.2 Printed materials

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 priority of the booth has been reduced by the SMESEC partners. It will be created upon demand.

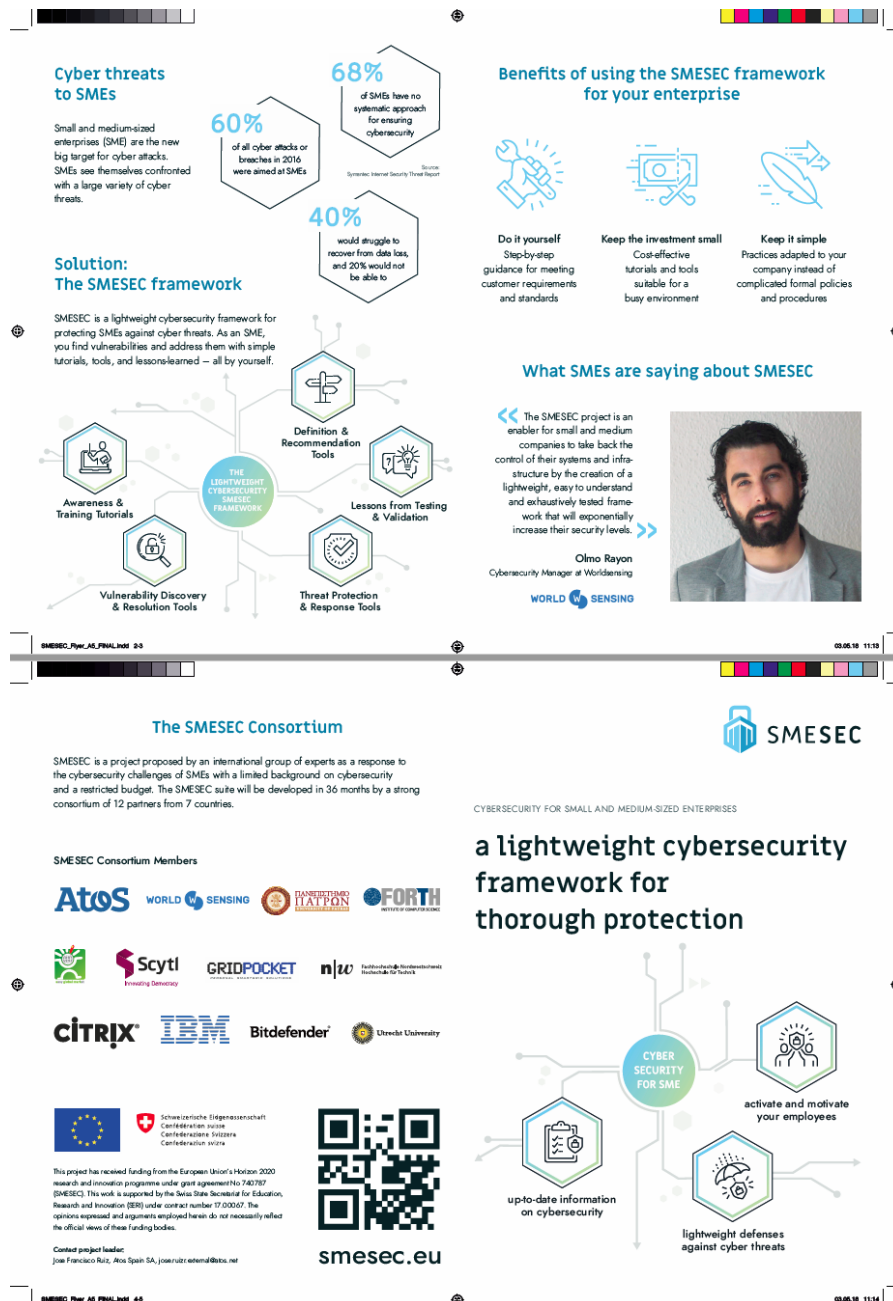


Figure 20: SMESEC flyer

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	57 of 126
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU
	<b>Version:</b>	1.2	<b>Status:</b> Final version

CYBERSECURITY FOR SMALL AND MEDIUM-SIZED ENTERPRISES



# a lightweight cybersecurity framework for thorough protection

40%

would struggle to recover from data loss, and 20% would not be able to

68%

of SMEs have no systematic approach for ensuring cybersecurity

60%

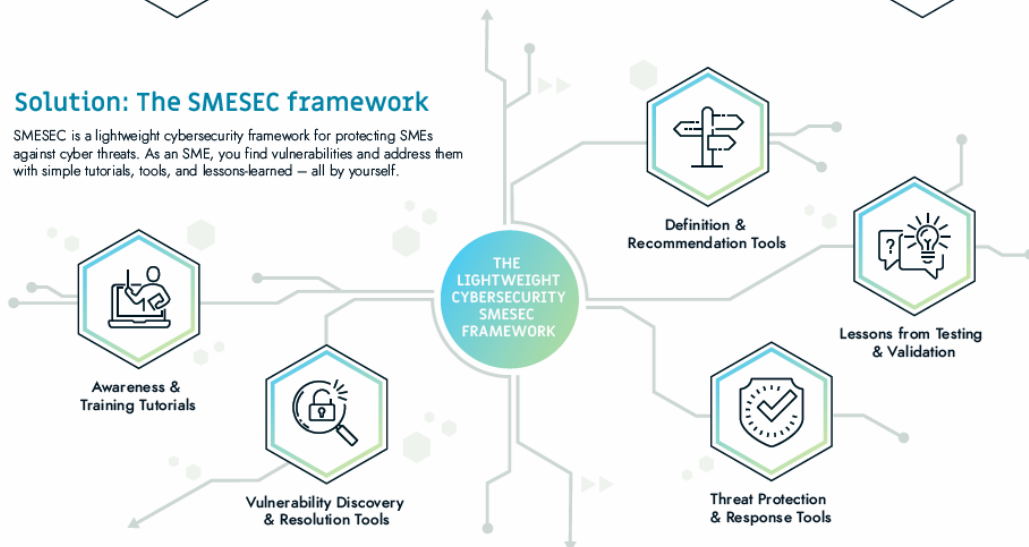
of all cyber attacks or breaches in 2016 were aimed at SMEs

## Cyber threats to SMEs

Small and medium-sized enterprises (SME) are the new big target for cyber attacks. SMEs see themselves confronted with a large variety of cyber threats.

## Solution: The SMESEC framework

SMESEC is a lightweight cybersecurity framework for protecting SMEs against cyber threats. As an SME, you find vulnerabilities and address them with simple tutorials, tools, and lessons-learned – all by yourself.



## Benefits of using the SMESEC framework for your enterprise

**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 Consortium Members



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740767 (SMESEC). This work is supported by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 17.00067. The opinions expressed and arguments employed herein do not necessarily reflect the official views of these funding bodies.

[smesec.eu](http://smesec.eu)



Figure 21: SMESEC poster.

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	58 of 126
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU
	<b>Version:</b>	1.2	<b>Status:</b>
			Final version

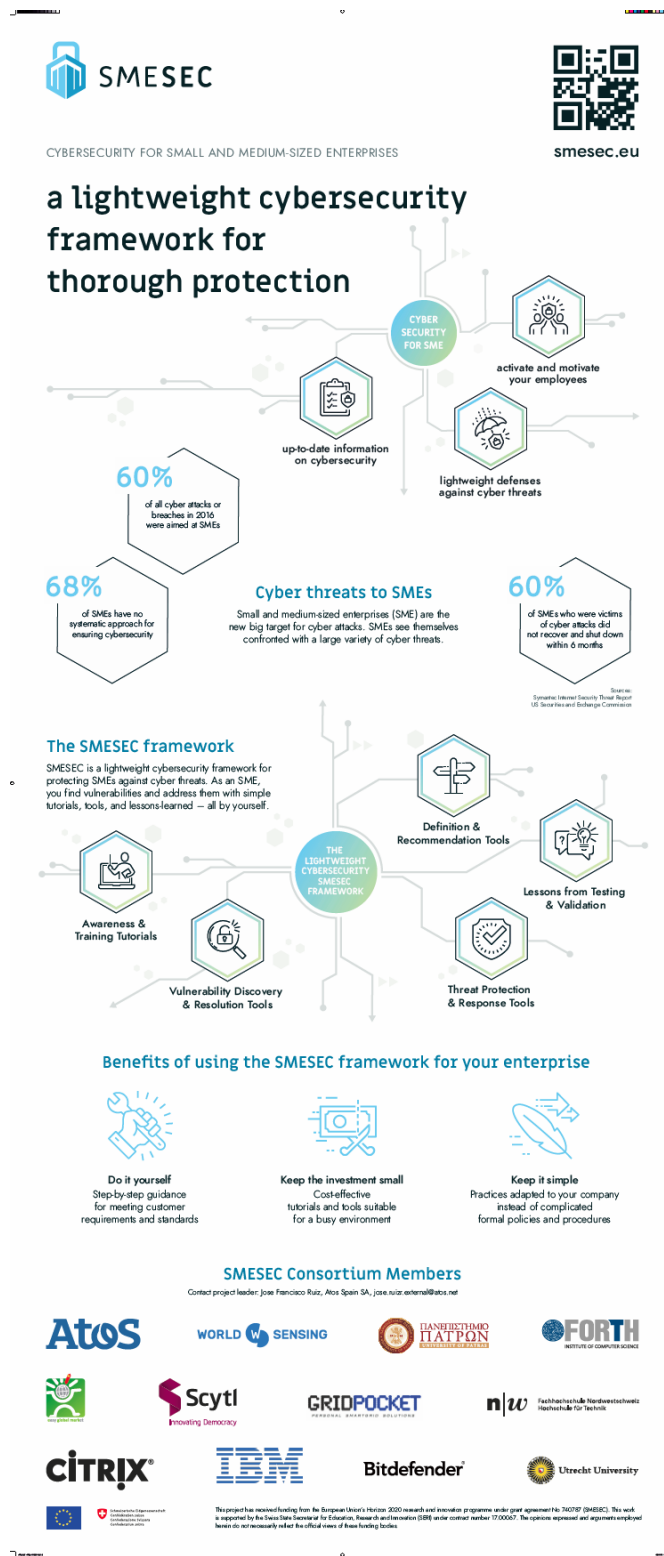


Figure 22: SMESEC poster.

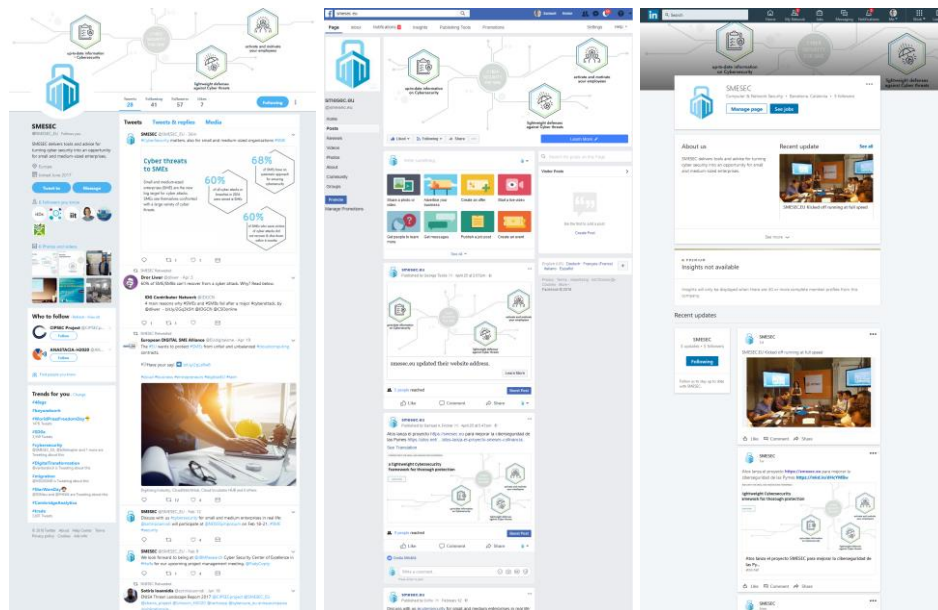
<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	59 of 126
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU
	<b>Version:</b>	1.2	<b>Status:</b> Final version

### 4.2.3 Other materials

Three videos were recorded to communicate SMESESEC use case SME, SMESESEC framework product management, and SMESESEC project management perspectives. The set of videos will be extended, cut, and annotated with the SMESESEC visual language during year 2. To support the open call promotion, the SMEs awareness plan, a press kit and the first webinar and tutorial will be created during year 2.

### 4.2.4 Social networks

These Twitter, Facebook, and Linked-In channels were adapted to the SMESESEC visual language.



**Figure 23: Snapshots of the SMESESEC presence on social channels**









The social network audience has evolved as shown in Table 11. The “restart” of the Linked-In follower figures on Feb 2018 is due to the change of the Linked-In SMESESEC group to a Linked-In SMESESEC company page.

Network	Jun 2017	Jul 2017	Aug 2017	Sep 2017	Oct 2017	Nov 2017	Dec 2017	Jan 2018	Feb 2018	Mar 2018	Apr 2018	May 2018
Twitter	16	19	19	26	32	32	32	42	48	54	60	*
Facebook	9	9	10	10	10	10	10	10	10	11	11	*
Linked-in	10	13	13	15	16	16	16	16	16	19	26	*

**Table 11: Social network followers by month (\*: no final figure available at the time of writing)**

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	60 of 126
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU
		<b>Version:</b>	1.2
		<b>Status:</b>	Final version

The following table shows examples of follower categories:

EU Projects	Cybersecurity Experts	IT Professionals
 <p><b>SOFIE</b> @EU_Sofie</p> <p>The SOFIE project aims to develop a blockchain driven federated platform for enabling information exchange of different IoTs and data silos.</p>	 <p><b>Marnix Dekker</b> @marnixdekker</p> <p>I work for ENISA, the EU Cybersecurity agency, PhD in Computer security and MSc in Quantum physics. Tweets are personal views.</p>	 <p><b>John Rotimi Ade</b> @Rotimi_1Adedeji</p> <p>Dad   husband   #IT Advisory &amp; #Consulting   #Change Agent   #XaaS   #Research   #Blockchain   #SDGs   #GPU   #Africa   #SDN   #HPC   #AI   #CTO [...]</p>
Consortium Member Organizations	European Institutions	SMEs
 <p><b>FHNW Institute for Interactiv...</b> @fhnw_iit Follows you</p> <p>Digital Interfaces for Humans and Processes</p>	 <p><b>Horizon 2020</b>   @EU_H2020</p> <p>The official account for the EU's #H2020 research and innovation programme. Managed by DG Research &amp; Innovation. Follow @EUScienceInnov &amp; Commiss...</p>	 <p><b>snoopmedia</b> @snoopmedia</p> <p>Seit 2000 entwickeln wir innovative Lösungen mit Herz und Verstand. Wir lieben, was wir tun und wir suchen Verstärkung: <a href="http://goo.gl/7xAaV6">goo.gl/7xAaV6</a></p>

### 4.3 External events

In this first year, partners investigated different channels participating in various events implying different communities. Mostly accompanied by project presentation, these first 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. A meeting is planned with this representative on May 25<sup>th</sup> to define the partnership roadmap and identify the synergies with national similar organizations. All project members will be part of this network activity, in charge of ensuring local contacts and exchanges with national points in their respective countries.

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	61 of 126
<b>Reference:</b>	D6.2	<b>Dissemination:</b> PU	<b>Version:</b> 1.2 <b>Status:</b> Final version



Table 12: Event participation of SMESEC consortium members during Year 1. summarizes the dissemination activities of the SMESEC consortium members. An event presentation and the role of SMESEC is presented in the following sections.

Target	Activity	Event / Channel	Partner	Date	Place
Cybersecurity	Conference Talk	Cyberstorm, Talk by Scytl	SCYTL, FHNW	Sept 1-3, 2017	Sursee, Switzerland
Cybersecurity	Conference Talk	AVAR 2017 conference	Bitdefender	Dec 6-8, 2017	Beijing, China
Cybersecurity	Conference Participation	34C3 - tuwat!	FHNW	Dec 28-30, 2017	Leipzig, Germany
Industry	Conference Talk	Industry 2025 R&D Conference	FHNW	Jan 11, 2018	Windisch, Switzerland
Engineering	Conference Talk (Poster)	REFSQ working conference	FHNW	March 20, 2018	Utrecht, Netherlands
Cybersecurity	Conference Talk	NDSS	FORTH	Feb 18-21, 2018	Sand Diego, CA, USA
Cybersecurity	Workshop participation	SAINT H2020 project workshop	UOP	Mar 21, 2018	Athens, Greece
Industry	Conference Talk	Software Product Summit	FHNW	Apr 17-18, 2018	Frankfurt, Germany
Cybersecurity	Workshop participation	Cyberwatching.eu concertation meeting	ATOS	Apr 26, 2018	Brussels, Belgium

**Table 12: Event participation of SMESEC consortium members during Year 1.**

### 4.3.1 Cyberstorm 2017



Swiss Cyber Storm was an international IT security conference in the domain of cyber-attacks and defence. It featured management and tech tracks with talks from international experts about the latest findings, techniques, visions, opinions, and lessons learned. The conference also linked with the Swiss finalists' team of the European Cyber Security Challenge and offered networking with national and international experts.

Jordi Puiggalí, Chief Security Officer, presented the Scytl and Swiss Post approach to the challenges of voter anonymization and verifiability in online voting scenarios. They showed that online voting has become a global trend and discussed how security and cryptography could be applied to the election industry.

Mark Zeman was participating at the conference on behalf of FHNW. For SMESEC, the conference offered the first opportunity to reach out and inform about the project. The talk showed that SMEs are

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	62 of 126
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU
	<b>Version:</b>	1.2	<b>Status:</b>
			Final version

not only vulnerable to cyber threats but that SMEs can become though leaders in the domains and use cases they serve. Also, the interaction with the present companies and cybersecurity experts initiated the dialogue on requirements for the SMESEC framework.

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

#### 4.3.2 AVAR 2017 Conference



AVAR (Association of Anti-Virus Asia Researchers), founded in June 1998, was composed of leading anti-virus experts from China, USA, Russia, UK, Germany, Japan, Australia, India, South Korea, Hong Kong, Taiwan, Singapore, Philippines, Malaysia, Vietnam, and other countries and regions. In the past 19 years, AVAR has been playing a vital role in stemming the spread of the virus worldwide. The annual

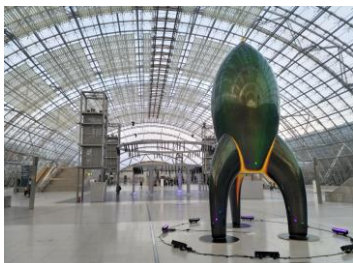
AVAR Conference has been one of the most authoritative technology exchange conferences.

Cristina Vatamanu, a Senior Malware Researcher, presented the EHDevel toolkit, a specialized framework that was used to gather information for years in different shapes and forms. Trying to find the purpose of this framework, Cristina was able to link it to the 2013 Operation Hangover APT.

For SMESEC, the conference offered the opportunity to present the cybersecurity expertise of the consortium and obtain feedback from a community of experts. The in-depth knowledge of malicious frameworks helps to design effective tools for thorough protection.

More information: <http://avar.skdlabs.com/>

#### 4.3.3 34C3 - tuwat!



The 34th Chaos Communication Congress (34C3) was an annual four-day conference on technology, society, and utopia. The congress offered lectures and workshops and events on information technology. The public and discussions had a critical-creative attitude towards technology and the effects of technological advances on society.

Mark Zeman was participating at the conference on behalf of FHNW. For SMESEC, the conference offered the first opportunity to reach out and inform about the project in informal discussions. Also, the interaction with the present companies and cybersecurity experts furthered the dialogue on requirements for the SMESEC framework.

More information: [https://events.ccc.de/congress/2017/wiki/Main\\_Page](https://events.ccc.de/congress/2017/wiki/Main_Page)

#### 4.3.4 Industry 2025 R&D Conference

The 3rd R&D conference of the Swiss Industry 2025 initiative offered an overview of activities at universities around Industry 4.0 and related technology. A poster exhibition allows networking and in-

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization			<b>Page:</b>	63 of 126		
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version

depth discussion of the presented topics between the speakers and the public from industry and politics.

Prof. Martin Gwerder presented challenges that SME encounter when they try to embrace cybersecurity. He explained how the SMESEC framework and the framework's cybersecurity coach can be used to address these challenges in a lightweight and cost-effective manner. He closed with an invitation to companies to become beta testers of the approach.



For SMESEC, the conference offered a significant opportunity to present and test the SMESEC concept for a lightweight Cybersecurity framework for the thorough protection of SME. Several companies have registered their interest to join the SMESEC beta testing programme.

More information: <http://www.industrie2025.ch/agenda/fe-konferenz-2018.html>

#### 4.3.5 NDSS Symposium

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.

Dr Sotiris Ioannidis presented the results of a large-scale analysis of open HTTP proxies, focusing on determining the extent to which user traffic is manipulated while being relayed. The study revealed incentives of publicly available web proxies and raised several concerns due to multiple cases where users can be severely affected by connecting to an open proxy. To mitigate the threat, FORTH built a service that collects and probes public proxies automatically and generates a list of safe proxies that do not perform any content modification.

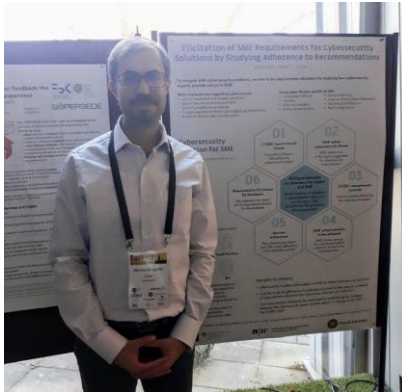
For SMESEC, the conference offered the opportunity to present the cybersecurity expertise of the consortium and obtain feedback from a community of experts. The in-depth knowledge of attacks helps to design effective tools for thorough protection.

More information: <https://www.internetsociety.org/events/ndss/2018/>

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization			<b>Page:</b>	64 of 126
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2
				<b>Status:</b>	Final version



### 4.3.6 REFSQ Working Conference



The REFSQ working conference series is an established international forum for discussing current and state-of-the-art requirements engineering practices, celebrating its 24th year. REFSQ held in Utrecht, returning to the location of the first REFSQ meeting in 1994.

Alireza Shojafar presented a poster that describes the challenges of SME regarding cybersecurity and introduces an approach to elicit requirements for cybersecurity solutions. The poster described CYSEC, a tool developed in SMESEC for offering cybersecurity advice to SME and eliciting cybersecurity requirements as a by-product. The poster concluded by outlining the planned research to develop and validate CYSEC.

For SMESEC, the working conference offered the opportunity of networking, feedback, and discussion of the SMESEC framework with a strong engineering research community.

More information: <https://refsq.org/2018/welcome/>

### 4.3.1 SAINT Project Workshop



The SAINT project proposes to examine the problem of failures in cyber-security using a multidisciplinary approach that goes beyond the purely technical viewpoint. The main objective of this workshop is to bring together several EU cybersecurity and privacy-related projects, to assist in the

exchange of knowledge and ideas and promote inter-project collaboration.

Dr Konstantinos Lampropoulos and Dr Apostolos Fournaris presented the SEMSEC project and lightweight cybersecurity framework for small and medium-sized enterprises.

For SMESEC, the workshop offered the opportunity to present and test the SMESEC concept and obtain feedback from European experts in cybersecurity. The workshop also offered opportunities for networking and cooperation across related European projects.

More information: <https://project-saint.eu/event/saint-workshop-march-2018>

### 4.3.2 Software Product Summit

The Software Product Summit was the first international conference dedicated to the management of software and software-intensive products. Participants in the Software Product Summit discussed how to grow the success of products and increase market share. During the 2-day gathering, they learned

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization			<b>Page:</b>	65 of 126		
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version

from industry leaders in software product management, exchanged experiences with fellow software product professionals, and participated in short but exciting hands-on sessions.

Prof. Dr Samuel Fricker presented the SMESEC cybersecurity awareness and capability improvement framework for SME. He discussed the challenges and success factors of do-it-yourself improvements and introduced the SMESEC approach. For SMESEC, the summit offered the opportunity to present and test the SMESEC concept and obtain feedback from software product professionals across the globe. Interested companies and the International Software Product Management Association, ISPMA, confirmed their interest in participating in the SMESEC beta programme.

More information: <https://softwareproductsummit.com/>

### 4.3.3 Cyberwatching.eu Concertation Meeting

Cyberwatching.eu is the European observatory of research and innovation in the field of cybersecurity and privacy. The objective of this first Cyberwatching.eu concertation meeting was to take stock of the current R&I landscape and to identify common themes and challenges for clustering activities. With a strong EC presence, this was a key event to ensure all the projects of the catalogue get noticed. There were opportunities for all projects to have their say through interactive discussions, break-out sessions, position papers and presentation opportunities.

Rodrigo Diaz Rodriguez presented the SMESEC project focusing on the objectives and challenges of cybersecurity for SMEs. Taking advantage of the attendance of other relevant projects in the area, we studied synergies both in solutions of cybersecurity and its awareness in organizations. He highlighted the more important barriers to adoption of cybersecurity and how SMESEC plans to go beyond them with a sound solution attractive from different points of view, including technical and budget.

The reception of the project was good and created open discussions about how necessary is for SMEs to be up-to-date in all cybersecurity aspects as they are one of the main actors of Europe...and the easier target to attack. Finally, we have reached concrete actions with relevant projects for joint work of dissemination and evaluation of results.

More information: <https://cyberwatching.eu/>

## 4.4 News / Blog Entries

In this first year, five blog entries related to the project start and activities were published. With the end of the first year, content-related blogging started.

The following subsections report these blogs.

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization				<b>Page:</b>	66 of 126	
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version

#### 4.4.1 SMESEC Project Launched



On June 8, the 12 project partners of the SMESEC consortium launched the project during the kick-off meeting in Barcelona, Spain. The event was the opportunity to focus on the project organization, the tool suite to be developed, and the use cases used to validate and demonstrate the SMESEC approach.

#### 4.4.2 Project Management Board Meeting in Patras



On October 5-6, the project partners of the SMESEC consortium gathered for the first project management board meeting. Reviewed were the work on requirements and architecture for the SMESEC framework addressing the cybersecurity needs for small and medium enterprises.

#### 4.4.3 Project Management Board Meeting in Haifa



On February 13-14, the project partners of the SMESEC consortium gathered for the second project management board meeting. Reviewed were the work on requirements and architecture for the SMESEC framework. First projects from the use case partners were presented and the problems of SMEs were discussed based on these use cases.

It has been clearly shown that dealing with Cybersecurity is hard for SMEs. They feel uncomfortable with the fact that on one side

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	67 of 126
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU
	<b>Version:</b>	1.2	<b>Status:</b>
			Final version

SMEs are a frequent target for cyber attacks and that there is no absolute protection. And on the other side, they feel overwhelmed by the large variety of threats and struggle to make the right decisions in regard to which mitigation strategies are suitable, cost-effective and practicable in the context of their own enterprise.

Based on the outcome of the last months, amendments to the framework were discussed to make the framework better suitable for SMEs.

#### 4.4.4 Atos presents SMESEC in a national press note

Atos has launched a press note about the SMESEC project in its webpage. There it is described the objectives of the project, challenges, and motivations together with all the partners involved in its work.

The press note was released at a national level for all Spanish organizations.

#### 4.4.5 Don't fail with EFAIL and stop panicking

In May, a new vulnerability sent rumblings through security mailing lists. The presented attack is called EFAIL and claims to target emails encrypted via S/MIME and PGP. While the flaws quoted in this finding are serious, there are some details which get glossed over in the general panic.

First of all: While the EFAIL attack is rather simple, it requires the capability to intercept emails. This requirement is rather easy for a state-sponsored actor or an internet service provider (ISP) to fulfil, but it is tough to achieve for a single hacker.

The attack shows that if an attacker can intercept a message and manipulate its content, the attacker may gain knowledge of the content. However, even then the attack only works if the recipient is using a non-standard, if common, security setting in his e-mail client. The attacker is tricking the client on the receiver's side to decrypt the email and then sending the content to a server of the hacker's choice.

To avoid being affected by EFAIL adhere to the following guidelines:

- Disable automatic loading of images or external content (do not enable it even for single sources). Loading external content is disabled by default in most email clients, but many users enable it later.
- Never expect that a colleague sends you emails with external content. While it is a common practice for advertisements to track reading of the emails, it involves having their own public servers providing content. Colleagues do not have external content even when sending emails containing images. Always be on alert if you receive an email with a request for external content.
- Be careful when clicking on links. In regard to this attack, you could say: the longer the link, the more suspicious. The plain text of a message could be sent with a link as well. When hovering over a link, most email clients display the full address. Using links may be dangerous, but in this specific case, you are most likely safe if the link shown is short.
- Never open emails from unknown sources.

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization			<b>Page:</b>	68 of 126		
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version

- If you receive emails not showing images, click on the link labelled "click here to see mail if not shown properly" provided by almost any advertising company. Clicking there is safer than enabling external content.
- Protect your keys with passphrases. Most clients force the users to do so but then offer to store a passphrase in a built-in store. Storing keys in a built-in store is usually unsafe. It is safer to type the passphrase if needed or use an external password store and require confirmation for the use of a password.

These recommendations are not new and in fact are common security practices. That is why all the settings above are the defaults in most email clients. Tooling helps us a lot to get into a secure state, but this attack is a great example of how users may make good tools fail.

Just by the way: If you want to stay safe, you should communicate using plain text instead of HTML or rich text emails. In this format, dangers are not lurking around every corner and merely lose access to formatting your text in bold or italic and adding HTML like links. On the plus side, it makes sure that no-one else has added HTML and steals your emails...

Stay safe  
The SMESEC security team

## 4.5 Publications

Table 13 summarizes the scientific results produced by the SMESEC consortium members.

Type	Title	Authors	Partner	Venue
Conference Proceedings	Uncloaking the Dragon: A Large-scale Analysis of Content Modification by Open HTTP Proxies	Sotiris Ioanmidis	FORTH	NDSS 2018, San Diego, CA, USA
Conference Proceedings	Elicitation of SME Requirements for Cybersecurity Solutions by Studying Adherence to Recommendations	Alireza Shojaifar, Samuel Fricker, Martin Gwerder	FHNW	REFSQ 2018, Utrecht, Netherlands

**Table 13: Dissemination activities of SMESEC consortium members during Year 1.**

## 4.6 Dissemination results

The first year of dissemination has focused on the creation of dissemination kits and establishing a digital and physical presence. Accordingly, SMESEC has started reaching out to target and stakeholder audiences with information about the importance of cybersecurity for SME and the SMESEC project. During the second year, information about the SMESEC framework will be disseminated and the open call launched. The third year will focus on disseminating results using the SMESEC framework and enable future exploitation.

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization			<b>Page:</b>	69 of 126		
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version



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

Channel	Indicators	Objectives Y1	Fulfilment Y1	Objectives Project End
Website	Downloads per year	0	0	1000
	Unique visitors per month	500	Monthly Average: 566 M12: 1612	1000
	Visits per month	2000	Monthly Average: 1438 M12: 2855	4000
	Website news per month	0.25	Monthly Average: 1.25	1.0
Social networks	Social networks posts per month	10	4.3	30
	Twitter followers	50	M12: 71	250*
	Facebook followers	20	M12: 11	100*
	Linkedin followers	20	M12: 9	100*
Publications / Communication materials / Contributions	Press releases	1	1	4
	Newsletters per quarter	0	0	1
Events	Attended conferences or exhibitions	25	9	75
	Webinars	0	0	3
	Tutorials	0	0	3

**Table 14: Visibility monitoring and related objectives (\*: no objective defined in DOA)**

Channel	Indicators	Objectives Y1	Fulfilment Y1	Objectives Project End
Publications / Communication materials / Contributions	Contributions to roadmaps	0	0	2
	Contributions to standards	0	0	2

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	70 of 126
<b>Reference:</b>	D6.2 <b>Dissemination:</b> PU	<b>Version:</b> 1.2	<b>Status:</b> Final version

Channel	Indicators	Objectives Y1	Fulfilment Y1	Objectives Project End
	Contributions to policy	0	0	2
	Journal Publications	0	0	8
	Conference Talks	5	6	20
Workshops	Number of workshops	0	0	2
Website	Open call registrations	0	0	20
	Registered members (SMESEC framework users)	0	0	100

Table 15: Scientific impact monitoring and related objectives (\*: c.f. also previous table)

## 4.7 Dissemination plan update

The core basis of the SMESEC dissemination strategy is maintained for the coming years but the acquired SMEs feedbacks led the consortium to adjust its roadmap to maximize the project audience. The use-case specialized events will be addressed in year 2 with a set of events participations such as a booth at the IoT solutions World Congress. The below Table 16 : Targeted coming events give an overview of the planned dissemination activities.

Audience	Event	Date	Place	Presence
All	GDPR Deadline	May 2018		
IoT	IoT Week	Jun 2018	Spain	Flyers
All	El correo de Andalucia	May 2018	Spain	Interview
IoT	Internet of Things World EU	Jun 2018	UK	Flyers
All	ETSI Security week	Jun 2018	Sophia, France	Flyers, Poster or presentation

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	71 of 126
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU
	<b>Version:</b>	1.2	<b>Status:</b> Final version

Audience	Event	Date	Place	Presence
SME	Security of Things World	Jul 2018	Germany	Flyers
SME	Patras IQ	Aug 2018	Greece	Flyers
Research	RAID	Sep 2018	Greece	Flyers, Session, Talk?
SME	Industry of Things World	Sep 2018	Germany	Flyers
Industry	Digital Festival	Sep 2018	Switzerland	Flyers
IoT	IoT Solutions World Congress	Oct 2018	Spain	Booth
SME	Cybersecurity Europe	Oct 2018	UK	Flyers
SME	SMESEC WEBINAR	Oct 2018	Online	Webinar
All	Computer security day			
Startup	Lift Conference	Nov 2018		Flyers
SmartCity	Smart City Expo World Congress	Nov 2018	Spain	Flyers
Startup	Web Summit	Nov 2018	Portugal	Flyers
All	ICT 2018	Dec 2018	Vienna	Booth shared with other H2020 projects
Research	IEEE Globecom	Dec 2018	UAE	Flyers / Poster

**Table 16 : Targeted coming events**

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization			<b>Page:</b>	72 of 126
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2
				<b>Status:</b>	Final version



This axis will be enhanced with a set of networking actions with key stakeholders, able to serve as information relay of the SMESEC communication, multiplying the SMEs contacts within their networks. Partners will establish in the year 2 sustainable links with the three identified key channels such as:

- SMEs organization, association and federation
- Security and SMEs economic clusters
- H2020 sister projects

This strategy will be deployed at the European scale with a multi-dimensional approach, European and Switzerland organizations will be involved and associated by the WP task leaders such as ATOS, FHNW and EGM. This EU coordination will be relayed by national contact points and all consortium members will be in charge of animating the national SMEs networks through these organizations activities. In concrete terms, SMESEC will collaborate by the following means:

- Joint event of cybersecurity for SMEs
- Invitation to events we organize
- Attendance at events they organize for presenting the results of SMESEC
- Invitation to participate in the advisory board for giving us their feedback/experience
- Participation in the open call we will organize
- SMESEC relay of communication materials via partner's channels

Some links are already established as presented in the previous sections and SMESEC will develop connections in the coming months with most of these organizations, a priority is already given to SMEs organizations, but partners will establish strong links with clusters and sisters' projects. Participation in the SAINT project and Cyberwatching.eu (umbrella project for cybersecurity solutions) will help the project to acquire a strong and qualitative audience. This work will be pursued with synergies creation, as for example, we may quote the IoT trust & security organized at the ICT 2018 in Vienna with four complimentary projects such as IoTcrawler, SOFIE, ENACT and ARMOUR. SMESEC will be part of this collaboration showcase, showing IoT stakes related to security and privacy, presenting under development solutions dedicated to IoT security issues.

In parallel, we will include in the current dissemination plan the awareness plan promotion with a constant promotion of SMEs training repository offered by SMESEC, a continuous survey on SMEs security watch to collect and interact with Small and medium companies. This online questionnaire will aim at getting a continuous feedback on cybersecurity risks for SMEs, collecting SMEs needs and identify key ideas to adjust the SMESEC framework but all also prepare next projects steps and constitute in building SMESEC SMEs communities.

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization			<b>Page:</b>	73 of 126	
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b> Final version

## 5 Standardization activities

In the D6.1 Dissemination Plan and Market Analysis document, the SMESEC standardization plan with five main phases, each consisting of several steps, was described. According to this plan, the investigation and the analysis phase were planned to be completed until month 12. The sections 5.2 and 5.3 explain the activities conducted in these phases and their respective results.

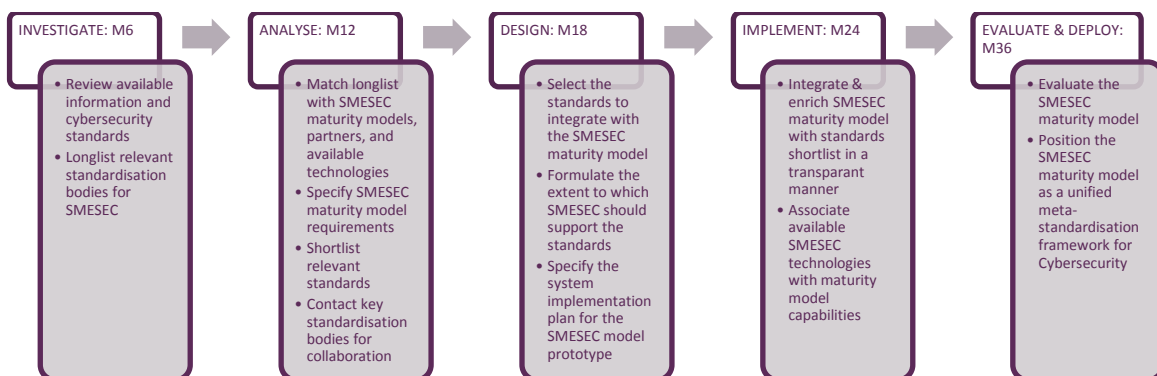
In this report, we don't prefer to duplicate the long list of standards that were investigated during the Investigate Phase. This list can be found in the deliverable D6.1 Dissemination Plan and Market Analysis in section 5.

Instead, in this report, we focus on the cybersecurity related standards and other standards that might be useful for the development of cybersecurity solutions for SMESEC use case domains (IoT, E-voting, Smart Grid and Smart City)

### 5.1 Standardization plan

#### 5.1.1 Standardization approach and phasing

This chapter outlines the SMESEC standardization strategy, coordinated by Utrecht University (UU). This standardization strategy builds upon the existing UU maturity models for information security and cybersecurity and is structured according to the standard system development lifecycle (SDLC). The cornerstone of the SMESEC standardization strategy is the SMESEC maturity model for personalized advice and subsequent incremental process improvement within SMEs throughout Europe. The model is accompanied by a reference implementation – i.e. assessment engine – to help improve its sustainability and relevance well beyond the SMESEC project timespan as depicted in Figure 24.



**Figure 24: Overview of the SMESEC Standardization plan with five main phases, each consisting of several steps.**

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	74 of 126	
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	
	<b>Version:</b>	1.2	<b>Status:</b>	Final version

First, in the INVESTIGATE phase during M1-M6 we have explored the abundance of available standardization bodies related to information and cybersecurity. This resulted in a longlist of standards which are elaborated upon below in section 5.2.

Second, in the ANALYSE phase from M7-M12 we have matched the longlist of available standards with the SMESEC maturity models, partners, and available technologies. In parallel, we are currently engineering the requirements for the envisioned SMESEC maturity model, including transparent standards lineage, implementation technology guidelines per capability, and maturity model maintainability-by-design, among others. These two steps result in a shortlist of security standards most relevant for SMESEC. We will contact these key standardization bodies to discuss collaboration opportunities.

Third, in the overlapping DESIGN phase from M10-M18 we select the standards to integrate with the SMESEC maturity model and formulate the extent to which SMESEC should support the standards. At the same time, we develop a technical specification for the IT implementation plan to more efficiently and effectively prototype the model adhering to the specified requirements.

Fourth, in the overlapping IMPLEMENT phase from M13-M24 we implement the technical specification to more efficiently and effectively prototype the model iterations while adhering to the specified requirements. The resulting prototype integrates and enriches the original UU/SMESEC maturity models with the standards shortlist in a transparent and sustainable manner while associating the available SMESEC technologies from all SMESEC partners with the appropriate maturity model capabilities. Note that piloting the model will already be possible at this stage using a paper-based version. However, a flexible and maintainable analytic system implementation of the encompassing SMESEC maturity model is considered crucial for a long-lasting SMESEC impact.

Fifth, in the EVALUATE & DEPLOY phase in M25-36 we evaluate the final SMESEC maturity model in our four case studies and possibly other environments to fine-tune its many aspects as appropriate. After a satisfactory evaluation, we will start positioning the SMESEC maturity model as a unified meta-standardization framework for cybersecurity in especially SMEs, that we expect to be received well by all stakeholders, thanks to its transparent meta-standards design, associated toolkit to help implement the personalized security advices, and the support of the standardization collaborators which we already contacted in phase 2.

### 5.1.2 Objectives

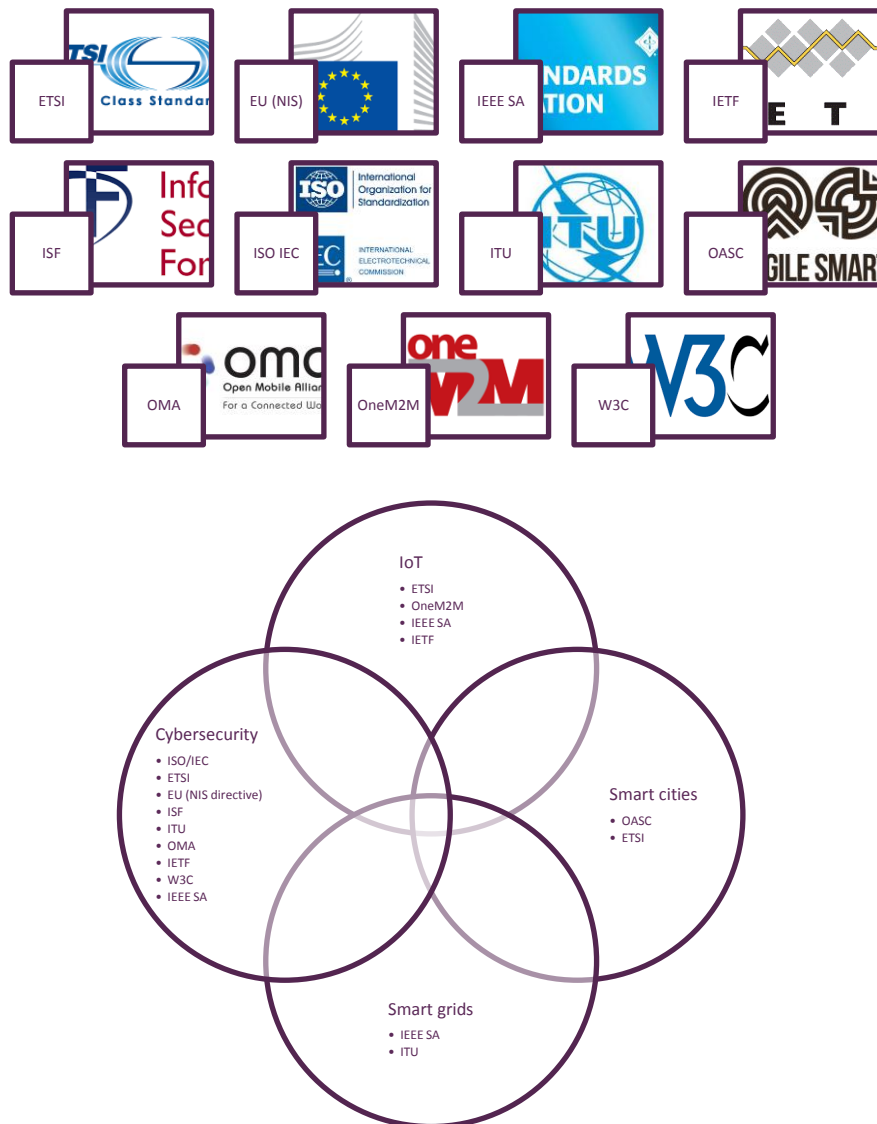
The standardization plan outlined above operationalizes the SMESEC T6.3 Standardization activities. The main goals of this plan are: **First**, to disseminate the SMESEC solution and promote the adoption of existing or emerging standards and cyber-security models specially defined for SMEs, ensuring our development will be consistent with the standards, and within the community making our outcomes available. **Second**, to provide feedback to the standardization bodies to help them to improve their standards and interoperability. Provide tools and methods to evaluate implementation (conformity, etc.). **Third**, to create links with active standardization bodies and participate in evolving standards, pushing the SMESEC results.

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	75 of 126
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU
	<b>Version:</b>	1.2	<b>Status:</b> Final version

### 5.1.3 Target standards developing organizations (SDOs)

The SMESEC project implies a wide range of areas where the standardization activities aim to contribute in. From the project features, with a similar approach as done in dissemination, a list of main players has been created to identify targets among International organization for Standardisation, ETSI, OneM2M and European Commission Directives and regulation.

This first work developed in the next sections (Investigation phase) enables us to build an overall landscape for SMESEC standardisation plan. The Figure 25 below shows the standardisation scope and target SDOs, involved in cybersecurity or more specifically involved in verticals contributions for IoT, Smart cities and Smart grids fields.



**Figure 25: SMESEC related SDOs landscape**

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	76 of 126
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU
		<b>Version:</b>	1.2
		<b>Status:</b>	Final version

## 5.2 Activities conducted during the Investigate Phase (M1-M6)

During this phase of the standardization plan, we have explored the abundance of available standardization bodies related to information security and cybersecurity. The websites of well-known standardization bodies (ISO, ETSI, etc.) have been searched for standards related to information security and cybersecurity. In addition, generic searches on the web using keywords such as ‘cybersecurity’, ‘information security’, ‘SME’ and ‘standard’ are conducted. This resulted in a long list of standards which was previously elaborated in section 5 of D6.1 Dissemination Plan and Market Analysis document as the cybersecurity-related standards.

We also investigated the standards related to the use case partners’ domains: IoT, smart cities, smart grid and e-voting. The standards related to these domains were also given in the previous deliverable.

An important document that was investigated is the EC Rolling Plan for ICT Standardization 2017 [10], prepared by The European Multi Stakeholder Platform (MSP) on ICT. We observed that Cybersecurity, IoT, Smart Grids, Smart Cities, and E-voting, which are all focus areas of SMESEC, are included in the EC Rolling Plan for ICT Standardization 2017. In addition, for 2018, the EC Rolling Plan for ICT Standardization 2018 [11] was published in March 2018 and these focus areas are also included in this new release.

During this phase, a survey has been carried out to identify the SMESEC partner’s involvement in the standardization activities in contact with standardization bodies. The results of this survey can be found in Table 17 : SMESEC Partners’ Involvement with Standardization Bodies.

Standardization Bodies											
SMESEC Partner	International Organization for Standardization (ISO)/IEC	ETSI (the European Telecommunications Standards Institute)	oneM2M (Standards for M2M and the Internet of Things)	NIS Network and Information Security Directive	Standard of Good Practice of the Information Security Forum (ISF)	ITU (International Telecommunication Union)	OMA (Open Mobile Alliance)	OASC (Open & Agile Smart Cities)	NIST	The Council of Europe/E-voting Standards	International Institute for Democracy and Electoral Assistance
EGM		Member of work group(s)/ Contributor	Member of work group(s)/ Contributor								
UOP		(intention to participate)									
FHNW		Member of work group(s)/ Contributor				Occasional guest in meetings					
SCYTL								Member of work group(s)/ Contributor	Member of work group(s)/ Contributor	Member of work group(s)/ Contributor	

**Table 17 : SMESEC Partners’ Involvement with Standardization Bodies**

The survey results show that some SMESEC partners have already been participating in work groups that are formed by the standardization bodies and they have been contributing to standardization activities. It is expected that knowledge and expertise gained by the SMESEC partners during the project will expand and add further value to these contributions.

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization				<b>Page:</b>	77 of 126	
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version

### 5.3 Activities conducted during the Analyse Phase (M7-M12)

In this phase, we have investigated the most relevant standards, recommendations, guidelines related to SMESEC framework components. After exploring standards specific to the components, we have also investigated the standards, recommendations, guidelines that are related to the SMESEC framework as a whole. The results of this study are given in the following tables (Table 18-Table 28). These tables might be updated as a result of the ongoing discussions with the partners.

Tool	Standard/ Recommendation/ Guideline
XL-SIEM - Security Information and Event Management System	<a href="#">ETSI GS ISI 002 V1.2.1 (2015-11)</a> <a href="#">A security event classification model and taxonomy (Group Specification)</a>
	<a href="#">ETSI GS ISI 005 V1.1.1 (2015-11)</a> <a href="#">Information Security Indicators (ISI); Guidelines for security event detection testing and assessment of detection effectiveness</a>
	<a href="#">ETSI GS ISI 004 V1.1.1 (2013-12)</a> <a href="#">Information Security Indicators (ISI); Guidelines for event detection implementation</a>
	ISO/IEC 27043:2015(en) Information technology — Security techniques — Incident investigation principles and processes
	<a href="#">FIRST - Information Exchange Policy (IEP)</a>

Table 18 : Standards related to ATOS XL-SIEM

Tool	Standard/ Recommendation/ Guideline
Bitdefender GravityZone - Protection Against Malware.	<a href="#">European Commission Information System Security Policy C(2006) 3602</a> <a href="#">STANDARD ON CONTROLS AGAINST MALICIOUS CODE</a>
	<a href="#">FIRST - Common Vulnerability Scoring System SIG</a>

Table 19 : Standards related to Bitdefender GravityZone

Tool	Standard/ Recommendation/ Guideline
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
	<a href="#">ICSA Labs Web Application Firewall Certification Criteria</a>

Table 20 : Standards related to Citrix NetScaler

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	78 of 126				
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version

Tool	Standard/ Recommendation/ Guideline
EGM TaaS solution - Security Testing	<a href="#">ETSI TR 101 583 V1.1.1 (2015-03)</a> <a href="#">Methods for Testing and Specification (MTS); Security Testing; Basic Terminology</a>
	<a href="#">ETSI EG 203 251 V1.1.1 (2016-01)</a> <a href="#">Methods for Testing &amp; Specification; Risk-based Security Assessment and Testing Methodologies</a>
	<a href="#">Automated Source Code Security Measure™ (ASCSMTM) V1.0</a>
	<a href="#">2011 CWE/SANS Top 25 Most Dangerous Software Errors</a>
	<a href="#">FIRST - Common Vulnerability Scoring System</a> <a href="#">ICSA Labs IoT Security Testing Framework</a>

**Table 21 : Standards related to EGM TaaS Solution**

Tool	Standard/ Recommendation/ Guideline
FORTH / Early Warning Intrusion Detection System	<a href="#">ETSI GS ISI 004 V1.1.1 (2013-12)</a> <a href="#">Information Security Indicators (ISI); Guidelines for event detection implementation</a>
	<a href="#">Common Attack Pattern Enumeration and Classification (CAPECT™)</a>
	<a href="#">ETSI GS ISI 003 V1.2.1 (2018-01)</a> <a href="#">Information Security Indicators (ISI); Key Performance Security Indicators (KPSI) to evaluate the maturity of security event detection</a>
	<a href="#">ETSI GS ISI 005 V1.1.1 (2015-11)</a> <a href="#">Information Security Indicators (ISI); Guidelines for security event detection testing and assessment of detection effectiveness</a> <a href="#">FIRST - Common Vulnerability Scoring System</a>

**Table 22 : Standards related to FORTH / Early Warning Intrusion Detection System**

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	79 of 126
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU
	<b>Version:</b>	1.2	<b>Status:</b>
			Final version



Tool	Standard/ Recommendation/ Guideline
IBM AngelEye - Virtual Patching	<a href="#">ETSI TR 101 583 V1.1.1 (2015-03) Methods for Testing and Specification (MTS); Security Testing; Basic Terminology</a>
	<a href="#">ETSI EG 203 251 V1.1.1 (2016-01) Methods for Testing &amp; Specification; Risk-based Security Assessment and Testing Methodologies</a>
	<a href="#">Automated Source Code Security Measure™ (ASCSMTM) V1.0</a>
	<a href="#">2011 CWE/SANS Top 25 Most Dangerous Software Errors</a>

**Table 23 : Standards related to IBM AngelEye - Virtual patching**

Tool	Standard/ Recommendation/ Guideline
IBM Anti-ROP	<a href="#">Evaluating the Effectiveness of Current Anti-ROP Defenses</a>
	<a href="#">Defending against Return-Oriented Programming</a>

**Table 24 : Standards/Literature related to IBM Anti-ROP**

The following tables include the standards, recommendations, guidelines and academic articles (in some of the domains) related to the use case domains of the SMESEC. During the investigation of these domain related standards we have exploited the State-of-the-Art Syllabus Overview of existing Cybersecurity standards and certification schemes document [12] published by ECSO (European Cybersecurity Organization). We opted for the international standards, recommendations and guidelines rather than the country specific ones.

Domain	Standard/ Recommendation/ Guideline
E-Voting	Recommendation CM/Rec(2017)5[1] on standards for e-voting(Council of Europe)
	E-voting Handbook (Council of Europe)
	OASIS Election Markup Language (endorsed by CE)
	Towards Security Modeling of e-Voting Systems

**Table 25 : Standards related to E-voting Domain**

Domain	Standard/ Recommendation/ Guideline
IoT	ITU SG20 Internet of things (IoT) and smart cities and communities (SC&C)
	European Technology & Innovation Platforms (ETIPs)
	ITU-T Recommendations under Study Group 15
	OWASP Internet of Things Project
	Industrial Internet of Things Security Framework
	IoT Security Foundation- IoT Security Compliance Framework
	BITAG Internet of Things (IoT) Security and Privacy Recommendations
	Cloud Security Alliance Future-proofing the Connected World

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	80 of 126				
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version



Domain	Standard/ Recommendation/ Guideline
	GSMA IoT Security Guidelines
	ETSI TR 103 118 Machine-to-Machine communications (M2M); Smart Energy Infrastructures security; Review of existing security measures and convergence investigations

**Table 26 : Standards related to IOT Domain**

Domain	Standard/ Recommendation/ Guideline
Smart Grid	IEEE Std 1686-2013 Standard for Intelligent Electronic Devices Cyber Security Capabilities
	IEEE Std 2030.2-2015 - IEEE Guide for the Interoperability of Energy Storage Systems Integrated with the Electric Power Infrastructure
	<a href="#">ETSI - TR 103 118 Machine-to-machine communications (M2M); smart energy infrastructures security</a>
	<a href="#">ENISA Smart Grid Security Certification</a>
	<a href="#">European Technology &amp; Innovation Platforms (ETIPs)</a>
	IEC/TR 62351-10: Power Systems Management and Associated Information Exchange – Data and Communications Security – Part 10: Security Architecture Guidelines
	NISTIR 7628 Rev. 1 Guidelines for Smart Grid Cybersecurity
	ISO 17800:2017 Facility smart grid information model
	ISO/IEC 30101:2014 Information technology -- Sensor networks: Sensor network and its interfaces for smart grid system
ISO/IEC 27019:2017 Information technology -- Security techniques -- Information security controls for the energy utility industry	

**Table 27 : Standards related to Smart Grid Domain**

Domain	Standard/ Recommendation/ Guideline
Smart Cities	<a href="#">ISO/IEC 30182:2017 Smart city concept model -- Guidance for establishing a model for data interoperability</a>
	<a href="#">ISA/IEC 62443 (Security for Industrial Automation and Control Systems) (Part 1)</a>
	<a href="#">ETSI TR 103 290 Machine-to-Machine communications (M2M); Impact of Smart City Activity on IoT Environment</a>

**Table 28 : Standards related to Smart Cities Domain**

In this phase, we have also investigated the domains related to SMESEC and which standardization bodies are active in these domains. The main concern of doing this study was to identify the standardization bodies to contact. Table 29 shows the results of this investigation. From this table, we can easily see that ETSI, ITU, ISO and IEEE SA are the ones that publish standards the most. Note that, even though ISO and IEEE also provide standards for many of our domains, we have opted for open, European standardization bodies instead.

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	81 of 126				
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version

Standardization Body/Organization	Cybersecurity	IoT	Smart Cities	Smart Grid	E-voting
ETSI	X	X	X	X	
ISO/IEC	X	X	X	X	
EU (NIS directive)	X				
ISF	X				
ITU	X	X	X	X	
OMA	X				
IETF	X	X			
W3C	X				
IEEE SA	X	X	X	X	
FIRST	X	X			
oneM2M		X			
OASC			X		
Council of Europe					X

**Table 29 : Standardization Bodies/Organizations and SMESEC Domains**

The standardization bodies are organized by focused workgroups. In order to contribute to the studies carried out by those workgroups, we first investigated which workgroups are active for ETSI and ITU. Table 30 and Table 31 show a list of clusters/workgroups active in the ETSI and ITU organizations respectively. These tables also show the relevance of the clusters/workgroups with the SMESEC project.

ETSI (European Telecommunications Standards Institute) Clusters	SMESEC Relevance
Home & Office	X
Better Living with ICT	X
Content Delivery	-
Networks	-
Wireless Systems	-
Transportation	-
Connecting Things	X
Interoperability	X
Public Safety	-
Security	X

**Table 30 : ETSI Clusters and SMESEC Relevance**

ITU (The International Telecommunication Union) Workgroups	SMESEC Relevance
SG2 - Operational aspects	-
SG3 - Economic and policy issues	-

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	82 of 126				
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version

ITU (The International Telecommunication Union) Workgroups	SMESEC Relevance
SG5 - Environment and circular economy	-
SG9 - Broadband cable and TV	-
SG11 - Protocols and test specifications	-
SG12 - Performance, QoS and QoE	-
SG13 - Future networks (& cloud)	X
SG15 - Transport, access and home	X
SG16 – Multimedia	-
SG17 – Security	X
SG20 - IoT, smart cities & communities	X

**Table 31 : ITU Workgroups and SMESEC Relevance**

Having this information and the SMESEC partners' standardization bodies involvement survey results and considering the effort required, it would be feasible to contact at least ETSI and ITU. The possibilities of participating in these work groups are currently under discussion with the partners and actions will be planned accordingly.

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization			<b>Page:</b>	83 of 126		
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version

## 5.4 Conclusions

---

For the period of this report, standardization activities are carried out according to the standardization plan and strategy given in the deliverable D6.1 Dissemination Plan and Market Analysis. The activity that we are focusing on is contacting key standardization bodies. The relevant partners' involvement is desired for contributing the existing standards' improvement if possible. This could be achieved by partners' participation in workgroups established by the standardization bodies. Table 17 shows already established relations between SMESEC partners and some standardization bodies.

In addition, Table 29 shows the standardization bodies mostly related to SMESEC domains. In Table 30 and Table 31 we have also investigated the clusters/study groups of ETSI and ITU which are mostly related to SMESEC domains. The possibilities of participating in these work groups will be discussed with the partners and actions would be planned accordingly.

The activities that were planned beyond month 12 will be carried according to the plan provided in the deliverable D6.1 Dissemination Plan and Market Analysis such as Design, Implement, Evaluate & deploy phases. The SMESEC contributions in standardization will be enhanced with a gradual roadmap based on the standards selection to be integrated in the SMESEC Framework (Design phase), followed by the effective implementation of the standards related technical specifications, prototyping the model iterations while enriching the UU/SMESEC maturity model (Implement phase) and finally assessing the SMESEC model from use cases experience and positioning the SMESEC framework and model as a unified meta-standardization framework for SMEs Cybersecurity (Evaluate & deploy phase).

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization				<b>Page:</b>	84 of 126	
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version

## 6 Conclusions

As the technical work packages progress, alongside the events and workshops participation, the SMESEC project adjust its strategy fine-tuning the dissemination plan to wider the SMEs audience and develop satellite project communities.

From the preliminary market analysis, advanced information is brought in this document to present the exploitation plan, with a joint approach for the unified SMESEC framework but also from each partner as the project contributes in developing each component, offering new exploitation opportunities.

Exploitation of project outcomes is a central guideline for the SMESEC consortium, partners are involved in maximizing impacts with strongly expected inputs in standardization and extended actions in dissemination to support this objective. SMEs, the central target of the project, is put at the centre of each action with the ambition to establish wide communities. Various channels have been identified and partners are actively involved in networking with all stakeholders at the European scale but also at a national level.

Mid-project is key milestone for SMESEC as the first version of the framework will be released. All plans are focusing on it, preparing the open call process with a special attention to continuously monitor the SMEs needs. Hence, SMESEC integrated in the roadmap, the awareness plan and established a continuous of SMEs cybersecurity watch. From this market feedbacks, the consortium will keep on updating its strategy on a regular basis to ensure that the technical dimension is oriented to the future market opportunities and to prepare an effective transfer to the market as soon as the project is finalized.

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization			<b>Page:</b>	85 of 126		
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version

## Annexes

---

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization				<b>Page:</b>	86 of 126	
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version

# 1 Anti-Rop exploitation fiche

## 1.1 Component fiche 1

Component name	Anti-Rop
Functionality	Anti-ROP is a tool to create applications that cannot be exploited by malicious software by shuffling its building blocks.
Key features	Shuffle C/C++ executables to protect against security vulnerabilities exploitation
Expected TRL	7
Licence	<ul style="list-style-type: none"> <li>• <b>Licensing:</b> The inventor company licenses its software directly to other companies.</li> </ul>
Owner	IBM
Component manager	Dov Murik <a href="mailto:Dov.Murik1@il.ibm.com">Dov.Murik1@il.ibm.com</a>

## 1.2 Commercial Assessment of the component

### 1.2.1 Value proposition

Problem statement	Shuffle C/C++ executables to protect against security vulnerabilities exploitation
Benefits	Indicate: <ul style="list-style-type: none"> <li>• Create various unique executable copies of a C/C++ application</li> <li>• break the attackers' ability to scale-up their knowledge of one device to attack another.</li> </ul>
Unfair advantage	Expert knowledge in source code and binary shuffling

### 1.2.2 Target users

Target user 1	Describe which is the intended user(s) of your solution, considering: <ul style="list-style-type: none"> <li>• The target users are the developers of new software that need to protect their software against vulnerability exploitation.</li> <li>• Additional usage is to protect binaries against vulnerability exploitation.</li> </ul>
---------------	--

## 1.3 Competition

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	87 of 126	
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	
	<b>Version:</b>	1.2	<b>Status:</b>	Final version

#	Name of competitor solution	Company	Strenghts	Weaknesses	Solution unfair advantage
1	Morphisec	Morphisec	Industrial strength,	Weak shuffling, can be bypassed by knowledgeable attacker	
2					
3					

#### 1.4 Distribution model

Distribution model	<ul style="list-style-type: none"> <li>This solution is planned to be distributed as an IBM research asset</li> </ul>
Customer contact	
Promotion means	

#### 1.5 Delivery model

Delivery model	on-premise
----------------	------------

#### 1.6 Customer relationships

Customer relationship	personal assistance
-----------------------	---------------------

#### 1.7 Financial Model

Cost structure	Not applicable
Revenue structure	Not applicable

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	88 of 126	
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	
	<b>Version:</b>	1.2	<b>Status:</b>	Final version



## 2 ExpliSAT exploitation fiche

### 2.1 Component fiche 2

Component name	ExpliSAT
Functionality	Software verification tool based on symbolic interpretation
Key features	Verify C/C++ code and identify security vulnerabilities
Expected TRL	7
Licence	<ul style="list-style-type: none"> <li>• <b>Licensing:</b> The inventor company licenses its software directly to other companies.</li> </ul>
Owner	IBM
Component manager	Sharon Keidar Barner sharon@il.ibm.com

### 2.2 Commercial Assessment of the component

#### 2.2.1 Value proposition

Problem statement	Identifying security vulnerabilities in C/C++ code
Benefits	Indicate: <ul style="list-style-type: none"> <li>• Identifying security vulnerabilities early in the development process</li> <li>• Releasing more secure code which increase the software resiliency to cyber attacks</li> </ul>
Unfair advantage	Expert knowledge in software verification

#### 2.2.2 Target users

Target user 1	Describe which is the intended user(s) of your solution, considering: <ul style="list-style-type: none"> <li>• The target users are the developers of new software that need to amend vulnerable code before they release their products.</li> <li>• Additional usage is to locate the vulnerability after an exploit to provide a timely patch with the right fix.</li> </ul>
---------------	--

#### 2.2.3 Competition

Document name:	D6.2 Annual report on exploitation, dissemination and standardization	Page:	89 of 126				
Reference:	D6.2	Dissemination:	PU	Version:	1.2	Status:	Final version

#	Name of competitor solution	Company	Strengths	Weaknesses	Solution advantage	unfair
1	Coverity	Coverity	Industrial strength, scalable	May give false positives		
2						
3						

### 2.2.4 Distribution model

Distribution model	<ul style="list-style-type: none"> <li>This solution is internally used at IBM</li> <li>In addition, it is distributed as an IBM research asset</li> </ul>
Customer contact	
Promotion means	

### 2.2.5 Delivery model

Delivery model	on-premise
----------------	------------

### 2.2.6 Customer relationships

Customer relationship	personal assistance
-----------------------	---------------------

## 2.3 Financial Model

Cost structure	Not applicable
Revenue structure	Not applicable

## 3.1 Component fiche 3

Component name	AngelEye
Functionality	AngelEye is a tool to create a virtual ahead-of-threat security patch.
Key features	Generate a virtual patch for C/C++ code or executables to protect against security vulnerabilities exploitation
Expected TRL	6
Licence	<ul style="list-style-type: none"> <li><b>Licensing:</b> The inventor company licenses its software directly to other companies.</li> </ul>
Owner	IBM

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	90 of 126	
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	
	<b>Version:</b>	1.2	<b>Status:</b>	Final version

Component manager	Fady Copty fadyc@il.ibm.com
-------------------	-----------------------------

## 3.2 Commercial Assessment of the component

### 3.2.1 Value proposition

Problem statement	Generate a virtual patch for C/C++ code or executables to protect against security vulnerabilities exploitation
Benefits	Indicate: <ul style="list-style-type: none"> <li>• Create a virtual patch of C/C++ application</li> <li>• The virtual patch can predict an input that may trigger a vulnerability before the vulnerability is found by testing technique</li> </ul>
Unfair advantage	Ahead-of-threat patching

### 3.2.2 Target users

Target user 1	Describe which is the intended user(s) of your solution, considering: <ul style="list-style-type: none"> <li>• Developers that want to create polymorphism in their code to obtain better resiliency to ROP attacks</li> <li>• Developers of IoT platforms that want to harden their gateways/endpoints and break the scalability of cyber-attacks on their platform</li> </ul>
---------------	---

### 3.2.3 Competition

#	Name of competitor solution	Company	Strenghts	Weaknesses	Solution unfair advantage
1	TBD				
2					
3					

### 3.2.4 Distribution model

Distribution model	<ul style="list-style-type: none"> <li>• This solution is planned to be distributed as an IBM research asset</li> </ul>
Customer contact	
Promotion means	

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	91 of 126
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU
	<b>Version:</b>	1.2	<b>Status:</b> Final version

### 3.2.5 Delivery model

Delivery model	on premise
----------------	------------

### 3.2.6 Customer relationships

Customer relationship	personal assistance
-----------------------	---------------------

### 3.2.7 Financial Model

Cost structure	Not applicable
TBD	Not applicable

## 4.1 Component fiche 4

Component name	<ul style="list-style-type: none"> <li>• Early Working Intrusion System(EWIS)</li> <li>• DDOS detection system</li> </ul>
Functionality	<ul style="list-style-type: none"> <li>• EWIS is based on honeypots sensors installed into various vantage network points to detect incoming attacks.</li> <li>• A distributed denial of system attack detection system based on the detection of amplification attacks</li> </ul>
Key features	Low-interaction honeypot, Attack detection on known protocols, timely report of the attacks and visualization functionalities,
Expected TRL	<ul style="list-style-type: none"> <li>• EWIS (TRL 7)</li> <li>• DDOS (TRL 4)</li> </ul>
Licence	<ul style="list-style-type: none"> <li>• <b>Open source:</b> <ul style="list-style-type: none"> <li>○ GNU General Public License (GPL)</li> </ul> </li> </ul>
Owner	
Component manager	

## 4.2 Commercial Assessment of EWIS

### 4.2.1 Value proposition

Problem statement	Detecting network based attacks to protocols and services that are running in a real environment without intervening or changing the main setup.
Benefits	EWIS: <ul style="list-style-type: none"> <li>• Lively reporting of attacks happening in the network</li> <li>• Network decoys that appear more “appealing” to the</li> </ul>

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	92 of 126	
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	
	<b>Version:</b>	1.2	<b>Status:</b>	Final version

Unfair advantage	<p>attacker, thus diverting them from attacking the real infrastructure.</p> <ul style="list-style-type: none"> <li>• Detect attack prior to happening to the real system</li> <li>• Emulation of real services that we want to protect</li> </ul>
	<ul style="list-style-type: none"> <li>• The honeypot attack detection system is non-intrusive and minimal changes are needed to the real operational system</li> <li>• Runs in parallel with the SME real infrastructure</li> </ul>

#### 4.2.2 Target users

Target user 1	All SMEs offering services over the internet using protocols like HTTP, SMB, MSSQL, MySQL etc

#### 4.2.3 Competition

- Not applicable as FORTH is a research institution with no access to the real market and all work done is distributed with GNU GPL.

#	Name of competitor solution	Company	Strengths	Weaknesses	Solution unfair advantage
1					
2					
3					

#### 4.2.4 Distribution model

Distribution model	<p>Describe the distribution model of your solution, considering:</p> <ul style="list-style-type: none"> <li>• Indirect channel: The solutions proposed by FORTH can reach the market through products produced in project like SMESEC, or through FORTHcert, which operates under the supervision of FORTH and provides alerts to governmental and non-governmental organizations, to businesses and to the public.</li> </ul>
Customer contact	Contact point: The project's website ( <a href="http://www.smesec.eu">http://www.smesec.eu</a> )
Promotion means	Through SMESEC's dissemination events, blog entries, Workshops etc. Also, through the numerous public deliverables that are going to be produced thought the project's lifetime and through the project's website ( <a href="http://www.smesec.eu">http://www.smesec.eu</a> ) .

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	93 of 126	
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	
	<b>Version:</b>	1.2	<b>Status:</b>	Final version

#### 4.2.5 Delivery model

<b>Delivery model</b>	An on-premises preconfigured Virtual Image that includes the solution
-----------------------	---

#### 4.2.6 Customer relationships

<b>Customer relationship</b>	automated service and personal/technical assistance if needed
------------------------------	---

#### 4.2.7 Financial Model

<b>Cost structure</b>	<ul style="list-style-type: none"> <li>• Not applicable</li> </ul>
<b>Revenue structure</b>	

### 4.3 Commercial Assessment of DDOS solution

#### 4.3.1 Value proposition

<b>Problem statement</b>	Detecting DDoS attack that target the SME Infrastructure
<b>Benefits</b>	DDOS solution: <ul style="list-style-type: none"> <li>• Reporting of DoS attacks happening in the network</li> <li>• Standalone solution can be deployed to the same network we want to protect</li> <li>• Based on the detection of amplification DoS attack no need for extensive network monitoring.</li> </ul>
<b>Unfair advantage</b>	<ul style="list-style-type: none"> <li>• Non-intrusive</li> <li>• Coupled with EWIS system</li> </ul>

#### 4.3.2 Target users

<b>Target user 1</b>	All SMEs offering services over the internet
<b>Target user 2</b>	
<b>Target user 3</b>	

#### 4.3.3 Competition

- Not applicable as FORTH is a research institution with no access to the real market and all work done is distributed with GNU GPL.

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	94 of 126	
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	
	<b>Version:</b>	1.2	<b>Status:</b>	Final version

#	Name of competitor solution	Company	Strenghts	Weaknesses	Solution unfair advantage
1					
2					
3					

#### 4.3.4 Distribution model

Distribution model	Describe the distribution model of your solution, considering: <ul style="list-style-type: none"> <li>Indirect channel: The solutions proposed by FORTH can reach the market through products produced in project like SMESEC, or through FORTHcert, which operates under the supervision of FORTH and provides alerts to governmental and non-governmental organizations, to businesses and to the public.</li> </ul>
Customer contact	Contact point: The project's website ( <a href="http://www.smesec.eu">http://www.smesec.eu</a> )
Promotion means	Through SMESEC's dissemination events, blog entries, Workshops etc. Also, through the numerous public deliverables that are going to be produced thought the project's lifetime and through the project's website ( <a href="http://www.smesec.eu">http://www.smesec.eu</a> ) .

#### 4.3.5 Delivery model

Delivery model	An on-premises preconfigured Virtual Image that includes the solution
----------------	---

#### 4.3.6 Customer relationships

Customer relationship	Automated service and personal/technical assistance if needed
-----------------------	---

#### 4.3.7 Financial Model

Cost structure	<ul style="list-style-type: none"> <li>Not applicable</li> </ul>
Revenue structure	

### 5.1 Component fiche 5

Component name	Risk Assessment Engine (RAE)
Functionality	This tool evaluates the risk faced by companies by executing a modeling algorithm as a set of machine-readable rules: a qualitative model and a quantitative one. The evaluation is done in almost real-time and covers also the analysis of the business profile of the

Document name:	D6.2 Annual report on exploitation, dissemination and standardization	Page:	95 of 126				
Reference:	D6.2	Dissemination:	PU	Version:	1.2	Status:	Final version



	company (specified by the user via configuration), the results of the vulnerability scan and the real-time monitoring of the target infrastructure.
Key features	The RAE provides several models in order to perform more complex analysis of the systems and provide, additionally, a business interpretation of the cyber risks, 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.
Expected TRL	TRL-6
Licence	<p>Indicate the type of license of the component</p> <ul style="list-style-type: none"> <li>• <b>Distribution agreement:</b> The inventor company licenses the software IP to one or more software vendors. Vendors typically pay an upfront fee to the lessor company.</li> <li>• <b>Licensing:</b> The inventor company licenses its software directly to other companies.</li> <li>• <b>Patent.</b></li> <li>• <b>Closed source:</b> Source code is closely guarded, often because it's considered a trade secret that creates scarcity and keeps the organization competitive. Such programs come with restrictions against modifying the software or using it in ways unintended by the original creators: <ul style="list-style-type: none"> <li>○ Freeware</li> <li>○ Shareware</li> </ul> </li> <li>• <b>Open source:</b> <ul style="list-style-type: none"> <li>○ Copyleft</li> <li>○ Apache Software License 2.0</li> <li>○ GNU General Public License (GPL)</li> <li>○ GNU Library or "Lesser" General Public License (LGPL)</li> <li>○ MIT License (MIT)</li> <li>○ Common Development and Distribution License (CDDL)</li> <li>○ Mozilla Public License (MPL)</li> <li>○ Eclipse Public License (EPL)</li> <li>○ Dual-license strategy of commercial open source</li> </ul> </li> </ul>
Owner	Atos
Component manager	Rodrigo Diaz rodrigo.diaz@atos.net

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	96 of 126	
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	
	<b>Version:</b>	1.2	<b>Status:</b>	Final version

## 5.2 Commercial Assessment of the component

### 5.2.1 Value proposition

Problem statement	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.
Benefits	The tool allows a real-time evaluation of the systems by executing qualitative and quantitative models. The assessment is done together with the business profile of the organization, allowing to have specific information about how the risks affect them from a management and financial point of view.
Unfair advantage	Our solution provides information at management and financial level, which helps organizations to have a better overview of the status and assessment of their system.

### 5.2.2 Target users

Target user 1	<p>Main target is the cybersecurity experts of the organizations. They are the ones that work in defining the models for assessment and analyzing the results of the tool. Together with this role it is important also the management level, as, together with the cybersecurity expert, works in defining the impact of the threats at management and financial level.</p> <p>The output will be used by both the cybersecurity expert (for identifying threats and vulnerabilities) and the management role for taking decisions at high-level.</p>
---------------	--

### 5.2.3 Competition

#	Name of competitor	Company	Strengths	Weaknesses	Solution unfair advantage
1	Titania Risk Assessment Tool	Titania	<p>Allows audit against several cyber essential checks and four best practice security checks</p> <p>Discover security gaps creating major risks in your</p>	It doesn't provides decision support for management levels, only analyses of cyber threats without providing information about the impact in the organization	Decision support for management level is very important nowadays, as it helps to guide solutions and strategies to be taken in the organization. Our tool supports this together with recommendations for fulfilling the cyber threats

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	97 of 126
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU
<b>Version:</b>	1.2	<b>Status:</b>	Final version

			business Protect the system against attackers Free version tool		
2	Octave	CERT	Methodology for assessing information security risks Low need of time, people and resources Supports business processes and services	It is only provided as a methodology and it is not supported by a tool Cannot provide automatic processing of threats	Our tool provides almost real-time information of the assessment It supports information for the management level, providing data of the impact and cost of the threats in the assets and services of the organization

#### 5.2.4 Distribution model

Distribution model	Same as with the XL-SIEM, the strategy we will follow will be direct sale of the product to clients. We will do online advertising of the solution in several channels and have direct contact with the clients, offering to support the integration of the tool and explain them how to take advantage of the tool according to their needs.
Customer contact	The channels we will use for selling the RAE are, initially, the website of the project, events where we present it, and internal channels of Atos
Promotion means	We plan to present our solution in several events focusing in cybersecurity for organizations (from SME to large ones) and in events of Atos as a cybersecurity solution for both internal use and external clients

#### 5.2.5 Delivery model

Delivery model	Our solution can be provided either as on-premise (installation in the system of the client) or as a service (providing it to the client from our cloud)
----------------	--

#### 5.2.6 Customer relationships

Customer relationship	TBD
-----------------------	-----

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	98 of 126				
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version

## 5.2.7 Financial Model

Cost structure	<p>Indicate:</p> <ul style="list-style-type: none"> <li>• What is your Capex structure(Purchase of a Building or Property, upgrade to equipment, software upgrade, equipment, infrastructure)</li> <li>• Opex structure (administrative costs, selling costs, advertising costs, travel costs, salaries, utilities, insurance, taxes)</li> <li>• Cost estimation</li> </ul>
Revenue structure	<p>Indicate:</p> <ul style="list-style-type: none"> <li>• Pricing model</li> <li>• Revenue estimation</li> </ul>

## 6.1 Component fiche 6

Component name	Cross-layer SIEM (XL-SIEM)
Functionality	The tool allows, on the one hand detection of intrusions and on the other hand vulnerabilities in the system. Together with this the tool is able to provide remediation activities to known cyber-incidents. It can handle large volumes of data and notify about security alerts from a business perspective thanks to its analysis and event processing.
Key features	Our solution provide, among other characteristics, identification of new and complex attack patterns, high-level risk metrics and correlation rules, user and entity behavior analytics, support for big data analysis, TLS certification for communication between the agents and SIEM, anonymization and encryption of data, an degeneration of heartbeats to monitor the status of the agents
Expected TRL	TRL-7
Licence	<p>Indicate the type of license of the component</p> <ul style="list-style-type: none"> <li>• <b>Distribution agreement:</b> The inventor company licenses the software IP to one or more software vendors. Vendors typically pay an upfront fee to the lessor company.</li> <li>• <b>Licensing:</b> The inventor company licenses its software directly to other companies.</li> <li>• <b>Patent.</b></li> <li>• <b>Closed source:</b> Source code is closely guarded, often because it's considered a trade secret that creates scarcity and keeps the organization competitive. Such programs come with restrictions against modifying the software or using it in ways untended by the original creators: <ul style="list-style-type: none"> <li>○ Freeware</li> </ul> </li> </ul>

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	99 of 126
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU
	<b>Version:</b>	1.2	<b>Status:</b>
			Final version

	<ul style="list-style-type: none"> <li>○ Shareware</li> <li>• <b>Open source:</b> <ul style="list-style-type: none"> <li>○ Copyleft</li> <li>○ Apache Software License 2.0</li> <li>○ GNU General Public License (GPL)</li> <li>○ GNU Library or "Lesser" General Public License (LGPL)</li> <li>○ MIT License (MIT)</li> <li>○ Common Development and Distribution License (CDDL)</li> <li>○ Mozilla Public License (MPL)</li> <li>○ Eclipse Public License (EPL)</li> <li>○ Dual-license strategy of commercial open source</li> </ul> </li> </ul>
Owner	Atos
Component manager	Rodrigo Diaz rodrigo.diaz@atos.net

## 6.2 Commercial Assessment of the component

### 6.2.1 Value proposition

Problem statement	SMEs nowadays are one of the more easy targets for cyber-delinquents. On the one hand they usually work with personal or critical data and, on the other hand, their level of cybersecurity is very low, both from the technology and awareness point of view. That way, cyberattacks and information about the status of cybersecurity of their systems is a need in order to protect their systems and taking decisions regarding cybersecurity.
Benefits	Our tool improves other existing open source solutions in different ways. Among other characteristics, one of the more interesting is the enhancement of the performance and scalability, allowing processing of big amounts of data and having the possibility of performing event correlation at different layers with more complex rules. Additionally, one key objective of the XL-SIEM is to increase the awareness of cybersecurity for the users, which is supported with an interface for visualization that includes high-level charts and diagrams in different dashboards, including decision-support ones.
Unfair advantage	Our solution supports big data processing, more data sources than any other of the competence (e.g. STIX and JSON), personalized dashboards for cybersecurity analysis and awareness, support of TLS certification between agents and the SIEM engine, and anonymization/encryption of normalized fields before transmission, which provides an additional layer of privacy.

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	100 of 126
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU
	<b>Version:</b>	1.2	<b>Status:</b>
			Final version

## 6.2.2 Target users

Target user 1	<p>The main role of our solution is cybersecurity experts of organizations, ranging from SMEs to large organization. This role is the better suit as could take the bigger advantage of the functionalities and information our tool provide, not only from the selection of solutions for their systems but also for refining the information of the cybersecurity status and provide it to other layers of the organization for decision support (e.g. management).</p> <p>Although our solution could be useful for any type of domain, the main target is information technology companies, which either support or work with data (e.g. personal, of organisations, etc.) or provide digital services. In that sense, organizations working with IoT devices, big data, cloud systems or services, etc. would be the ones that take more advantage of our tool.</p>
---------------	--

## 6.2.3 Competition

#	Name of competitor solution	Company	Strengths	Weaknesses	Solution unfair advantage
1	QRadar SIEM	IBM	<p>Integrated view of log and event data with network flow and packets, vulnerability and asset data and threat intelligence</p> <p>Network traffic behavior analysis can be correlated across NetFlow and log events</p> <p>Supports security event and log monitoring in IaaS environments</p> <p>Allows integration of third-party technologies into the SIEM dashboards</p>	<p>Supports mainly midsize and large enterprises</p> <p>Not really supporting bigdata (mainly through third-party solutions)</p> <p>Incident response is not natively integrated in the SIEM</p> <p>Full orchestration and automation of workflow and incident response is only available in the premium solution</p>	<p>Supports any type of organization (ranging from SME to large one)</p> <p>Support of big data analysis</p> <p>Reports include economic assessment (supported by Risk Assessment Tool)</p>
2	ArcSight	HPE	<p>Data enrichment</p> <p>Categorization and normalization of data</p> <p>Multidimensional real-time</p>	<p>Due to the introduction of different functionalities in some cases there is</p>	<p>Different services are specific and do not overlap</p>

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization			<b>Page:</b>	101 of 126		
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version

			<p>correlation</p> <p>Ultra-fast investigation and forensics</p> <p>Out-of-the-box security use cases</p> <p>Workflow automation</p>	<p>duplication of data</p> <p>Licensing can be complicated, with volume-based pricing for ADP, velocity-based pricing for ESM and user-based pricing for UBA</p> <p>It is found to be more complex and expensive to deploy, configure and operate than other leading solutions</p>	<p>Licensing is simple for any type of need or organization</p>
3	Splunk	Splunk Enterprise	<p>Advanced security analytics capabilities are available from both native machine learning functionality and integration with Splunk UBA for more advanced methods, providing advanced threat detection monitoring and inside threats use cases</p> <p>In-house experience and existing infrastructure and data for implementing security monitoring capabilities</p>	<p>Provides only basic predefined correlations for user monitoring and reporting requirements</p> <p>License models are based on data volume in gigabytes indexed per day</p> <p>Requires separate infrastructure and leverages a license model different from other solutions of Splunk</p>	<p>Provides high-level correlation functionality and reporting at different levels of data</p> <p>Easy to deploy and run into a single infrastructure</p> <p>User-friendly configuration of different tools of the SIEM</p>

#### 6.2.4 Distribution model

<b>Distribution model</b>	The strategy we will follow will be direct sale of the product to clients. We will do online advertising of the solution in several channels and have direct contact with the clients, offering to support the integration of the tool and explain them how to take advantage of the tool according to their needs.
<b>Customer contact</b>	The channels for selling the XL-SIEM are the website of the project, events where we present it, and internal channels of Atos
<b>Promotion means</b>	We plan to present our solution in several events focusing in cybersecurity for organizations (from SME to large ones) and in

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	102 of 126	
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	
	<b>Version:</b>	1.2	<b>Status:</b>	Final version



	events of Atos as a cybersecurity solution for both internal use and external clients
--	---

### 6.2.5 Delivery model

Delivery model	Our solution can be provided either as on-premise (installation in the system of the client) or as a service (providing it to the client from our cloud)
----------------	--

### 6.2.6 Customer relationships

Customer relationship	TBD
-----------------------	-----

### 6.2.7 Financial Model

Cost structure	<p>Indicate:</p> <ul style="list-style-type: none"> <li>• What is your Capex structure(Purchase of a Building or Property, upgrade to equipment, software upgrade, equipment, infrastructure)</li> <li>• Opex structure (administrative costs, selling costs, advertising costs, travel costs, salaries, utilities, insurance, taxes)</li> <li>• Cost estimation</li> </ul>
Revenue structure	<p>Indicate:</p> <ul style="list-style-type: none"> <li>• Pricing model</li> <li>• Revenue estimation</li> </ul>

## 7.1 Component fiche 7

Component name	Secure wireless monitoring and data acquisition system
Functionality	Secure and low power IIoT architecture compatible with different sensors
Key features	<ul style="list-style-type: none"> <li>• Long lifespan</li> <li>• High sampling rate</li> <li>• Improved sensor compatibility</li> <li>• Long range communication (radio)</li> <li>• Secure data flow and robust system</li> </ul>
Expected TRL	TRL9
Licence	<ul style="list-style-type: none"> <li>• <b>Closed source:</b> Source code is closely guarded, because it's considered a trade secret that creates scarcity and keeps the organization competitive.</li> </ul>

Document name:	D6.2 Annual report on exploitation, dissemination and standardization	Page:	103 of 126				
Reference:	D6.2	Dissemination:	PU	Version:	1.2	Status:	Final version

Owner	Worldsensing in agreement with the security technology vendors (beneficiaries) within SMESEC
Component manager	Dr. Andrea Bartoli (responsible for the Innovation Department)

## 7.2 Commercial Assessment of the component

### 7.2.1 Value proposition

Problem statement	Adding security features to a commercial product: data securization and improvement of the system robustness
Benefits	<ul style="list-style-type: none"> <li>Quality of service for the target users improved: the system is not easily hacked, and the service continuity is achieved (resilience improvement).</li> <li>Data protection: data are acquired, processed and stored with secure protocols to guarantee their integrity in their whole lifecycle.</li> </ul>
Unfair advantage	Commercial IoT technologies have often neglected the security aspects due to the intrinsic constraints (i.e. low power consumption requirements). The adoption of new security features in Worldsensing' solution turns into a disruptive step forward in the market niche of IIoT, providing a unique competitive advantage to the company.

### 7.2.2 Target users

Target user 1	The intended users of the “evolved” solution of Worldsensing are basically the same than those from the already-commercial product LoadSensing. By adding new features to this new release of LoadSensing, Worldsensing aims to improve the market penetration offering a differentiating factor regarding the competence. Right now, LoadSensing is addressed worldwide to city and infrastructure operators, construction companies and mines operators mainly.
Target user 2	
....	

### 7.2.3 Competition

- Indicate similar existing solutions in the market or in the R&D field.
- For each identified competitor, indicate its strengths and weaknesses.
- For each identified competitor, indicate what the advantage is provided by XXX.

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	104 of 126	
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	
	<b>Version:</b>	1.2	<b>Status:</b>	Final version

None of the competitors offer security features in their solutions

#	Name of competitor solution	Company	Strenghts	Weaknesses	Solution unfair advantage
1	GeonNet Wireless	Geokon	Low cost	Short lifespan  No software-based solution and limited data download capabilities  Limited range	Cost-effective solution for some applications
2	L900 RSTAR Array	RST	Long lifespan  Number of nodes high enough for many applications  Easy node installation  Radio range good enough	Difficult installation (network)  No software-based solution and limited data download capabilities  High-cost	High sensor compatibility
3	CRVW3	Campbell	High sampling rate  Sensor compatibility	Short lifespan  Difficult installation (nodes and network)  No software-based solution and limited data download capabilities  High-cost  Poor radio reception	Extremely-high sensor compatibility

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization			<b>Page:</b>	105 of 126
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2
				<b>Status:</b>	Final version

#### 7.2.4 Distribution model

Distribution model	<ul style="list-style-type: none"> <li>• Direct sale: sale of a product or solution by means of the work force by means of face-to-face meetings, inside sales (phone, email) or online (internet) to reach customers.</li> <li>• Indirect channel: sale of the good by a third-party, such as a partner or affiliate.</li> </ul>
Customer contact	organization website, fairs and direct F2F meetings
Promotion means	Marketing campaign (website, newsletter to current customers, social media) and presentation in key fairs.

#### 7.2.5 Delivery model

Delivery model	The solution of the current LoadSensing product is served to the customer on-premise. The system acquires the nodes and the gateways and deploy them in the final venue with the support of Worldsensing staff. In the process of moving towards a more software-based product, other options are being considered, such as SaaS (to be decided).
----------------	---

#### 7.2.6 Customer relationships

Customer relationship	Right now, the customer relationship is self-service with personal technical assistance.
-----------------------	--

#### 7.2.7 Financial Model

Cost structure	<p>CAPEX</p> <ul style="list-style-type: none"> <li>• upgrade od equipment: some of the elements of LoadSensing will be modified to be powerful enough to adopt security solutions with guarantees.</li> <li>• software upgrade: the firmware of the elements and the software will be modified to run the adopted security solutions.</li> <li>• infrastructure: A Cloud infrastructure will be developed to act as a backend of the data processing solution (Operational Intelligence capabilities). This is only feasibly once the entire solution is securized to avoid an undesired risk propagation</li> </ul> <p>Opex structure: once the new solution is in place, the extra cost from an opex point of view will be the extra resources necessary (upgraded hardware and servers in the cloud (hosting), and the license of the security solutions offered by the vendors (to be decided)</p>
----------------	---

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	106 of 126	
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	
	<b>Version:</b>	1.2	<b>Status:</b>	Final version

Revenue structure	Pricing model – First payment for the hardware and general license to the software (data platform) suite. Later, regular fees for the license to the security functionalities and ad-hoc data services (operational intelligence capabilities). To be decided in the coming months
-------------------	--

## 8.1 Component fiche 8

Component name	Endpoint Protection Platform
Functionality	<p>GravityZone is a business security solution built from ground-up for virtualization and cloud to deliver security services to physical endpoints, mobile devices, virtual machines in private, public cloud and Exchange mail servers.</p> <p>GravityZone is one product with a unified management console available in the cloud, hosted by Bitdefender, or as one virtual appliance to be installed on company's premises, and it provides a single point for deploying, enforcing and managing security policies for any number of endpoints and of any type, in any location.</p> <p>GravityZone delivers multiple layers of security for endpoints and for Microsoft Exchange mail servers: antimalware with behavioral monitoring, zero day threat protection, application control and sandboxing, firewall, device control, content control, anti-phishing and antispyware.</p> <p>GravityZone provides the following security services:</p> <ul style="list-style-type: none"> <li>● <i>Security for Endpoints</i></li> <li>● <i>Security for Virtualized Environments</i></li> <li>● <i>Security for Exchange</i></li> <li>● <i>Security for Mobile</i></li> <li>● <i>Hypervisor Memory Introspection</i></li> </ul>
Key features	<p><b>Advanced application behaviour monitoring</b></p> <p>Bitdefender Advanced Threat Control (ATC) permanently monitors running processes for signs of malicious behaviour. A pioneering technology launched in 2008 as AVC, ATC has constantly been enhanced, keeping Bitdefender one step ahead of emerging threats.</p> <p><b>Largest security intelligence cloud</b></p> <p>With over 500 million machines protected, the Bitdefender Global Protective Network performs 11 Billion queries per day and uses</p>

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	107 of 126	
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	
	<b>Version:</b>	1.2	<b>Status:</b>	Final version

	<p>machine learning and event correlation to detect threats without slowing down users.</p> <p><b>AI and machine learning perfected in years</b></p> <p>Artificial Intelligence and machine learning are essential to combat a threat landscape that is larger and more sophisticated than ever. Unlike other vendors, Bitdefender has years of experience in perfecting these technologies and the results clearly show this: better detection rates with fewer false positives.</p>
Expected TRL	TRL8-9
Licence	Distribution agreement: The inventor company licenses the software IP to one or more software vendors. Vendors typically pay an upfront fee to the lessor company.
Owner	Licensing: The inventor company licenses its software directly to other companies.
Component manager	Ovidiu Costel

## 8.2 Commercial Assessment of the component

All components described in the previous section address networking and cyber-security issues and are commercially placed in a similar manner to the overall market. In addition, the aforementioned components can be purchased bundled or separately and be deployed in private datacenters, independently hosted, or over the cloud, following the as-a-Service deployment scheme.

### 8.2.1 Value proposition

Problem statement	<p>Context</p> <p>Providing solutions that are capable of securing SMEs from attacks has never been a more challenging and pressing issue. There has been a rise in attacks against SMEs. The common denominator of these attacks is that they are all using malware or exploit vulnerabilities that antimalware solutions can efficiently block.</p> <p>Given the growing complexity and interconnectivity of the different building blocks and components the attack surface has greatly</p>
-------------------	--

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	108 of 126				
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version

Benefits	<p>increased. Furthermore, better targeted social engineering from hackers and attackers leads successful attacks that can penetrate highly ranked individuals inside organizations and open new opportunities for lateral moves and persistence inside networks that manage or control the SMEs.</p> <p>At this point an attacker that has enough money can buy full-fledged solutions for cyber espionage against complex targets with features that would enable passing through air-gapped networks, strong encryption for data exfiltration, persistence modules, command and control infrastructures, stealth or hidden communication techniques.</p> <p>Another layer of complexity to this problem is given by the fast adoption of IoT's inside SMEs networks and organizations. Smart and interconnected, these new devices leave at the edge of the network and can be used either as bridge heads to get inside the network or as direct target themselves. The lack of security standards, the market fragmentation pose a big security issue that can be address by using complex security solutions.</p> <p>Security solutions should be capable of providing a complete and layered approach that protects endpoints (both infrastructure and end-user endpoints), IoT devices and communications against malicious threats. Such a solution needs to be capable of predicting attacks through vulnerability assessments, preventing or detecting attacks at any point in the attack kill chain, and offer full remediation capabilities to reduce the risk, limit the payload execution or fix the affected systems.</p>
----------	---

### 8.2.2 Target users

Target users	<ul style="list-style-type: none"> <li>• Bitdefender is already addressing the global market, encompassing Start-ups, SMEs and Large Corporations, usually seeking contact with the CIO or the cybersecurity responsible of the targeted organisation.</li> </ul>
--------------	---

### 8.2.3 Competition

Main competitors	Bitdefender's main competitors that have a commercial solution that can be considered suitable for securing SMEs are Karsperky, McAfee,
------------------	---

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	109 of 126				
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version

Sophos, Symantec and Trend Micro.

#### 8.2.4 Distribution model

Distribution model	<p>Bitdefender has been investigating how to better position itself within the SMEs market. Therefore, the following actions have been performed during the 1st year of implementation:</p> <ol style="list-style-type: none"> <li>1) Analysis of key-providers of protective solutions for SMEs;</li> <li>2) Discussion with the rest of SMESEC partners (Worldsensing, ATOS etc.) to identify common approaches for SMESEC commercialisation;</li> <li>3) Preliminary discussions with Romanian companies considering the good understanding of local conditions.</li> </ol> <p>The commercial strategy will follow the existing proven commercialisation approach which stands on multiple marketing channels (B2B via online channel, B2B via direct contact, B2B via partnerships and B2B via conferences and thematic industry-events) supported by appropriate funnels (awareness, consideration, acquisition and retention).</p> <p>Bitdefender is participating as well in another Horizon2020 projects which is a good channel of information and good practices exchange.</p>
Customer contact	TBD
Promotion means	TBD

#### 8.2.5 Delivery model

Delivery model	TBD
----------------	-----

#### 8.2.6 Customer relationships

Customer relationship	TBD
-----------------------	-----

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	110 of 126	
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	
	<b>Version:</b>	1.2	<b>Status:</b>	Final version



## 9.1 Component fiche 9

Component name	NetScaler AppFirewall
Functionality	<p>Citrix NetScaler AppFirewall is a comprehensive web application firewall that analyzes all bi-directional traffic, including SSL-encrypted communication, to protect against a broad range of security threats. It provides the ability to perform deep-packet inspection of HTTP(S) and XML as well as protection against OWASP top 10. NetScaler AppFirewall threat protection includes and is not limited to SQL injection attacks, cross-site scripting attacks, cookie tampering, form validation and protection, HTTP and XML reply and request format validation, JSON payload inspection, signature and behavior based protections, data loss prevention (DLP) support including the monitoring of traffic for intended and unintended data exposure, DoS protection, authentication, authorization and auditing support and reporting.</p>
Key features	<p>NetScaler AppFirewall</p> <ul style="list-style-type: none"> <li>▪ Comprehensively addresses the challenge of delivering centralized application- layer security for all web applications and web services</li> <li>▪ Uses a hybrid security model by enforcing both positive and negative security models to ensure proper application behavior</li> <li>▪ Thwarts a variety of DoS attacks, including external entity references, recursive expansion, excessive nesting and malicious messages containing either long or a large number of attributes and elements.</li> <li>▪ Incorporates an advanced and proven adaptive learning engine that discovers aspects of application behavior that might be blocked by the positive security model</li> <li>▪ Permits flexible, stepwise deployment of web application protection.</li> </ul>
Expected TRL	TRL-9
Licence	Closed source: Source code is closely guarded, often because it's considered a trade secret that creates scarcity and keeps the

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	111 of 126				
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version

	<p>organization competitive. Such programs come with restrictions against modifying the software or using it in ways unintended by the original creators</p> <p>Customers purchase licenses that allow on premise software deployment (VPX) or purchase a customized plug-and-play hardware box (MPX)</p>
Owner	Citrix Systems Inc.
Component manager	N/A

Component name	<b>NetScaler Gateway</b>
Functionality	<p>Implementing a traditional SSL VPN solution or an IDaaS (IDaaS) solution will not provide single sign-on (SSO) to all applications and data. While an SSL VPN will provide network access and SSO to applications in a datacenter, an IDaaS solution will just provide SSO to applications in the cloud or delivered as SaaS.</p> <p>NetScaler Gateway provides users with one access point and SSO to business applications and data deployed in a datacenter, the cloud, or delivered as SaaS across a range of devices—laptops, desktops, thin clients, tablets, and smart phones. It provides consolidation; helps reduce the footprint of remote access infrastructure; reduces cost; and provides ease of management and a better end-user experience.</p>
Key features	<p>NetScaler Gateway</p> <ul style="list-style-type: none"> <li>▪ Provides federated identity and supports SAML 2.0, OAuth, and OpenID to achieve single sign-on across all applications whether they are web, VDI, enterprise, or SaaS applications.</li> <li>▪ Provides a single URL and consolidates remote access infrastructure allowing any affiliated device to access any available application.</li> <li>▪ Allows IT administrators to define and enforce access</li> </ul>

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	112 of 126	
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	
	<b>Version:</b>	1.2	<b>Status:</b>	Final version

	control policies based on certain parameters like state of the end-user device, location of the user, and applications being accessed. IT administrators can prioritize policies to be enforced if a user is part of multiple groups and sub-domains.
Expected TRL	TRL-8
Licence	<p><b>Closed source:</b> Source code is closely guarded, often because it's considered a trade secret that creates scarcity and keeps the organization competitive. Such programs come with restrictions against modifying the software or using it in ways unintended by the original creators</p> <p>Customers purchase licenses that allow on premise software deployment</p>
Owner	Citrix Systems Inc.
Component manager	N/A

Component name	<b>NetScaler Secure Web Gateway</b>
Functionality	NetScaler Secure Web Gateway (NetScaler SWG) is a solution that enables organizations to cost-effectively eliminate blind spots within their environment and strengthen their security posture through efficient SSL decryption. With NetScaler SWG, organizations have the visibility and control they need over encrypted traffic to ensure compliance with their privacy, regulatory, and acceptable user policies. NetScaler SWG is uniquely positioned in the network to allow high-capacity, high-performance web security.
Key features	NetScaler SWG is capable of

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	113 of 126				
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version

	<ul style="list-style-type: none"> <li>▪ Addressing main security challenges through advanced traffic inspection, intrusion blocking, malware elimination, and application control.</li> <li>▪ Selectively decrypt traffic.</li> <li>▪ Accessing User behavior analytics and provide extensive reporting.</li> <li>▪ Enforce tailor-made security policies and closely monitor user transactions.</li> </ul> <p>Purpose-build NetScaler SWG appliances use dedicated SSL acceleration processors that can scale to handle up to 80K 2048-bit SSL handshakes per second.</p>
Expected TRL	TRL-7
Licence	<p><b>Closed source:</b> Source code is closely guarded, often because it's considered a trade secret that creates scarcity and keeps the organization competitive. Such programs come with restrictions against modifying the software or using it in ways unintended by the original creators.</p> <p>Customers purchase licenses that allow on premise software deployment or custom hardware which allows plug and play functionality and industry-leading performance.</p>
Owner	Citrix Systems Inc.
Component manager	N/A

## 9.2 Commercial Assessment of the component

All components described in the previous section address networking and cyber-security issues and are commercially placed in a similar manner to the overall market. In addition, the aforementioned components can be purchased bundled or separately and be deployed in private datacenters, independently hosted, or over the cloud, following the as-a-Service deployment scheme.

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	114 of 126	
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	
	<b>Version:</b>	1.2	<b>Status:</b>	Final version

## 9.2.1 Value proposition

### A. NetScaler AppFirewall

Problem statement	Although traditional network firewalls and intrusion prevention systems are useful for screening out high volumes of lower-layer threats, they are considerably less capable of defending against the increasingly targeted, application-specific threats routinely being used against organizations today. Despite delivering markedly improved granularity for controlling access to network resources, even next-generation firewalls fall short in the critical area of web property protection.
Benefits	<b>NetScaler AppFirewall</b> is a comprehensive web application firewall that analyzes all bi-directional traffic, including SSL-encrypted communication, to protect against a broad range of security threats.

### B. NetScaler Gateway

Problem statement	Single sign-on solutions are meant to reduce cost of management, provide better security and an improved user experience, but with the evolution of applications and distributed architectural frameworks, most solutions fail to deliver these advantages. Making the wrong choice when choosing an SSO solution can result in a need for multi-vendor solutions, poor integration, a costly investment price, poor user experience and reduce productivity.
Benefits	<b>NetScaler Gateway</b> provides users with one access point and single sign-on (SSO) to business applications and data deployed in a datacenter, the cloud, or delivered as SaaS across a range of devices.

### C. NetScaler Secure Web Gateway

Problem statement	With the exponential growth in web traffic and SaaS apps, customers need complete visibility and control over their web traffic. This includes visibility into encrypted traffic that helps customers to apply their corporate policies and block malicious content to protect their users and endpoints.
-------------------	---

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	115 of 126	
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	
	<b>Version:</b>	1.2	<b>Status:</b>	Final version

Benefits	<p><b>NetScaler Secure Web Gateway</b> addresses main security challenges through advanced traffic inspection, intrusion blocking, malware elimination, and application control</p>
----------	---

### 9.2.2 Target users

Target users	<ul style="list-style-type: none"> <li>Networking Vendors / Large Enterprises</li> <li>Key Networking Industry players</li> <li>SME, SMB, Large companies</li> </ul>
--------------	--

### 9.2.3 Competition

Detailed information for competitive solutions can be found in the attached SMESEC Competitive Landscape document.

### 9.2.4 Distribution model

Distribution model	<p>Citrix Systems Inc. follows diverse distribution models for each provided solution which include but are not limited to:</p> <ul style="list-style-type: none"> <li>Answering to RFPs issued by large vendors, leading to PoC and Trial deployments.</li> <li>Direct sales: where the actual sale of a product or solution is conducted through of face-to-face meetings, inside sales (phone, email) or online (internet) to reach customers.</li> <li>Indirect channels, where the actual sale of a good or service is conducted by a third-party, such as a partner or affiliate, rather than a company's personnel.</li> </ul>
Customer contact	<ul style="list-style-type: none"> <li>Publicly available RFPs</li> <li>PoC/Trials</li> <li>Live demonstration</li> </ul>
Promotion means	<ul style="list-style-type: none"> <li>Large business venues i.e. Citrix Synergy (<a href="https://www.citrixsynergy.com">https://www.citrixsynergy.com</a>) or Mobile World Congress (<a href="https://www.mobileworldcongress.com">https://www.mobileworldcongress.com</a>)</li> </ul>

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	116 of 126				
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version

	<ul style="list-style-type: none"> <li>▪ Independent Trials and PoC deployment</li> <li>▪ Events and Webinars</li> <li>▪ Providing Training and Certification</li> <li>▪ Articles and Insights</li> <li>▪ Citrix Community (<a href="https://www.citrix.com/community/">https://www.citrix.com/community/</a>)</li> <li>▪ Active Blogging platform (<a href="https://www.citrix.com/blogs/">https://www.citrix.com/blogs/</a>)</li> </ul>
--	---

### 9.2.5 Delivery model

Delivery model	<ul style="list-style-type: none"> <li>▪ On-premise</li> <li>▪ Hosted in third-party datacentres</li> <li>▪ Over the cloud, following the as--Service scheme</li> </ul>
----------------	---

### 9.2.6 Customer relationships

Customer relationship	<p>Citrix Systems Inc. always puts customer satisfaction above everything else, it has therefore created diverse customer support mechanisms including but are not limited to:</p> <ul style="list-style-type: none"> <li>▪ Personal assistance</li> <li>▪ Automated services</li> <li>▪ Highly active community</li> </ul>
-----------------------	---

## 10.1 Component fiche 10

Component name	Information security assessment model
Functionality	Overarching and personalized maturity model for maturity assessment and incremental organizational capability improvement throughout all security domains.
Key features	<p>Overarching security domains.          Specific to SME's.          Personalized advice for incremental improvement.          Maintainability. (adaptable to everchanging standards)          Transparent to underlying standards.</p>

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	117 of 126	
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	
	<b>Version:</b>	1.2	<b>Status:</b>	Final version

Expected TRL	7
Licence	<ul style="list-style-type: none"> <li>• <b>Open source:</b> GNU General Public License (GPL)</li> </ul>
Owner	Utrecht University
Component manager	Dr. Marco Spruit, m.r.spruit@uu.nl

## 10.2 Commercial Assessment of the component

### 10.2.1 Value proposition

Problem statement	There is a lack of harmonized, modular, federative and standards compliant security maturity model that can be easily utilized by SMEs. SMEs are not able to evaluate their information security capabilities and maturity level and they are not able to establish where and how to start their improvement initiatives.
Benefits	<ul style="list-style-type: none"> <li>• SMEs will be able to conduct self-assessments on their information security capabilities.</li> <li>• SMEs will be able to better understand information security requirements, their dependencies and associate these requirements with the standards.</li> <li>• SMEs will be able to formulate their personalized improvement plans for their desired improvement path.</li> <li>• SMEs will be able to compare their information security capabilities with other SME's.</li> </ul>
Unfair advantage	There is currently no other overarching information security maturity model targeted for SMEs.

### 10.2.2 Target users

Target user 1	Regardless of the industry, information security maturity model could be used by any SME. The usage of the maturity model requires basic knowledge on information security and information technology concepts.
Target user 2	
....	

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	118 of 126	
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	
	<b>Version:</b>	1.2	<b>Status:</b>	Final version



### 10.2.3 Competition

- Not applicable as Utrecht University is a research institution with no access to the real market and all work done is distributed with GNU GPL. However, the affiliated spin-off Spru IT BV is available for professional services.

#	Name of competitor solution	Company	Strengths	Weaknesses	Solution unfair advantage
1					
2					
3					

### 10.2.4 Distribution model

Distribution model	<p>Indirect channel: The models proposed by Utrecht University can reach the market through products produced in project like SMESEC, or through Utrecht University.</p> <p>Direct channel: Spru IT BV for professional support.</p>
Customer contact	<p>The project's website (<a href="http://www.smesec.eu">http://www.smesec.eu</a>)</p> <p>Utrecht University website (<a href="http://www.uu.nl">http://www.uu.nl</a>)</p> <p>Spru IT BV (<a href="mailto:marco@spru.it">marco@spru.it</a>)</p>
Promotion means	<p>Through SMESEC's dissemination events, blog entries, workshops, journal and conference publications. Also, through the numerous public deliverables that are going to be produced through the project's lifetime and through the project's website (<a href="http://www.smesec.eu">http://www.smesec.eu</a>). Finally, via commercialisation activities of Spru IT BV.</p>

### 10.2.5 Delivery model

Delivery model	<p>The information security maturity model is planned to be delivered as a stand-alone prototype/application that would be downloaded to the SME's environment. Furthermore, the model may be integrated into a commercial web and/or mobile app by Spru IT BV.</p>
----------------	---

### 10.2.6 Customer relationships

Customer relationship	<p>Self-service, off-line personal assistance if needed. Professional support by Spru IT BV.</p>
-----------------------	--

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	119 of 126	
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	
	<b>Version:</b>	1.2	<b>Status:</b>	Final version

## 10.2.7 Financial Model

Cost structure	To be defined
Revenue structure	To be defined

## 11.1 Component fiche 11

Component name	Cybersecurity Coach (CYSEC)
Functionality	Offers support for cybersecurity capability assessment, planning, and tracking
Key features	In comparison to consultants: allows do-it-yourself capability improvements In comparison to training tools: guides through the journey of capability improvements.
Expected TRL	7
Licence	Dual-license with selected elements being MIT.
Owner	FHNW
Component manager	<a href="mailto:samuel.fricker@fhnw.ch">samuel.fricker@fhnw.ch</a>

## 11.2 Commercial Assessment of the component

### 11.2.1 Value proposition

Problem statement	Cybersecurity is overwhelming and requires domain knowledge and tenacity to apply.
Benefits	CYSEC offers step-by-step guidance, reminders, and indicators giving confidence that cybersecurity has been adequately implemented in the end-user organization.
Unfair advantage	Knowledge and expertise in cybersecurity, incremental capability improvements, and self-adaptive personalization.

### 11.2.2 Target users

Target user 1	Market: SME with low awareness and cybersecurity capabilities (horizontal) Industry: horizontal cybersecurity. Initial pilots with SMESEC use case SMEs. Geographical area: Europe, English-speaking with first priority.
---------------	---

Document name:	D6.2 Annual report on exploitation, dissemination and standardization	Page:	120 of 126				
Reference:	D6.2	Dissemination:	PU	Version:	1.2	Status:	Final version

Target user 2 ....	Role: chief security officer

### 11.2.3 Competition

- Indicate similar existing solutions in the market or in the R&D field.
- For each identified competitor, indicate its strengths and weaknesses.
- For each identified competitor, indicate what the advantage is provided by XXX.

#	Name of competitor solution	Company	Strengths	Weaknesses	Solution unfair advantage
1	CYSFAM	Uni Utrecht	Incremental capability improvement	Too complex for SME do-it-yourself	Self-adaptive coach
2	ISFAM	Uni Utrecht	Incremental capability improvement	Too complex for SME do-it-yourself	Self-adaptive coach
3					

### 11.2.4 Distribution model

Distribution model	Registration or download from SMESEC website, delivery of ordered hardware.
Customer contact	SMESEC website.
Promotion means	SMESEC dissemination efforts.

### 11.2.5 Delivery model

Delivery model	SaaS, deployed as a software on-premise, deployed as a hardware device on-premise.
----------------	--

### 11.2.6 Customer relationships

Customer relationship	Self-service, personal assistance
-----------------------	-----------------------------------

### 11.2.7 Financial Model

Cost structure	CAPEX most important investments: software development, incremental capability improvement journey (empirical research),
----------------	--

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	121 of 126				
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version

Revenue structure	<p>validation with SME end-users.</p> <p>OPEX most important costs: hosting of SaaS, production of hardware variant, cost of product organization (maintenance, marketing, sales, distribution, service, support).</p> <p>Cost estimation during SMESEC project: 530 kCHF.</p>
	<ul style="list-style-type: none"> <li>• Hardware: cost per item.</li> <li>• Hardware, SaaS, on-premise: license fees including updates.</li> <li>• Estimated revenue: TBD.</li> </ul>

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization			<b>Page:</b>	122 of 126	
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b> Final version

## 12 TaaS platform exploitation fiche

### 12.1 Component fiche 12

Component name	TaaS Platform
Functionality	Lightweight Testing as a service platform
Key features	End to end and in depth testing of solutions and implementations.
Expected TRL	7
Licence	<ul style="list-style-type: none"> <li>• <b>Licensing:</b> The inventor company licenses its software directly to other testing laboratories.</li> <li>• <b>Internal component:</b> The tool is an internal resource for EGM consultancy offer.</li> </ul>
Owner	Easy Global Market SAS
Component manager	expertise@eglobalmark.com

### 12.2 Commercial Assessment of the component

#### 12.2.1 Value proposition

Problem statement	Testing is cost and time consuming for small organizations and requires technical and advanced knowledge. The TaaS platform hence offers testing platform with reactiveness in each software/implementation development process.
Benefits	<ul style="list-style-type: none"> <li>• Benefits for the target users <ul style="list-style-type: none"> <li>○ Flexibility – Lightweight offer without integration or maintenance phases</li> <li>○ Modularity – Modular and flexible infrastructure</li> <li>○ Reactivity and quality – MBT powered tool enabling fast integration of new security standards or customer test suites, full test coverage and traceability</li> </ul> </li> <li>• Added value for the target users <ul style="list-style-type: none"> <li>○ Cost efficient – No maintenance cost, efficiency in software development with non-regression testing, continuous testing during the development phase.</li> <li>○ Quality oriented – User-friendly interface, full details testing reports, fully customizable</li> </ul> </li> </ul>
Unfair advantage	The TaaS platform is based on a modular architecture able to execute test suites. EGM uses open and well-known standards such as TTCN-3, guarantee of state-of-the-art testing. The tool also offer

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	123 of 126				
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version

end to end testing able to test the solution or implementation in near-real conditions.

### 12.2.2 Target users

Target user 1	Describe which is the intended user(s) of your solution, considering: <ul style="list-style-type: none"> <li>Market addressed: ICT companies</li> <li>Specific industry more suited for the component: IT related SMEs especially in IoT such as system integrators</li> <li>Specific size of organization being targeted: SME</li> <li>Geographical area: Europe</li> <li>Role in the organization: Test engineer, Security analyst</li> </ul>
Target user 2	<ul style="list-style-type: none"> <li>Market addressed: Testing laboratories</li> <li>Specific industry more suited for the component: IT Certification centres</li> <li>Specific size of organization being targeted: SME, Large company)</li> <li>Geographical area: Europe</li> <li>Role in the organization: Test engineer, Security analyst</li> </ul>
....	

### 12.2.3 Competition

- No known similar existing solutions in the market or in the R&D field. Custom-made solutions for each pilot.

### 12.2.4 Distribution model

Distribution model	<ul style="list-style-type: none"> <li>Direct sale: sale of a product or solution by means of the work force by means of face-to-face meetings, inside sales (phone, email) or online (internet) to reach customers.</li> </ul>
Customer contact	Organization website
Promotion means	Website activities and promotion in relevant events and conferences, part of the ARMOUR security centre of excellence.

### 12.2.5 Delivery model

Delivery model	aaS
----------------	-----

### 12.2.6 Customer relationships

Customer	Self-service with personal assistance
----------	---------------------------------------

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization	<b>Page:</b>	124 of 126				
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b>	Final version

relationship

### 12.2.7 Financial Model

Cost structure

- Personnel costs for platform development - Infrastructure maintenance and hosting services

Revenue structure

- Customers access fees, associated consulting activity

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization			<b>Page:</b>	125 of 126	
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b> Final version

## References

- [1] Grant Agreement SMESEC Number 740787
- [2] [https://ec.europa.eu/jrc/sites/jrcsh/files/annual\\_report\\_-\\_eu\\_smes\\_2015-16.pdf](https://ec.europa.eu/jrc/sites/jrcsh/files/annual_report_-_eu_smes_2015-16.pdf) SMESEC, D6.1 Dissemination plan and market analysis, Giunta Nicolas, 2018.
- [3] SMESEC, D2.1 SMESEC security characteristics description, security and market analysis report, George Oikonomou, 2017.
- [4] European Commission, ANNUAL REPORT ON EUROPEAN SMEs [https://ec.europa.eu/jrc/sites/jrcsh/files/annual\\_report\\_-\\_eu\\_smes\\_2015-16.pdf](https://ec.europa.eu/jrc/sites/jrcsh/files/annual_report_-_eu_smes_2015-16.pdf), retrieved date 2017-11-14
- [5] KBV Research, Europe IoT Data Management Market, <https://kbvresearch.com/europe-iot-data-management-market/>, retrieved date 2017-11-14
- [6] European Commission, Energy, <https://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters>, retrieved date 2017-11-14
- [7] e-voting.cc , Market Overview, <https://www.e-voting.cc/en/market-overview/>. retrieved date 2017-11-14
- [8] FireCompass.com, Security Market Analysis, <https://www.firecompass.com/about/>
- [9] Mendelow, A. (1991) ‘Stakeholder Mapping’.
- [10] [2017 Rolling Plan for ICT Standardisation](#)
- [11] [2018 Rolling Plan for ICT Standardisation](#)
- [12] [ECSO Overview of existing Cybersecurity standards and certification schemes](#)
- [13] [http://ec.europa.eu/eurostat/statistics-explained/index.php/ICT\\_security\\_in\\_enterprises](http://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_security_in_enterprises)
- [14] [SMESEC D6.1 Dissemination plan and market analysis, SMESEC consortium, Dec 2017](#)

<b>Document name:</b>	D6.2 Annual report on exploitation, dissemination and standardization			<b>Page:</b>	126 of 126	
<b>Reference:</b>	D6.2	<b>Dissemination:</b>	PU	<b>Version:</b>	1.2	<b>Status:</b> Final version