Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

SMESEC

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

D3.2 SMESEC Unified Architecture – First Internal Release

Document Identification			
Status	Final	**Due Date**	30/11/2018
Version	1.0	**Submission Date**	19/12/2018

Related WP	WP3	**Document Reference**	D3.2
Related Deliverable(s)	D3.1	**Dissemination Level (*)**	PU
Lead Organization	IBM	**Lead Author**	Fady Copty
Contributors	ATOS, FNHW, FORTH, WoS, Citrix, BD	**Reviewers**	Jose F. Ruiz (ATOS) Sotiris Ioannidis (FORTH)

Keywords:

security, system, design, architecture, integration, WP3, requirements, stakeholder, goals, innovation, use case, protection, defence, management, context, concept, pattern, composition, interface, rationale, sequence, orchestration, security operations centre, functionalities.

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

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

Document Information

List of Contributors	
Name	Partner
Fady Copty	IBM
Manos Athanatos, Christos Papachristos, Sotiris Ioannidis	FORTH
Alberto Miranda, Jose Francisco Ruiz, Pablo Barrientos Lobato	ATOS
Olmo Rayón	WoS
Ciprian Oprisa	BD
Samuel Fricker, Martin Gwerder, Ulrike Schock	FHNW

Document History			
Version	Date	Change editors	Changes
0.0	15/10/18	Fady Copty (IBM)	Initial version of table of contents based on D3.1
0.1	15/11/18	Manos Athanatos (FORTH)	Section 2 and Annex A
		Alberto Miranda (ATOS)	Section 3 introduction
		Olmo Rayón (WoS)	Section 5.1.6 – external API, and 6.5
		Fady Copty (IBM)	Section 3, 4, 5.1.1, 7
0.2	21/11/18	Ciprian Oprisa (BD)	Update section 6.2, 6.4
		Fady Copty (IBM)	Section 1
		Samuel Fricker, Martin Gwerder, Ulrike Schock (FHNW)	SMESEC user interface – section 5.2.
		Jose Francisco Ruiz, Pablo Barrientos Lobato	Sections 5.1.1, 5.1.4, 5.1.6, 6.2, 6.5 and 7
0.3	06/12/18	Fady Copty	Rewrite section 5
0.4	07/12/18	Fady Copty	Rewrite section 6
0.5	10/12/18	Fady Copty	Update references, figure, and tables

0.6	13/12/18	Jose Francisco Ruiz (ATOS), Christos Tselios (Citrix)	Review and update
0.7	14/12/18	Fady Copty	Answer all review comments
0.8	18/12/18	Fady Copty	Clean version
1.0	19/12/18	ATOS	Quality review, Submission.

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Fady Copty (ATOS)	19/12/2018
Technical manager	Christos Tselios (Citrix)	30/11/2018
Quality manager	Rosana Valle Soriano (Atos)	19/12/2018
Project Manager	Jose Fran. Ruíz (Atos)	19/12/2018

Table of Contents

List of Tables

List of Figures

List of Acronyms

Abbreviation / acronym	Description
API	Application Programming Interface
APT	Advanced Persistent Threat
AST	Application Security Testing
AV	Anti-Virus
CISO	Chief Information Security Officer
CISSP	Certified Information Systems Security Professional
CVE	Common Vulnerabilities and Exposures
DDoS	Distributed Denial of Service (network attack; also seen as DDSA)
DT	Deception Technology
Dx.y	Deliverable number y belonging to WP x
DoA	Document of Action
EC	European Commission
EPP	Endpoint Protection Platform
GRC	Governance, Risk Management and Compliance
HTTP	Hyper Text Transfer Protocol
HTTPS	HTTP Secure
IaaS	Infrastructure as a Service
IC	Innovation Committee
IDSISO	Intrusion Protection System International Organization for Standardisation
IDS	Intrusion Detection System
IoT	Internet of things
IP	Internet Protocol
ISFCISSP	Information Security Forum Certified Information Systems Security Professional
ISFAM	Information Security Focus Area Maturity
ISOISF	International Organization for Standardisation Information Security Forum
IT	Information Technology
JSON	JavaScript Object Notation
MiTM	Man-in-the-Middle

Abbreviation / acronym	**Description**
OWASP	Open Web Application Security Project
PaaS	Platform as a Service
PCI-DSS	Payment Card Industry Data Security Standard
SaaS	Software as a Service
SIEM	Security Information and Event Management
SME	Small Medium Enterprise
SOC	Security Operations Centre
SSL	Secure Socket Layer
SUT	System Under Test
SW	Software
SWG	Secure Web Gateways
SWG	Secure Web Gateway
TaaS	Test-as-a-Service
TRL	Technology Readiness Levels
UI	User interface
URL	Uniform Resource Locator
USG	Unified Service Gateway
VDI	Virtual desktop infrastructure
VM	virtual machine
VPN	Virtual Private Network
WAF	Web Application Firewall
WP	Work Package
XML	Extensible Mark-up Language

Executive Summary

The aim of the present document is to describe the enhancement made on the “SMESEC System Design” (D3.1) [15] towards a unified architecture and robust integration of the SMESEC Framework.

The main challenges addressed in this document are: (1) refining the SMESEC Framework architectural requirements, (2) providing in-depth description of the architecture communications, interfaces, and user design, (3) documenting the current integration of SMESEC tools into the current development of the SMESEC Framework, (4) and defining the SMESEC Framework functionalities.

In D3.1 the SMESEC use case requirements were produced based on input from WP2 and WP6. Here we present the detailed process and methodology of collecting these requirements and describe further requirements that rose since as a result of the feedback we gathered and the integration process.

The SMESEC Framework is enhanced to meet those requirements. New design views are added, and detailed UML diagrams are developed. Additionally, user experience is developed to answer multiple and evolving persona requirements.

The current modular integration and development of SMESEC tools into the SMESEC Framework is documented. Last, the SMESEC Framework functionalities where defined and described. These functionalities fall into two categories: SMESEC tools functionalities and SMESEC Framework beyond-the-tools functionalities

This document will serve as basis for “SMESEC Unified Architecture and the Initial Version of the SMESEC Framework prototype” (D3.3).

1 Introduction

1.1 Purpose of the document

The aim of the present document is to describe the unified architecture of the SMESEC security framework including the integration and deployment of the SMESEC Framework proof-of -concept. To achieve this objective the feedback about the design described in “SMESEC System Design” (D3.1) [15] was collected, new requirements from the integration process were collected and were considered with the objective of ensuring that the proposed design fulfils the market needs and demands.

1.2 Relation to other project work

As described in the DoA [12], this document will report the preliminary draft of the system level functionalities for the proposed SMESEC, and the First Internal Release of the SMESEC Unified Architecture. This document considers as an input the system design described in D3.1 and introduces the enhancements to the architecture and design of the SMESEC Framework. The definition of the SMESEC Framework will continue with the release of the final version of the SMESEC Unified Architecture and the Initial Version of the SMESEC Framework prototype (D3.3) in M24.

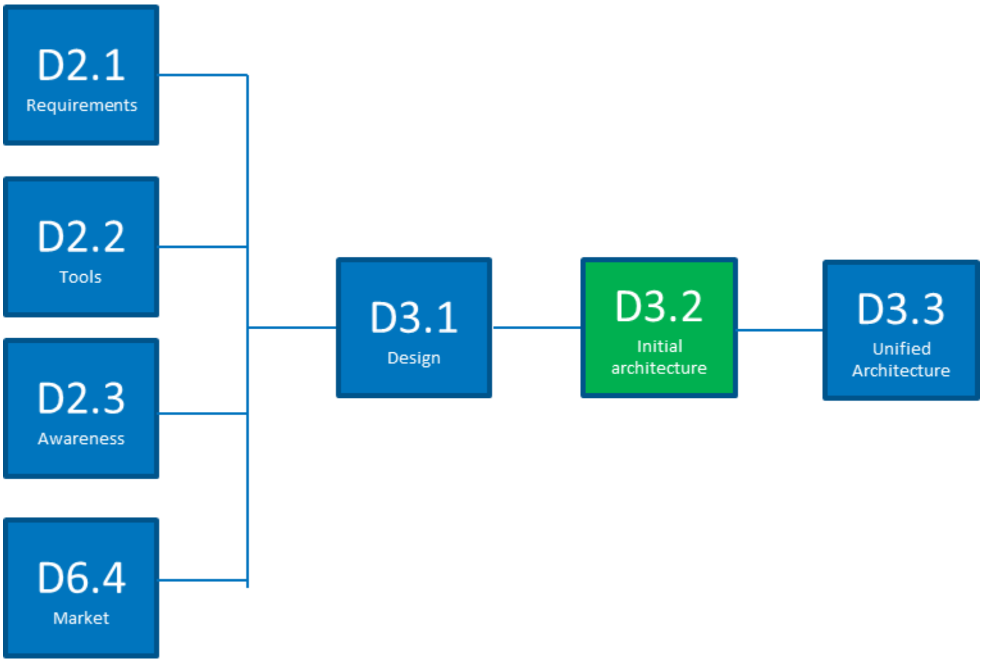


Figure 1: High-level view on the methodology for designing the SMESEC Framework

¡Error! No se encuentra el origen de la referencia. shows a high-level diagram of the process we followed for designing, refining and enhancing the SMESEC Framework architecture.

1.3 Structure of the document

This document is structured in 7 major chapters:

- **Chapter 1** presents the main objectives of the deliverable and describes the following sections.
- **Chapter 2** introduces updates to the stakeholder's concerns.
- **Chapter 3** extend the main requirements to be fulfilled by the SMESEC Framework extracted as described in D3.1.
- **Chapter 4** enhance existing and provide new SMESEC Framework design views.
- **Chapter 5** describes the integration activities of the SMESEC tools in the proposed design.
- **Chapter 6** describes the extended functionality of the proposed SMESEC Framework on top of the functionality of each individual tool.
- **Chapter 7** describes the conclusions of the work presented in this deliverable.

2 Goals of SMESEC Framework

In order to cover the needs of SMEs, SMESEC objectives, as defined in the DoW, are as follow: i) high-quality cyber-security solution attractive to companies with restricted budget, ii) increase protection by focusing on increasing awareness and training for SMEs, iii) SMESEC solution validated in multiple SMEs environments, iv) consolidating international and European links and harmonizing solutions with general standards and directives, v) ready to market solutions and immediate market impact.

These objectives were the ones guiding the initial design of the SMESEC Framework, in terms of modular architecture, deployment and components of the solution. After the initial output we had advanced discussions with the use case partners and other SMEs through questionnaires and other dissemination activities where they commented us their issues for working with cybersecurity. Some of the more important ones we compiled are:

- Usability and user experience is critical. SMEs do not usually have expertise in cybersecurity and, therefore, both the use of the framework and the tools must be as user-friendly as possible. Also, the SMESEC Framework should help as much as possible users in understanding the status of their system and how better protect it (e.g. recommendations).
- Cost-reduce. SMEs span from medium companies with a specific budget for cybersecurity, planned training and appointed cybersecurity experts to small companies where cybersecurity is used as an "add-on" for their products. One of the main comments we received from SMEs is that the cost of cybersecurity tools is usually high and therefore not affordable (the more specific, the more cost). The cost of the framework and related functionalities should be based in business strategies that allow companies to use only the products they want with a minimum cost.
- Solution tailored for SMEs. Another important feedback we have obtained from SMEs is that most of the tools are very generic for cybersecurity, not supporting or aimed for the specific needs of SMEs. The information provided and way of working of the cybersecurity tools should be done with the needs of SMEs as a basis.
- Extension of the framework with new functionalities/being up-to-date. A concern of SMEs is that cybersecurity tools they use offer a specific solution that, after a time, is not updated or adapted to the new needs of systems or business. The solution they look forward should allow for extension with other tools or improved functionalities of the existing ones in order to cover their evolving needs.

Therefore, the SMESEC project aims at supporting SMEs by offering characteristics that can cover their requirements and needs. More specifically, and updating the initial list of objectives of the project, the SMESEC solution is being designed/developed with the following goals in mind:

- Support non-cybersecurity users in the use of the SMESEC solution. This is done in two different ways: on the one hand the tools of the SMESEC Framework (the elements interacting with the user more specifically such as interfaces and output) are being evaluated/tested by the use case partners in order to refine the information or functionalities they provide and make them easier to understand by any type of user of their organization, ranging from cybersecurity expert to non-expert; on the other hand, the framework, being the main entry point, is being refined through several iterations in order to increase the user experience. This will be supported not only by the use case partners (which already have experience of the SMESEC Framework) but also by the new SMEs participating by the open call or other through any other program supported in the project. This way, we will have a very valuable feedback about how to improve the use of SMESEC for experienced and new users.

- Cost-reduced SMESEC Framework. We are working, together with the exploitation team of the project, on different strategies for providing the solution in the more affordable way. We are working bearing in mind the budget SMEs may have (which is very diverse) and the price/cost of the cybersecurity tools of SMESEC. Therefore, the modular aspect of the project will allow us to make available different sets of tools for covering the needs of the organizations and offer what is more necessary for each SME, being courses or solutions for specific cybersecurity problems.
- SMEs are at the heart of the SMESEC Framework. We are interacting with the use case partners with every new characteristic we add to the solution in order to have it aligned with their needs and be sure that any functionality we add is valuable to them. This will be later extended in the open call in order to refine further the solution for SMEs.
- Modular aspect. The SMESEC Framework follows a modular aspect that allows, not only the update of the tools we include on it, but also the addition of third-party tools for providing new functionalities. This will help the SMESEC solution to be always up-to-date and cover needs or problems not existing today but that could be a critical threat in the (short-medium-large) future. The tools of SMESEC will be able to be updated independently so the support of the framework and availability will be also high.

2.1 SMESEC stakeholders' concerns

The SMESEC stakeholders can be categorized into three groups:

- The SMESEC use-case partners.
- The SMESEC tool partners.
- The EU commission.

The concerns of each stakeholder group are described below.

2.1.1 SMESEC use-case partners

We hereby detail the methodology we followed in WP2 for requirement gathering of SMESEC use-case partners input. The results of the requirement gathering process is detailed in D3.1 [15]. In order to confirm our results, and stay updated on SMEs concerns, we plan to follow this methodology again with SMEs that respond to the open call.

2.1.1.1 Methodology for requirements elicitation

In order to identify the security requirements for the SMESEC we focused on the requirements as perceived by the end users, in our cases the four pilots. Thus, we created a requirements elicitation template (see: Annex A) distributed to the partners and requested input from them. The template was created based on common and high-level requirements both for their systems e.g. availability, robustness but for the proposed cybersecurity framework e.g. Usability, Cost, Alerting. Along with that high-level identification of requirements we requested specific lists of systems/assets that need to be protected, potential threats/attackers that are applicable in their specific use-case, security systems and recovery methods that are already in place, incident handling and data protection and recovery methods.

In the requirements' elicitation phase eighteen representatives took part in total. Five from the Smart City pilot, three for the industrial monitoring-IoT, six from the Smart Energy Grid pilot and four from the e-Voting pilot. All of the pilots' use cases belong to the Small and Medium enterprises with employees' size ranging from 11 to 200 as shown in Figure 2. The participants of the requirements' questionnaire were from all age ranges with most of the them belonging to the 45-54 group with years of expertise in Cybersecurity as shown in Figure 3.

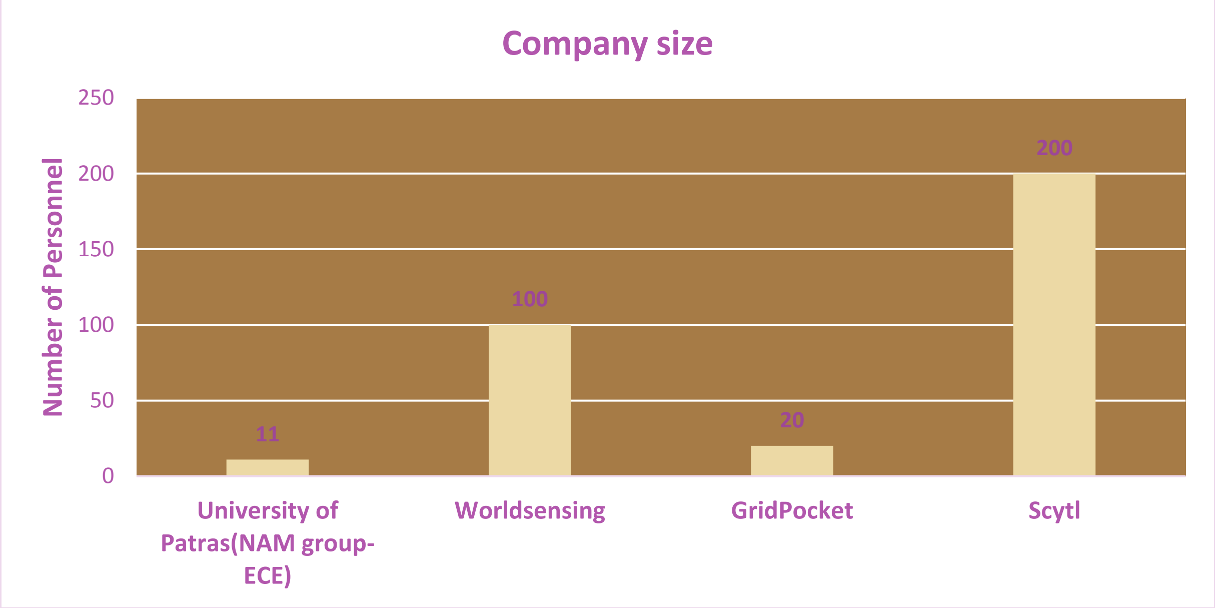


Figure 2: Company Size for each Use Case

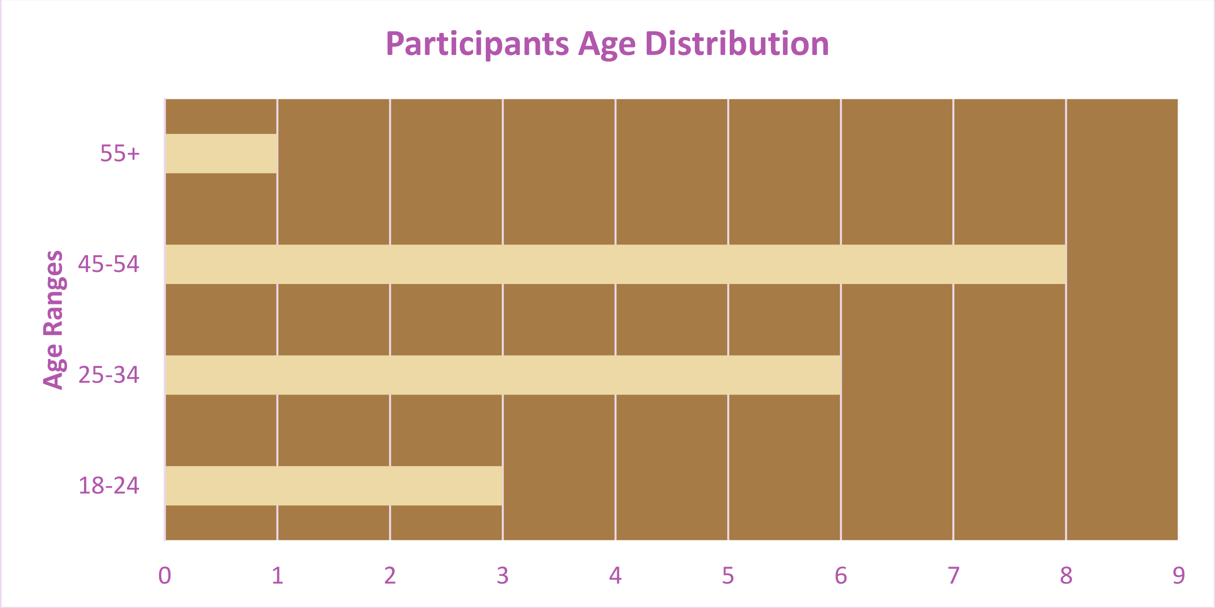


Figure 3: Requirements' Questionnaire Participants' Age Distribution

The participant's expertise in Cybersecurity shown in Figure 4 varied from one to twenty years, but the majority of the sample had long expertise in cybersecurity (more than three years) with an average of more than five years in the area. Also, the level of studies of the sample is high, with most of the participants having a master's and a Ph.D. degree and just one out of the eighteen to with bachelor's degree as shown in Figure 5. Finally, we studied the role of the participants in the company as shown in Figure 6, 16 % of them were C-level executives, 21% developers, 21% researchers, most of the participants were project managers 32% and 10% Cybersecurity managers. The sample had the expertise and the level of involvement with Cybersecurity to be able to provide coherent requirements, that aided a complete requirements'' gathering and design of the SMESEC framework on top of the true needs of the SMEs. Since, the requirements' questionnaire included both high-level requirements, that govern all SMEs, as well as, per pilot specific needs and assets to be protected, the majority of SMEs, even those not belonging into our specific use cases, can be represented by our requirement gathering process.

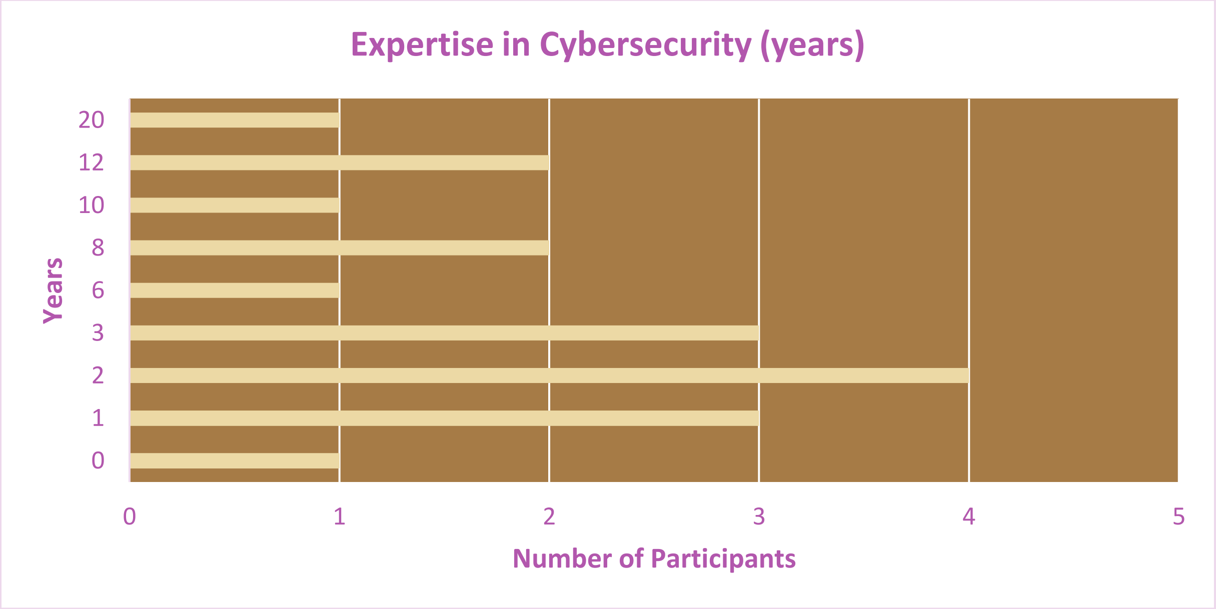


Figure 4: Expertise in Cybersecurity(years)

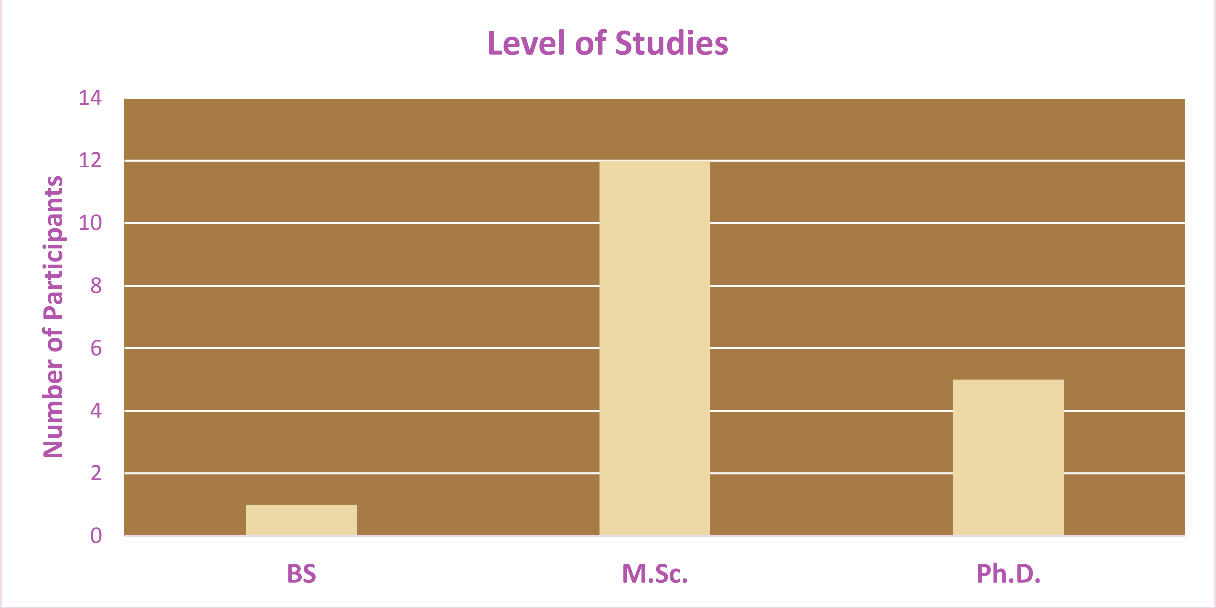


Figure 5: Level of Studies, for all participants in the Requirements' Elicitation

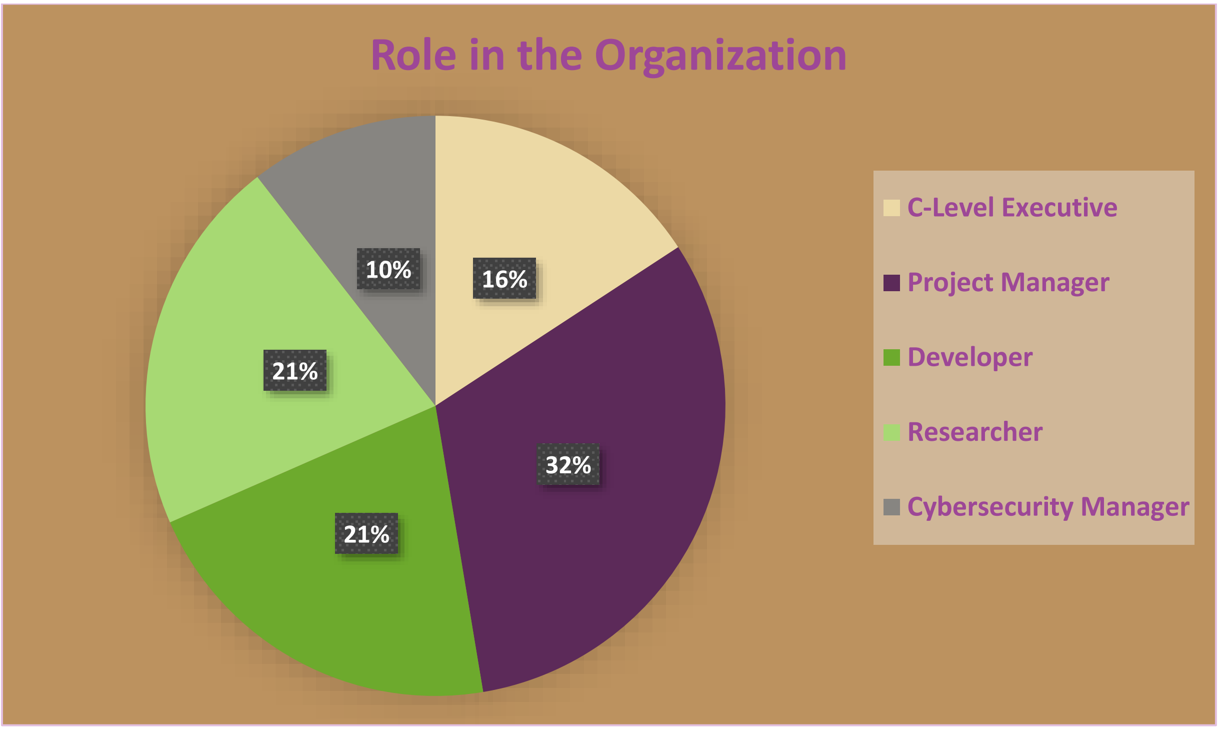


Figure 6: Participant role in the organization

This requirement gathering process has identified several high-level requirements coming from use-case partners referring to their desired service level. Please refer to D3.1 for details of the use-case needs, identified threats, use-case requirements and prioritization of concerns. To summarize, we identified the following as the main requirements of use case partners: Availability, Usability, Privacy, Cost, Alerting, System integrity, Confidentiality, Non-repudiation, Authentication, Scalability.

2.1.2 SMESEC product partners

We have identified the product partners concerns in D3.1, these can be summarized as: Integrating with other products, getting feedback from SMEs, and extending product capabilities.

2.1.3 European Commission

In D3.1 we have detailed the EU commission concerns, these can be summarized as: (1) High degree of usability and automation, (2) provide an adequate degree of cyber situational awareness and control for end-users, (3) incorporate the "human factor" (focusing on psychological and behavioural factors) in the design process, (4) follow existing relevant best practises and adoption of standards, tailored to SMEs and individuals.

2.1.4 SMESEC consortium concerns

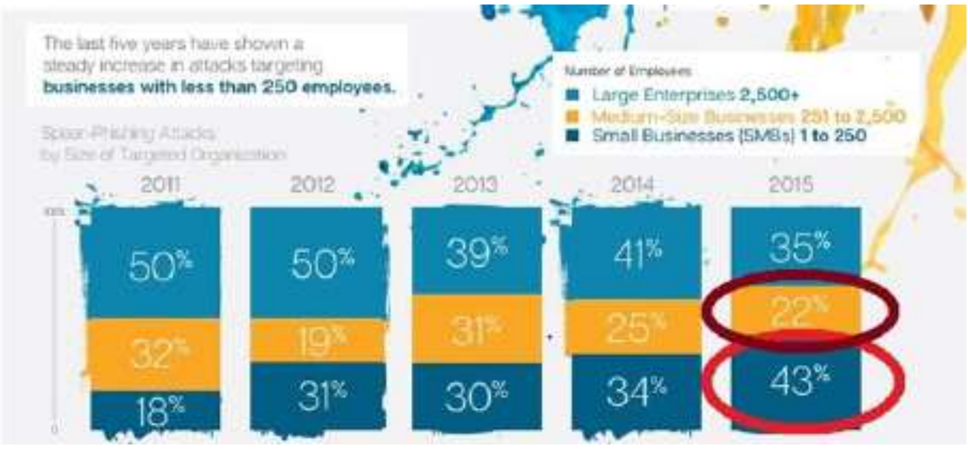


Figure 7: Statistics of cyber-attacks to SMEs (Reference: Grant Agreement)

The threats to cyber-security have been given prominence and are becoming one of the most important emerging threats to security. From an SME perspective, cyber security solutions are highly intensive in both economic and technical wise investment (they are considered expensive, take too much time to deploy, and need highly skilled staff to manage). Limited budget on that respect have a very negative impact in the investments SMEs (both SMEs public and private institutions need to be considered) do in cyber-security services and products.

SMESEC consortium aims to produce a product that will become a "ready-to-market solution with an immediate market impact. 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 consortium orbits around *SME's in Europe* (primary target), its direct market target should include all SME's domains. The project has made special emphasis in the *four main markets* targeted which correspond to the 4 project pilots (Smart-City, Industrial Internet of

Things (IIoT), e-Voting, Smart Grids) 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.

The key motivations for SMESEC consortium can be summarized as follows:

- The cyber security needs for SMEs are specific to each entity. SMESEC should be able to provide a tailor-made approach to those needs
- SMESEC framework will integrate diverse and cutting-edge technologies not only form the security field and will be able to adopt the latest innovations by integrating products within the framework in an effortless way.
- SMESEC will create cyber security awareness and will "educate" SMEs on how important cyber-security is for them and the critical impact neglecting it can have.
- Security awareness and automatic tools are mandatory aspects to increase security in the SME context (to prevent breaches originated by malicious insiders).
- SMEs targeted segments include technology providers (companies designing and selling security products) and end-users.

The interconnection of tools in the SMESEC product allows the creation of a security operations centre in the SMESEC Framework. In this security operations centre events from various real time monitoring tools can be reasoned upon and new knowledge can be extracted about systems under attack. The operations centre will also serve as an orchestrator of real time threats and offline threats such as lack of testing and lack of training. This orchestration will create testing and training requests for users based on real time attacks on their system. Finally, the operations centre will leverage security management and configuration along with threats detected to produce actionable items for security admins of the SME.

This type of orchestration usually requires and extensive expert knowledge for setting up rules and enforcing regulations. In SMESEC we propose to research machine learning and artificial intelligence to deduce these rules from data collected by our security operations centre. We will be able to collect the required data and research machine learning models in the next phase of our project and will report results in D3.3. Our vision of this machine learning interconnection will reduce the burden of constant research from the security admins and make security more affordable without compromising quality.

3 Requirements fulfilled by the SMESEC Framework

In D3.1 [15] we identified the functional requirements as protect, detect, monitor, alert, respond, and discover. As a result of reviews and interaction with use case partners we added the following functional requirement:

- Audit the security alerts of the SME's infrastructure, allowing forensic capabilities to the SMESEC Framework.

We also identified the following non-functional requirements:

- Authentication and authorization – The SMESEC Framework must allow authentication of users and manage user roles.
- As-a-service and on-premise deployment - The SMESEC Framework must allow both as-a-service and on-premises solutions.

Last, we decided not to exclude "Incident response" as stated in D3.1 as it is one of the main features of the Security Operation Centre functionality we plan to support. Further details about this can be found in Section 6.1.

4 Design of SMESEC Framework

In this chapter we describe the enhancements made to the design as described in D3.1 [15]. We choose to describe this according to the IEEE Standard 1016-2009 Software Design Description[1]. For the reader convenience we summarize each view's description in D3.1 and describe the enhancements made.

4.1 SMESEC Framework design views

This section describes: context view, concept view, pattern view, composition view, interface view, interaction view, and deployment view.

4.1.1 Context view

In D3.1 we identified the primary use cases of the Framework, these can be summarized as: monitor, protect, discover vulnerabilities, train employees, randomize software, assess security, and update SMESEC configurations. We have identified an additional use case of the SMESEC Framework: orchestration. The following figure describes the security orchestration use cases:

- An actor requests orchestration of SMESEC security management and threat defence tools; the SMESEC Framework creates new orchestrated alerts and responses.

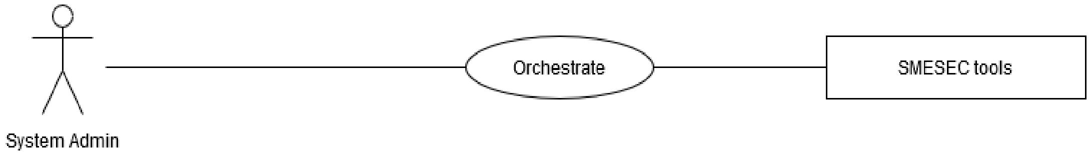


Figure 8: Orchestration use case

In addition to describing the use cases, we describe here the roles of users in the system. The SMESEC Framework comes with different roles defined with appropriate permissions to be used by different profiles in the company. These roles aim to cover different necessities identified along with the use case partners usage of the framework.

These roles are described below:

- Admin: This is the role for the system administrator. Users with this role can do any possible action in the framework. They are in charge of configuring the SMESEC Framework, deploy/install tools, integrate services provided by third-party tools, etc.

- Security Analyst: This role is intended for the company's security team. It provides permissions to see the output of the security tools included in SMESEC. Also, the security analyst can configure some settings of the tools.
- Auditor: The auditor is a role thought for internal or external audits. The users with this role can see the configuration of the SMESEC Framework and its tools, but they are not allowed to modify anything.
- Reporter: Users with this role can see and download the reports produced by the framework.
- User: This role does not offer any permissions to see security related information of the SMESEC framework, but to access the training platform of SMESEC and track their advances.

Although these roles come with the initial SMESEC installation, the system administrator can create new roles with custom permissions in the Keycloak console. We will provide more information about this functionality in the next deliverable of the SMESEC Framework.

4.1.2 Concept view

The main design concerns addressed in this concept view are:

- How to design a Framework that orchestrates all SMESEC partner tools
- How to design a Framework that answers the various use case requirements

In D3.1 we suggested a concept view with all tools revolving around and extended XL-SIEM. We have revised this to all tools revolving around an SOC. This was done because we understand that event management (SIEM) is not at the heart of the SMEs concerns and that automatic response and operations are more important. Further, The Framework functionalities can be divided into three main categories: threat defence, security management, and orchestration. Conceptually it is advised to keep those in independent components so that management is always monitoring the threat defence components. This is visually depicted in Figure 9.

In the coming sections we will develop this concept into the appropriate design views.

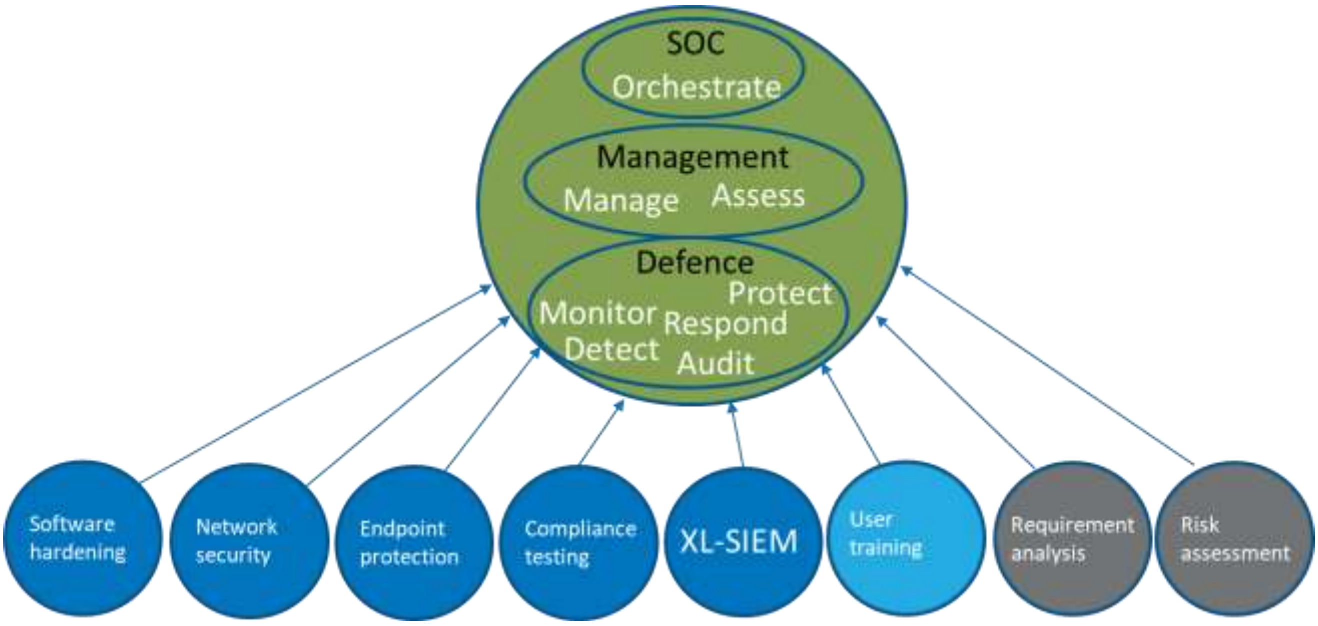


Figure 9: Concept view

4.1.3 Pattern use view

In D3.1 we describe the design pattern we choose. This design pattern is based on the PAC software architecture pattern [20]. The main reasons for choosing this pattern are the modularity of deployment and development concerns, and the confidentiality concerns. More on the design rationale can be found in section 4.3.

4.1.4 Composition view

In D3.1 we have described the composition view that address concerns related to the composition and modular assembly of the system. Given the new requirements identified above we have enhanced this view. Figure 10 and Table 1 show the component diagram and components description of our system.

In addition to the diagram described in D3.1 we add an authentication and authorization mechanism is connected to all components and actor in order to assure role management and enable decentralized deployment of the components.

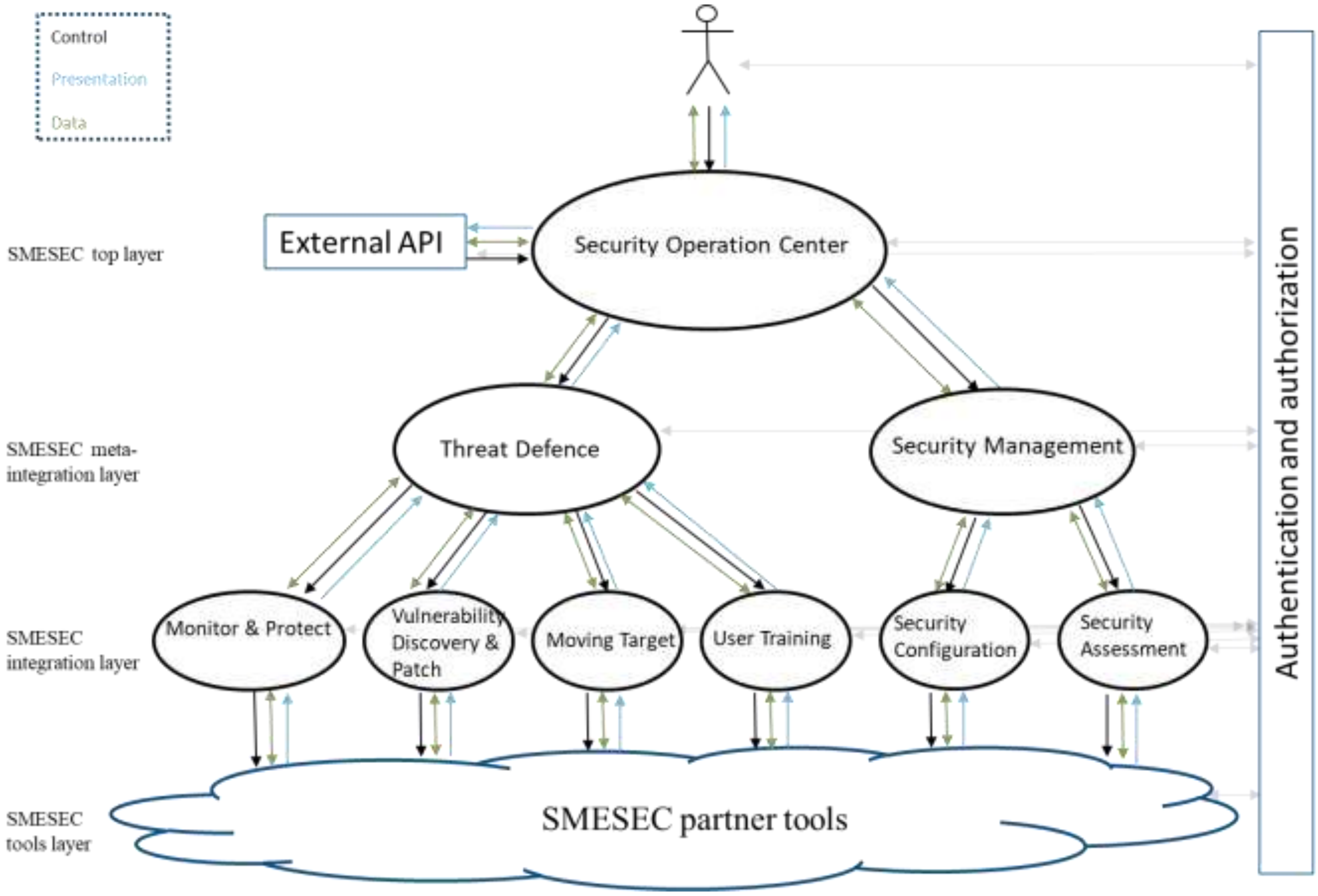


Figure 10: High-level composition view

Table 1 summarizes the packages and components description of our system. A detailed description can be found in D3.1 [15]

Table 1: Composition view component summary

Package	Component	Description
SOC	Presentation	User interface responsible to answer the user experience concerns. Present all tools interfaces, and Framework interface. Provide external interaction.
	Reasoning	Orchestration of meta layers results, providing monitoring and response orchestration
	History	Gathering request history and status of requests, and caching the results history
Threat Defence	Presentation	Interaction with the Security Operations Centre package
	Reasoning	Providing "monitor orchestration" of Monitor and

Package	Component	Description
		Protect, Vulnerability Discovery and Patch, Vulnerability Discovery and Patch, Moving Target, and User Training integration layers results.
	History	Caching the results history and obfuscating data if required
Security Management	Presentation	Interaction with the Security Operations Centre package
	Reasoning	Providing “management orchestration” of Security Assessment and Security Configuration layers results
	History	Caching the results history and obfuscating data if required
Monitor and Protect	Presentation	Interaction with the Threat Defence package
	Reasoning	API to tools
	History	Caching the results history and obfuscating data if required
Vulnerability Discovery and Patch	Presentation	Interaction with the Threat Defence package
	Reasoning	API to tools
	History	Caching the results history and obfuscating data if required
Moving Target	Presentation	Interaction with the Threat Defence package
	Reasoning	API to tools
	History	Caching the results history and obfuscating data if required
User Training	Presentation	Interaction with the Threat Defence package
	Reasoning	API to tools
	History	Caching the results history and obfuscating data if required
Security Assessment	Presentation	Interaction with the Security Management package
	Reasoning	API to tools

Package	Component	Description
	History	Caching the results history and obfuscating data if required
Security Configuration	Presentation	Interaction with the Security Management package
	Reasoning	API to tools
	History	Caching the results history and obfuscating data if required
Authentication and Authorization		Provide authentication of all SMESEC user, and authorization per user roles. This component interfaces with all component of the SMESEC Framework and tools

4.1.5 Interface view

Detailed interface description tables of internal package interface and internal interface to SMESEC partner tools is described in D3.1. We here bring an updated UML component diagram in Figure 11.

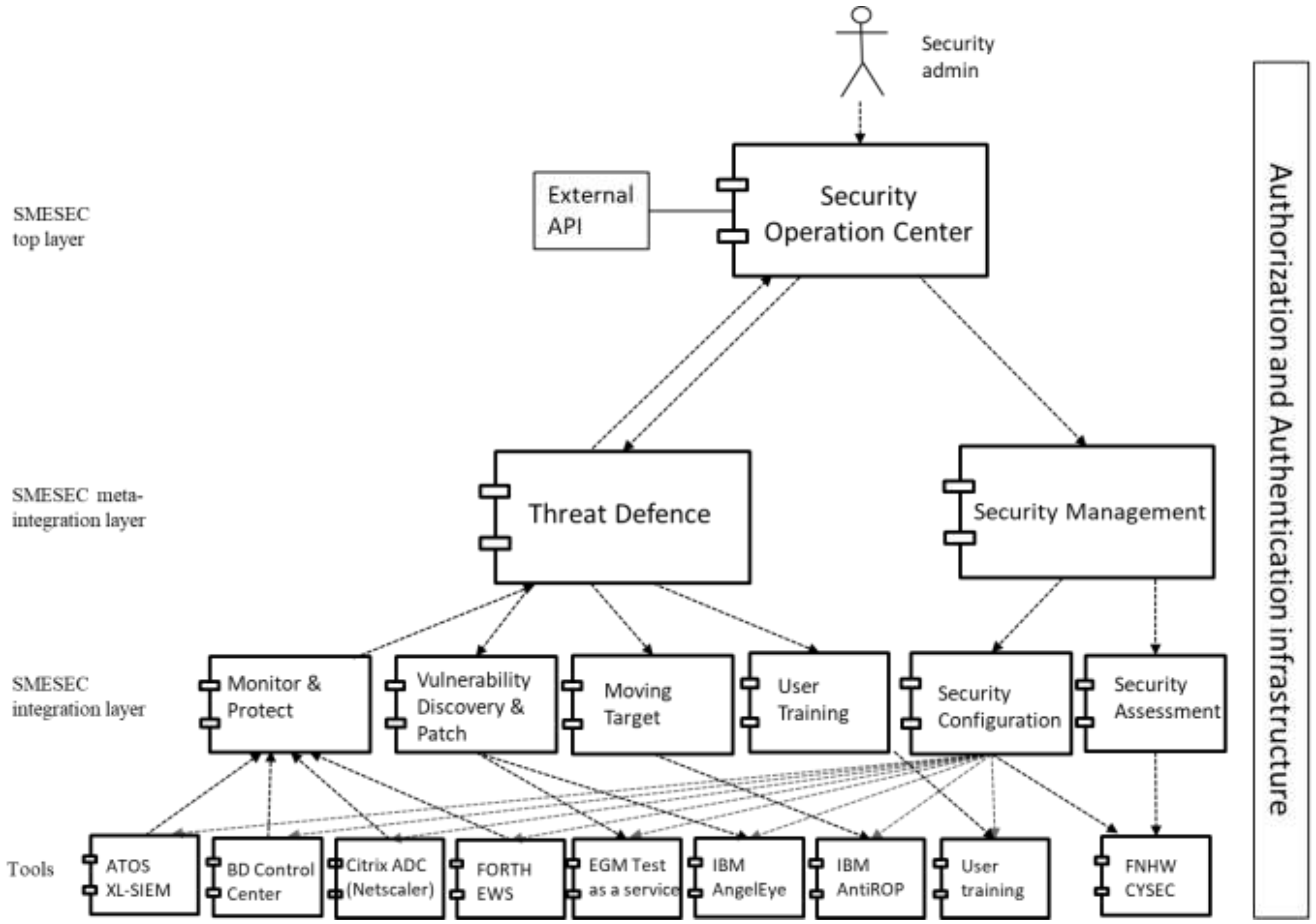


Figure 11: UML component diagram

4.1.6 Interaction view

In this view we present several sequence diagrams depicting the most common interactions between the SMESEC components. This will aid in better defining of the strategies for interaction among entities.

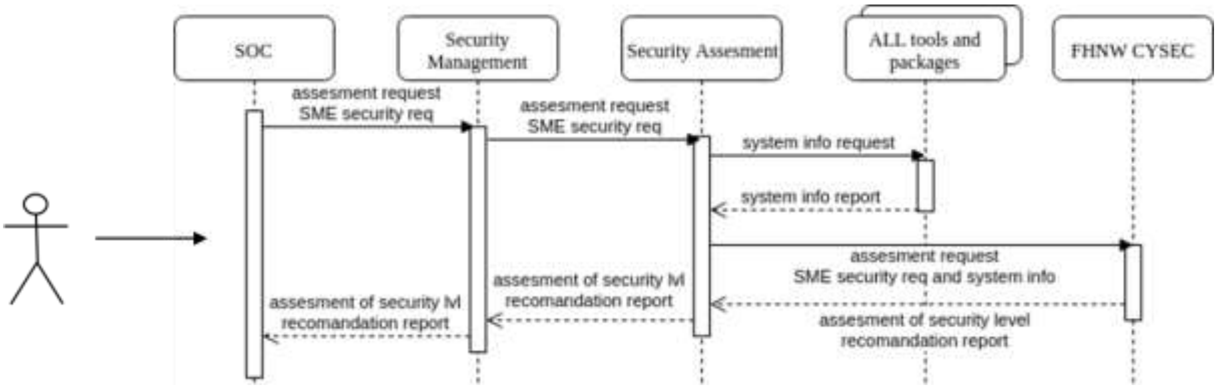

SOC
Security Management
Security Assesment
ALL tools and packages
FHNW CYSEC
assesment request SME security req
assesment request SME security req
system info request
system info report
assesment request SME security req and system info
assesment of security level recomandation report
assesment of security lvl recomandation report
assesment of security lvl recomandation report

Figure 12: Security assessment

Figure 12 presents the security assessment use case. The request from the user is sent to the top level (SOC) and propagates to the Security Assessment layer, next it is sent to the all tools and packages. The information is collected back and sent to CYSEC tool for assessment. The assessment is propagated back in the various layers with the proper data filtering. The SOC presents the assessment and recommendations to the user.

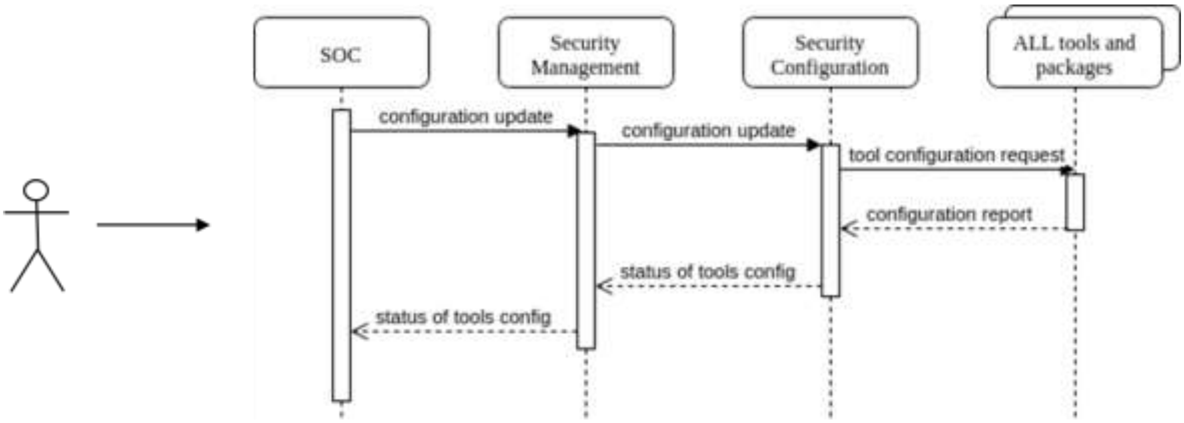


Figure 13: Configuration update

Figure 13 depicts a configuration update use case where the request is propagated from SOC through Security Management and Security Configuration. The Security Configuration holds the information required to send to all tools and packages installed and search for outdated configuration. The configuration report than propagates back to the top layer.

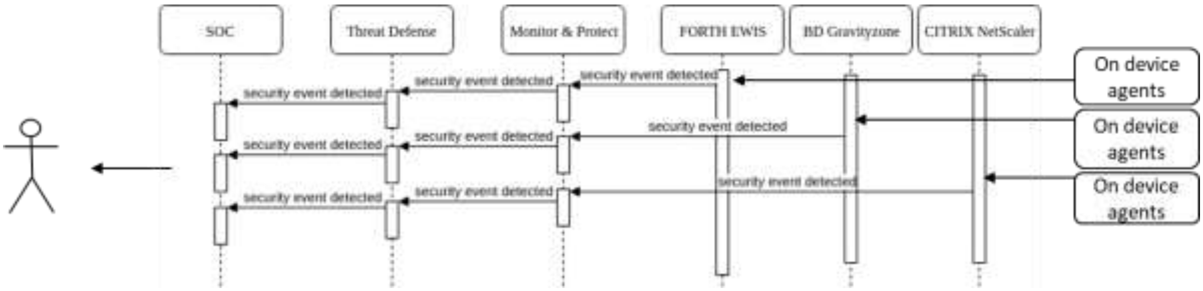


Figure 14: Security event detected

The monitoring use case is depicted in Figure 14. Agents installed in the SME’s IT report events to various tools like: FORTH EWIS, BD GravityZone and CITRIX NetScaler in real-time. The events are propagated upwards through Monitor & Protect and Threat Defence components. The threat and defence decides if to propagate to SOC based on monitoring orchestration, and SOC decides how to present to use-case actor based on orchestration with security management and users maturity level.

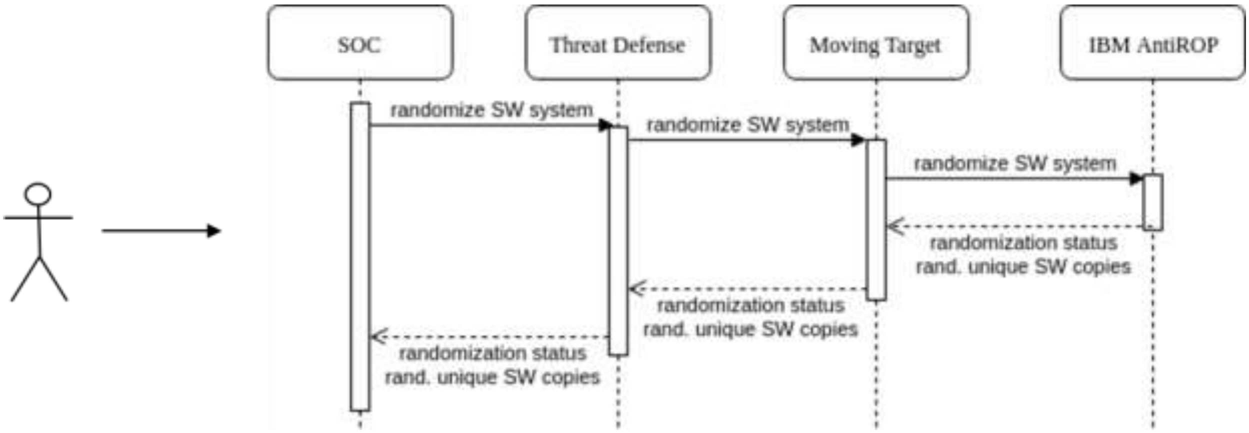


Figure 15: Software system randomization request

The randomization use case is depicted in Figure 15. The user requests a software system randomization request from Security Operations Centre. This is then propagated to the Moving Target components and to IBM AntiROP tool. The tool produces randomized copies and outputs a randomization status that propagates back to the SOC.

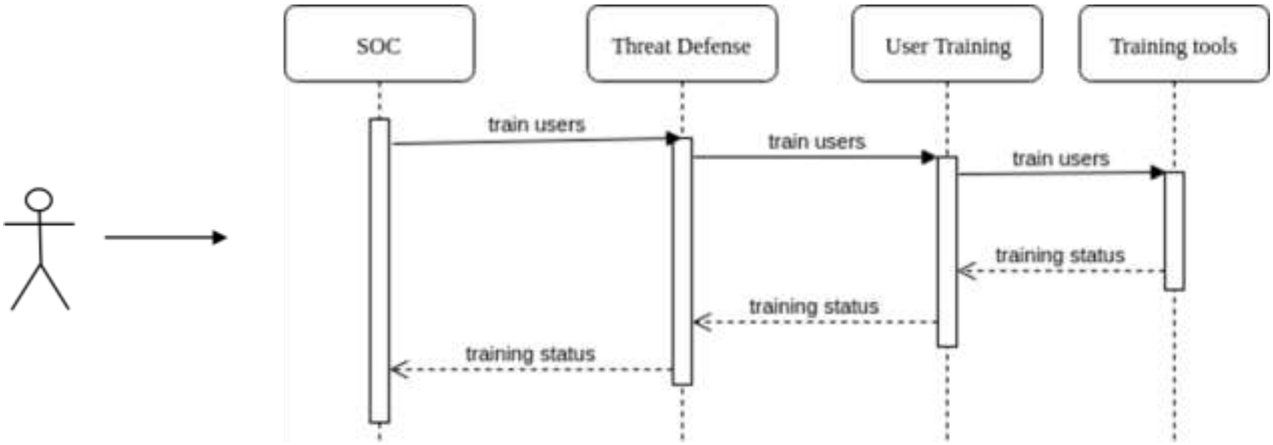


Figure 16: Users training

The user training use case is depicted in Figure 16. The request comes from the SOC is sent to User Training and to the training tools. The training tools initiates a training modules for the employees and notify them that new training modules are available. The training status is periodically sent back to the SOC.

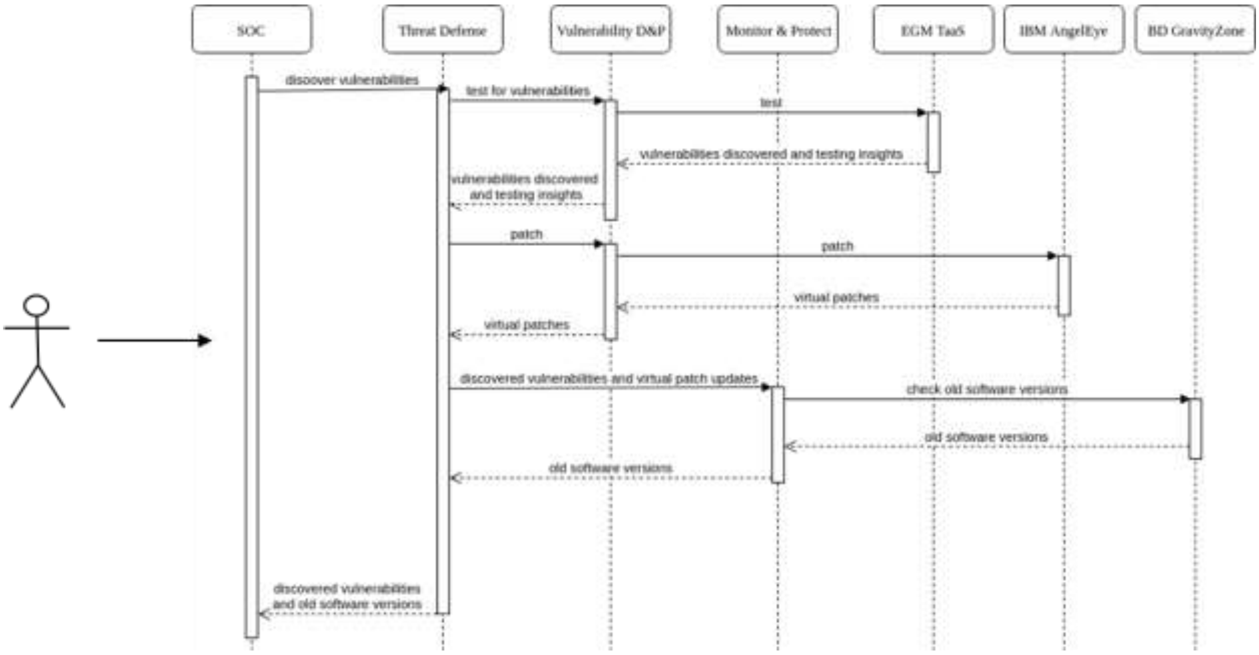

SOC
Threat Defense
Vulnerability D&P
Monitor & Protect
EGM TaaS
IBM AngelEye
BD GravityZone
discover vulnerabilities
test for vulnerabilities
test
vulnerabilities discovered and testing insights
vulnerabilities discovered and testing insights
patch
patch
virtual patches
virtual patches
discovered vulnerabilities and virtual patch updates
check old software versions
old software versions
old software versions
discovered vulnerabilities and old software versions

Figure 17: Vulnerability assessment and patch

The vulnerability assessment and patch use case is mostly handled by the Threat Defence component, as depicted in Figure 17. The testing tools will receive the test request and will perform the required vulnerability and compliance testing. The output of discovered vulnerabilities and the testing insights is sent propagated back to user, while the data generated along the testing process is sent to IBM AngelEye tool that is responsible for virtual patches. A virtual patch is created. Bitdefender GravityZone identifies and outdated and vulnerable software and even patch in some scenarios. The request for this operation will be propagated through the Monitor and Protect component and the output will be a list of old software found. Finally, the results from all these tools will reach back the XL-SIEM at the SOC.

4.1.7 Deployment view

The main design concerns in this view are cloud readiness and cloud deployment. Cloud deployment was identified as one of the possible measures to reduce cost of the SMESEC Framework for SME's. A survey of cloud readiness of SMESEC partner tools was reported in D2.1 [3]. SMESEC partner tools we not fully ready for cloud deployment, and further development has been done since. SMESEC Framework will support on-premise, and cloud deployment.

The SMESEC Framework offers different services supporting both as-a-service and on-premises solutions. This way, the deployment strategy of the SMESEC Framework must be in-line with the needs and characteristics of the expected functionality for the tools that compose the framework and the framework itself. In Figure 18 we describe our initial deployment plans that answer the concern of enabling future hybrid cloud deployment.

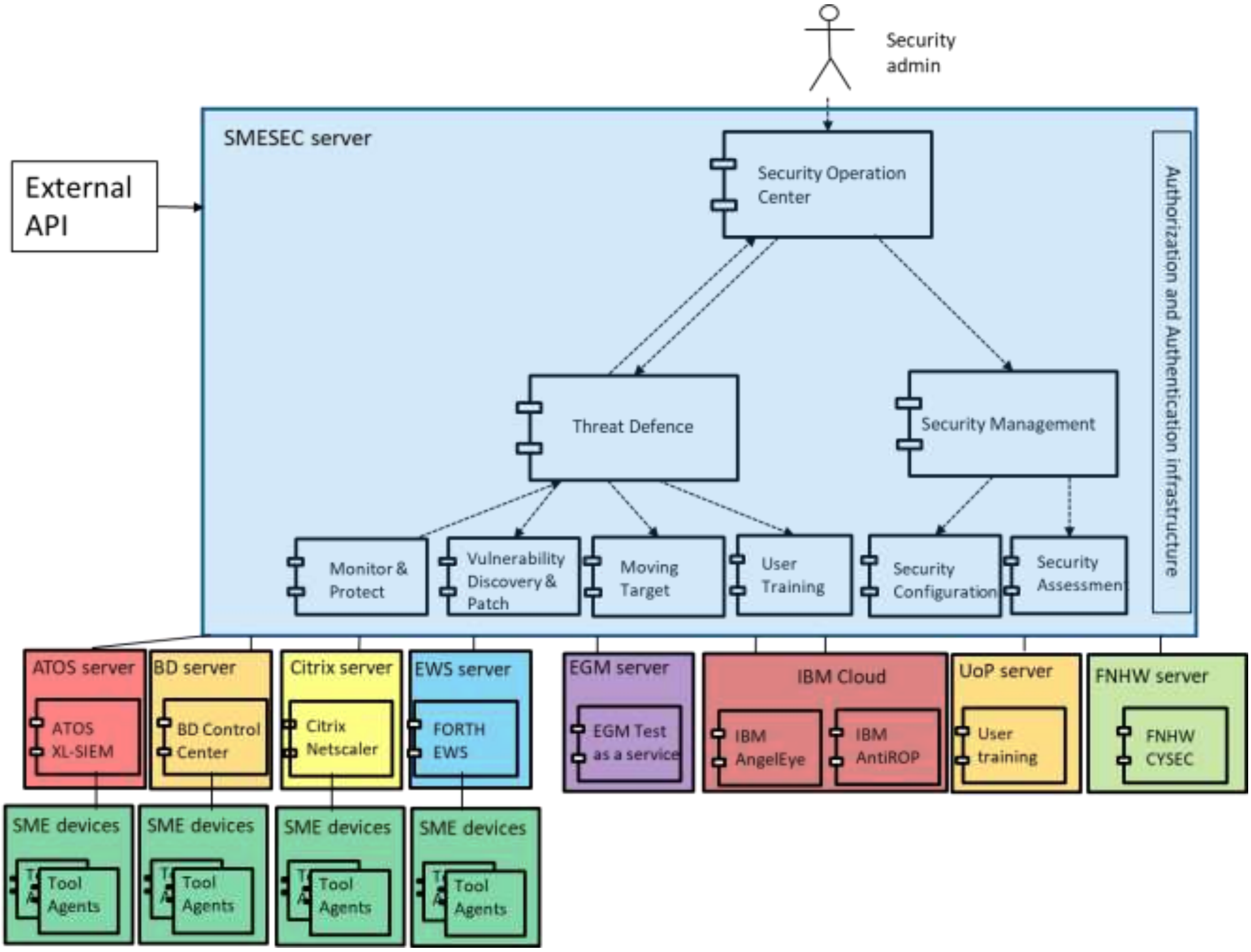


Figure 18: Deployment diagram

The first step to laying the foundation for cloud deployment is to set up an authentication and authorization infrastructure applicable to all tools and components of the solution. This is done by integrating KeyCloak [17] Identity Management and Access Management into the Framework and managing roles and access to components and tools through KeyCloak only.

The SMESEC Framework is deployed in a SMESEC node, initially with all tools working as-a-service. It is offered in the cloud to allow high resource flexibility. Note that the confidentiality requirement of SMEs might differ from one SME to another, and some might be more conservative about running SMESEC on public cloud. Therefore, our current instance is private for the consortium and will use the needs and requirements of the use cases for better identify the deployment options. This will allow us to work better in scalability of the framework, which is a very important element for the project and the business opportunities bearing in mind the capacities and technical requirements of the tools of SMESEC and the need for reducing the cost as much as possible.

Next, we address the online monitoring tools of the SMESEC solution. These tools require deployment of agents at the SME's IT infrastructure. Those agents can be deployed on servers, PC's, mobile, or IoT devices. All agents send information to a centralized analysis that analyzes information and forwards alerts to the SMESEC Framework. SMESEC currently offers four analysis components:

XL-SIEM, GravityZone, NetScaler, and EWIS. Each one of these tools is currently deployed at the tool provider premise, and is available for deployment on the SME's premise, public cloud, or private cloud. All these tools are providing next to real time monitoring, and load scalability can become a bottleneck with the current deployment, therefor we plan to deploy those tools on a public cloud where high flexibility is provided.

The non-monitoring tools are deployed either on a public cloud or on the tool owner premise. IBM tools are deployed on IBM Cloud, FHNW and EGM are deployed on the tools' owner premises, and the user training is deployed on UoP servers.

4.2 User interface

Usability is a key requirement of the SMESEC Framework. Being aimed to organizations and users ranging from no expertise on cybersecurity to high, it is important that the usage and understanding of the framework is as high as possible. The SMESEC Framework design offers a unified interface for all tools included in the SMESEC Framework. The user interface (UI) supports the unification, while offering the needed simplicity, with a tool launcher and an integration hook for the SMESEC tools' information and display of events. This section describes the targeted user personas, gives an overview of the provided UI functions, specifies the navigation, and describes the details of the UI views.

4.2.1 Personas

To design the proper user experience (UX) and identify the target personas of the SMESEC Framework we have conducted interviews with the use-case partners cybersecurity responsible in the SME. The UI has been designed for use by a persona in the SME. According to the so far collected survey data and by following the SMESEC fast ramp-up recommendations for cybersecurity capability improvement in the SME, we can expect that in each end-user SME there will be a person appointed for handling cybersecurity in the SME. To summarize our interview and describe in a specific way how to use the framework we defined a user called "Nicolas" which has this responsibility. Table 1 specifies his characteristics, expertise, etc. It is to be noted that personas are not identical to the user roles identified above, as user roles represent privileges and responsibilities of a person at a given time, while personas present catechistic, goals, desires, and expectations of a person [21].

Table 1: Persona "Nicolas, the cybersecurity responsible in the SME"

Attributes	Values
Name	Nicolas
Responsibility	Cybersecurity responsible in the SME
Characteristics	Curious about cybersecurity, while being afraid that it might be too complicated. Appointed by the SME management to handle the topic of cybersecurity in the SME. Cybersecurity is a side-topic and not the sole work priority for the person.
Background	Marginal knowledge of cybersecurity, which is improving through the use of the SMESEC Framework. First-time and repeated occasional user of the SMESEC framework without preparatory training.

Tasks	Expected to assess threat, vulnerability, and protection status; decide about and set cybersecurity controls; involve the SME's employees; and report to the management.
Expectations	Guidance with support of the personal learning of cybersecurity and how to address cybersecurity with the SMESEC framework. Minimal effort to obtain and maintain overview and awareness of cybersecurity in the SME and to report about it.

Additional users that have other responsibilities are of relevance in the extended SMESEC framework use. Their enablement is the concern of the on-going version of the SMESEC framework. The current version presented here covers only the initial responsibility (employee of the SME with minimum knowledge of cybersecurity) but will be extended to support more roles, identified with the following users:

- Martin, the cybersecurity expert and consultant offering personalized help and advice for SMEs.
- Jose, the cybersecurity reference person and community manager interacting with stakeholders and advancing cybersecurity for SME in Europe.
- Christos, the cybersecurity external auditor responsible to verify that the SME is compliant with regulations.

4.2.2 Functions

The SMESEC framework UI offers a comprehensive overview of tools and access to the functionality and information they offer. The following table offers an overview of the functions offered by the SMESEC framework UI, including the targeted benefits and key design decisions for the implementation.

Table 2: Overview of User Interface (UI) functions, including motivating benefits and implementation approach.

Responsibility	Functions	Targeted Benefits	Implementation
Cybersecurity responsible in the SME	FWUI-UC01: Single sign-on	Allow access to all SMESEC-protected information and tools with one effort.	KeyRock-based authentication and authorization.
Cybersecurity responsible in the SME	FWUI-UC02: Integrated display of information about addressed cybersecurity themes and available tools	Minimize cybersecurity knowledge required to use SMESEC. Flexibility for consortium to add and remove SMESEC tools.	1-page tool information visualization and launcher with hierarchical categorization of tools.

Responsibility	Functions	Targeted Benefits	Implementation
Cybersecurity responsible in the SME	FWUI-UC03: Display cybersecurity KPI and alarms for the SME	Awareness of current threats and protection status. The SMESEC tools report the following information: real-time security detected events, discovered SW vulnerabilities, vulnerable SW versions detected, user training status, randomized unique copies of a SW, assessment of security level, security recommendations, and status of tool configuration. The SMESEC tools issue the following alarms to: discover vulnerabilities in SME's SW, train SME employees, create new unique copies of a SW, assess of security level, Input system information and security requirements, and update tool configurations.	Frame offering dynamic visualization rendered by SMESEC tools.
Cybersecurity responsible in the SME	FWUI-UC04: Switch between tools fast and easily.	Support exploration of tools. Support visual inspection and correlation of tools' settings and outputs.	Integrated tool display with header indicating chosen tool, tool display, and accordion with compact tool launcher.

The UI of the SMESEC framework can be used with a browser and offers visual and textual interfaces and allows display of dynamic tool-rendered information with an iFrame-based approach. Firefox v63 and Chrome v70 on Windows 10 and Safari v12 MacOS High Sierra planned for acceptance tests. This allows integration of the SMESEC Framework tools and integration of security for the SMESEC Framework.

The UI can will be accessible by signing in on the SMESEC homepage [19], and used as a public-cloud service offered by the SMESEC consortium. The UI may also be deployed on-premise and used in conjunction with locally deployed tools.

4.2.3 Navigation

To minimize the complexity of the SMESEC framework use, the UI offers a simple navigation approach based on two paradigms: a) one-page overview view allowing to access functionality through vertical navigation and information through horizontal navigation, and b) detailed full-screen tool view with an accordion allowing to switch between the tools and return to the overview view. The following figure shows the screens and navigation pathways.

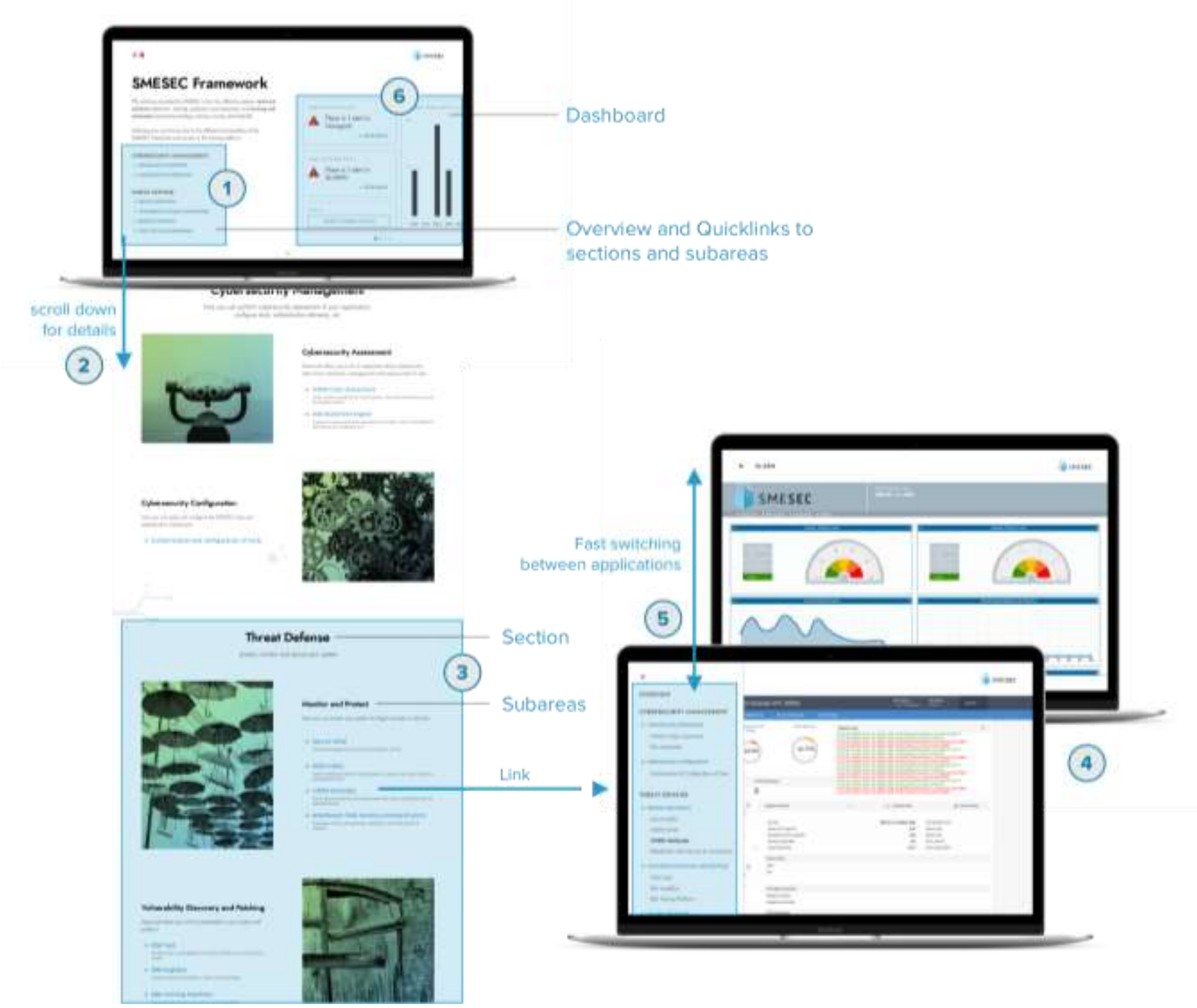


Figure 19: SMESEC UI navigation with one-page tool and information access (left) and detailed tool view with accordion for fast switching between the tools (right).

Users who visit the framework, will get on the main page a one-page overview of the options available to them (1). All applications are grouped into the SMESEC sections and subareas to provide structure for user guidance and fast access to a desired cybersecurity topic for which SMESEC offers tools (3). If the user has little experience in the field of cybersecurity, the UI offers support through the structured content and short text information. In addition, the images give the user a rough feel for the subject areas. If the user does not yet know which topics are of interest or relevance, he can browse through them by scrolling through page (2). As a benefit, even inexperienced users can quickly gain an understanding of the individual functionalities.

If the user has found the right application, it will be opened in the same tab in a screen-filling mode, in the tool view (4). For the design of the UI, it was important that after the user has decided on an application, the entire focus is on the application. The other applications are hidden but remain accessible via an accordion menu (5). Through that menu, the user can quickly switch between applications or return to the main page.

As soon as the user has started to use applications, a dashboard is displayed on the start page (6). The dashboard gives the user a quick overview of the status, alarms, and information of the applications he is using.

4.2.4 View: One-Page Overview

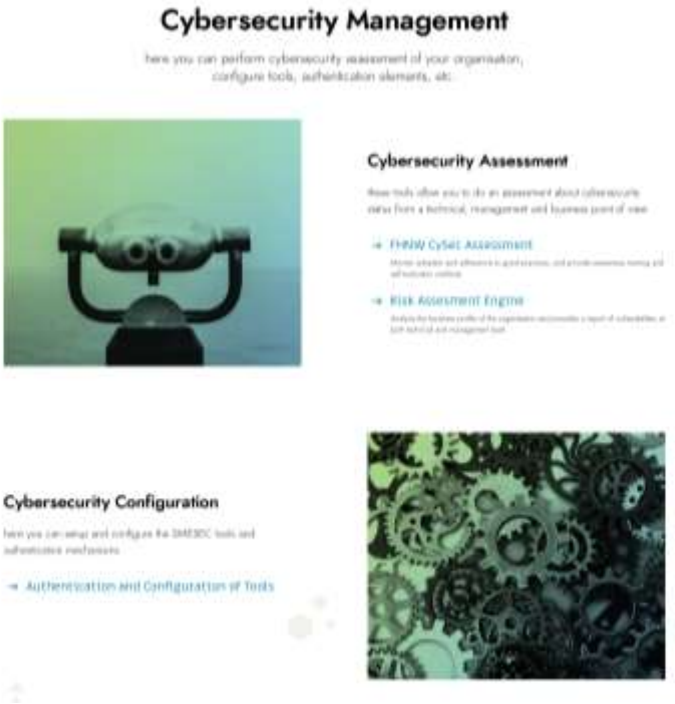
The one-page overview offers an introduction with quick-links allowing to understand the scope of the page, a section with hierarchical structuring and explanation of the SMESEC framework, and a dashboard with SMESEC tool KPIs and alerts.

The following table specifies the sections. The ensuing figures show the visual appearance.

Table 3: Elements of the One-Page Overview UI.

View	Section	Targeted Benefits	Implementation
FWUI-P01: One-Page Overview	FWUI-P01.1: Quick-Links	The human end-user gets a one-attempt overview of the SMESEC tool categories without the need to interact with the UI. The human end-user can navigate to the tool category with a single click.	HTML with in-page links.
FWUI-P01: One-Page Overview	FWUI-P01.2: Tool Launcher	The human end-user gets introduced into the topic of cybersecurity through the categorical grouping of SMESEC tools into sections and subareas that offer short explanations. The human end-user can launch a tool with full understanding of the tool's scope.	HTML with cross-page links.
FWUI-P01: One-Page Overview	FWUI-P01.3: Dashboard	The human end-user is aware of the threat exposure and protection offered by the SMESEC tools. The human end-user can launch a SMESC tool by clicking on the KPI or alert shown by that tool.	iFrame integration of tool-rendered HTML views.
FWUI-P01: One-Page Overview	FWUI-P01.4: Header Bar	The human end-user knows he is using the SMESEC framework. The human end-user is alerted by an icon of updates and alerts to be checked in one of the tools.	HTML always shown on top of screen.
FWUI-P01: One-Page Overview	FWUI-P01.5: Footer	The human end-user knows that the SMSEC framework is delivered by trustworthy parties.	HTML with logo and disclaimers at the bottom of the page.

Figure 20: Top-view of the one-page overview, showing the quick-links, dashboard, and header bar sections.



Cybersecurity Management

here you can perform cybersecurity assessment of your organisation, configure tools, authentication elements, etc

Cybersecurity Assessment

these tools allow you to do an assessment about cybersecurity status from a technical, management and business point of view

→ FHNW CySec Assessment

[illegible]

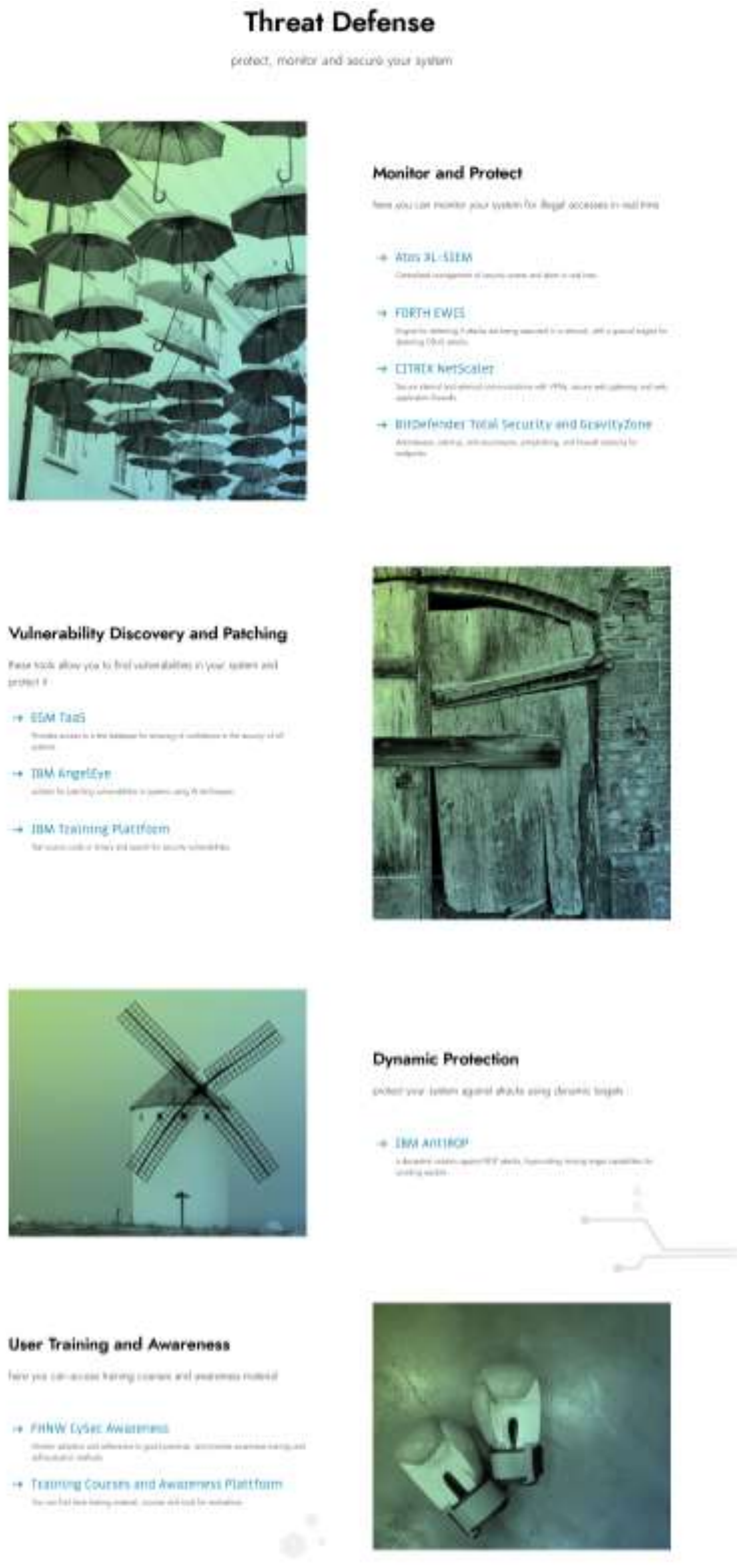
→ Risk Assessment Engine

[illegible]

Cybersecurity Configuration

here you can setup and configure the SMESEC tools and authentication mechanisms

→ Authentication and Configuration of Tools



Threat Defense

protect, monitor and secure your system

Monitor and Protect

Here you can monitor your system for illegal accesses in real time

→ Atos XL-SIEM

Centralized management of security events and alarms in real time.

→ FORTH EWIS

[illegible]

→ CITRIX NetScaler

[illegible]

→ BitDefender Total Security and GravityZone

[illegible]

Vulnerability Discovery and Patching

These tools allow you to find vulnerabilities in your system and protect it

→ ESM TaaS

[illegible]

→ IBM AngelEye

[illegible]

→ IBM Training Plattform

[illegible]

Dynamic Protection

protect your system against attacks using dynamic targets

→ IBM AntiROP

[illegible]

User Training and Awareness

here you can access training courses and awareness material

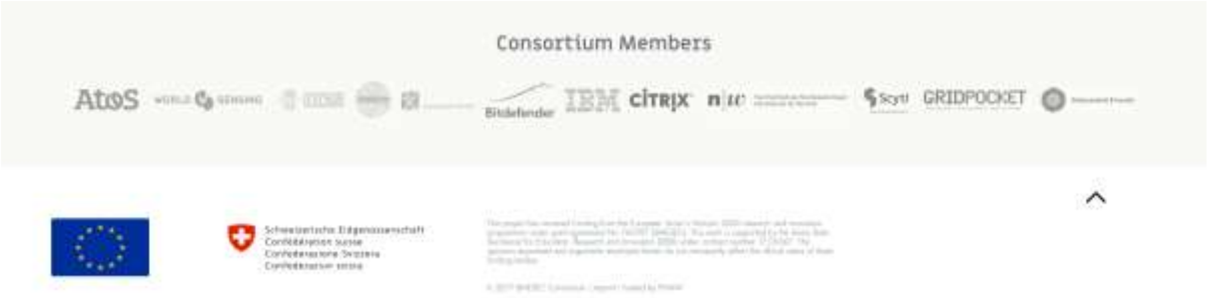
→ FHNW CySec Awareness

[illegible]

→ Training Courses and Awareness Plattform

[illegible]

Figure 21: SMESEC tool launcher introducing the human end-user into the cybersecurity topics.



Consortium Members

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

[illegible]

© 2017 SMESEC Consortium | Imprint | Hosted by [illegible]

Figure 22: Footer for trust-building.

4.2.5 View: Tool View

The tool-view puts a launched SMESEC tool full-screen into the centre with an attempt to distract the user minimally. The tool view allows interaction with the SMESEC tool as if the tool would be used standalone, while offering framework benefits. The framework benefits are branding for trust-building and rapid switching between framework tools.

The following table specifies the sections. The ensuing figures show the visual appearance.

Table 4: Elements of the Tool View UI.

View	Section	Targeted Benefits	Implementation
FWUI-P02: Tool View	FWUI-P02.1: Tool UI	The human end-user uses the launched SMESEC tool without distracting cluttering.	iFrame integration of tool front-end.
FWUI-P02: Tool View	FWUI-P01.4: Header Bar	The human end-user knows he is using the SMESEC framework. The human end-user is alerted by an icon of updates and alerts to be checked in one of the tools.	HTML always shown on top of screen.
FWUI-P02: Tool View	FWUI-P02.2: Launcher Accordion	The human end-user switches between the SMESEC tools without being required to leave the tool view. The human end-user knows which SMESEC tools have updates or alerts to be checked.	Canvas toggled by clicking the accordion in the header bar.

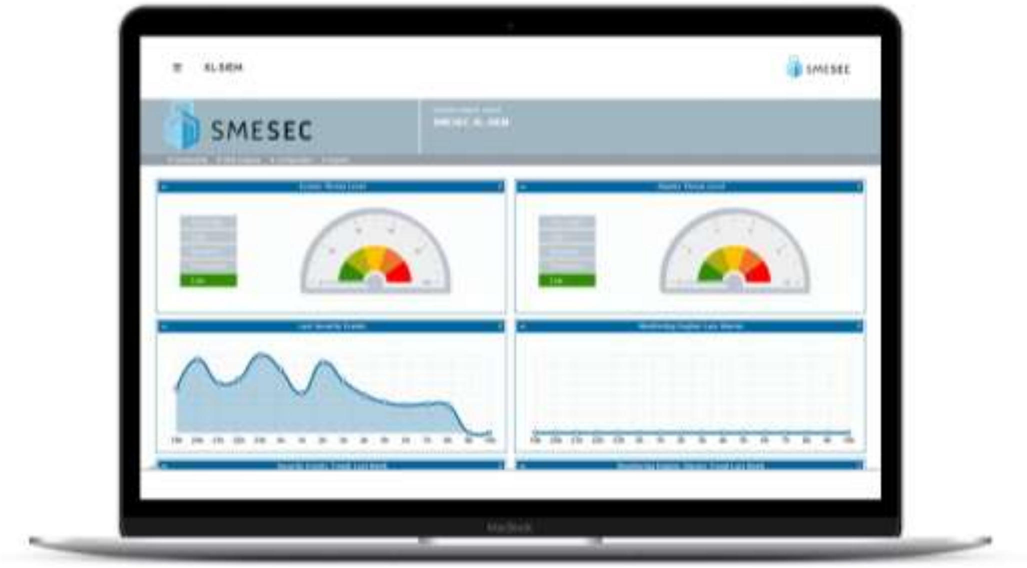


Figure 23: Tool view with header bar and tool UI. An orange number besides the accordion indicates the number of updates and alerts to be reviewed by the human end-user.

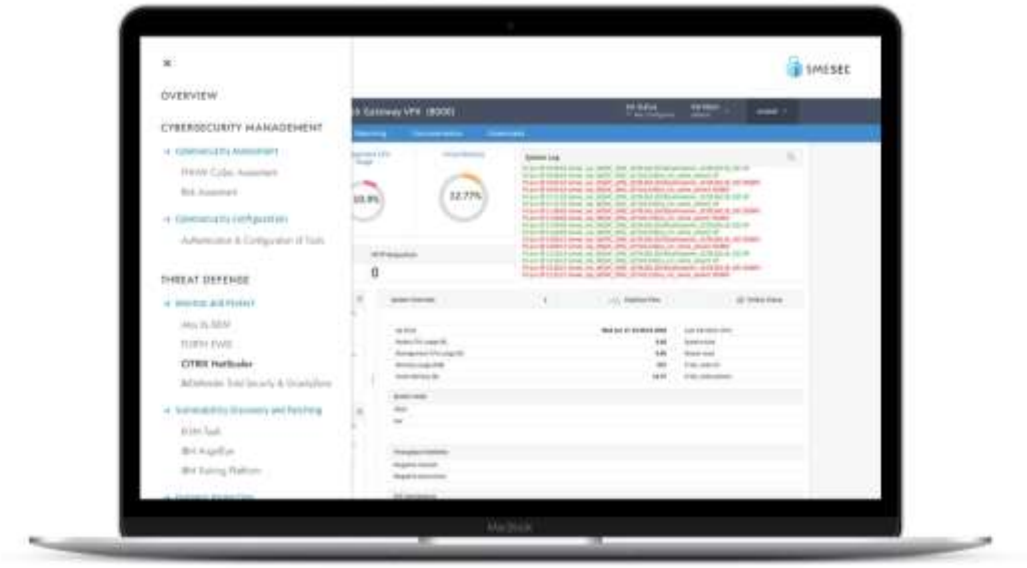


Figure 24: Tool view with opened launcher accordion for switching between the tools. An orange number besides the tool indicates the number of updates and alerts to be reviewed by the human end-user.

4.2.6 Discussion

The SME user interface and interaction view aims at fulfilling the SMESEC principles of *do it yourself*, *keep the investment small*, and *keep it simple*, while offering GUI-level integration of the SMESEC framework tools. To support human end-users with minimal cybersecurity and framework knowledge, the UI offers that guidance. At the same time, it does not hinder experienced users. The UI also offers awareness and guides attention through a dashboard and cues about important tool content updates.

The UI has been validated in the discussions with the SMESEC Framework and SME use case partners. Further validation, including on-site human end-user usability tests are planned as part of task T4.5 during months 19-24 and will be reported in the deliverable D4.2, D4.4, D4.6, D4.8, and D4.9. The thereby acquired feedback and lessons-learned will be used for updating the UI in the task T3.4 during months 22-36 with the final specification being reported in the deliverable D3.7.

4.3 Design rationale

We have described the design rationale in D3.1. We would like to elaborate on this by adding the following points:

- The cyber security domain is growing very fast; thus the designed system must allow easy evolution of new tools. The separation of components in our design forces well defined boundaries and a standard API that maintains high deployment independence between components. In our view this will enable easy extendibility of the framework into new domains.
- The designed system must allow cloud deployment while maintaining confidentiality and privacy. This implies that proper data segregation, governance and obfuscation mechanism are required. We believe that the chosen pattern allows adding data governance and obfuscation measure wherever necessary
- The design must allow load scalability for parts of the system, where new components can be flexibly instantiated or terminated. This can create an imbalance between the real-time and offline components, where one would like to run more instances of the real-time components while keeping the offline as is. We believe that the chosen patter allows this with minimal overhead.
- The design must allow multi-tenancy while preserving security, privacy, and access management of tenants.
- The design must allow modular deployment and development of existing and future tools.

In addition, we identified two major use cases for SMESEC Framework: security management and threat defence. This imposed on the design a clear separation of the packages serving those use cases, and a design that supports security management full control of the various threat defence components.

5 Integration of SMESEC tools into the proposed design

5.1 Description of SMESEC tools

We have described the SMESEC partner tools in D3.1. To summarize, the tool set cab be divided into two main categories: real time monitoring and offline discovery, assessment, and protection. The real time monitoring tools cover the following security domains: End-point-protection, network security, honey-pot early warning, and event management. The offline discovery, assessment, and protection cover: moving target, patching, and testing.

5.2 SMESEC tool extensions

During the project the SMESEC tools were enhanced by multiple innovations and extensions, meant to strengthen the market position for each individual tool, raise TRL, and strengthen the SMESEC Framework interconnection capabilities. These extensions are detailed in D3.4 [18]. This section summarizes them.

The SMESEC tool-providing partners worked on two kinds of extensions: individual and collaborative. The individual extensions improve each tool and the work on them was performed by the tool owner. In the collaborative extensions, two or more partners worked together for implementing information exchange and reasoning to provide improved security.

In Deliverable 2.1 [2], a market analysis was performed, and several products extensions were proposed. Most of the proposed extensions were implemented during the Task 3.2.

Atos worked on providing an overview of indicators about cybersecurity threats and attacks, with a focus on indicators for small and medium enterprise networks and worked on extending the SIEM to the IoT domain.

For collaborative extensions, Bitdefender worked on the integration of the GravityZone tool with Atos XL-SIEM, while for individual extension, they improved the ransomware protection and added support for detecting outdated and vulnerable software.

Citrix added new security features such as DDoS, malware and bots detection. They also support more complex security policies and deploy-as-a-service.

EGM integrated in the SMESEC dashboard and added support for more tests, including IoT testing.

FHNW added risk and audit management, data aggregation from multiple sources and custom dashboards.

Forth incorporated SME-oriented honeypots, integrated with the SIEM and the SMESEC dashboard and worked on events correlation from multiple sources.

IBM extended their tools Anti-ROP and AngelEye, while providing a platform for testing JavaScript extensions.

5.1 Integration plan

Figure 25 describes the final integration plan of the SMESEC tools into the SMESEC Framework design. The SMESEC and the tools are planed to be deployed on a cloud to enjoy the flexibility and agility of deployment and development. Where each tool comuunicates via API to the SMESEC Framework.

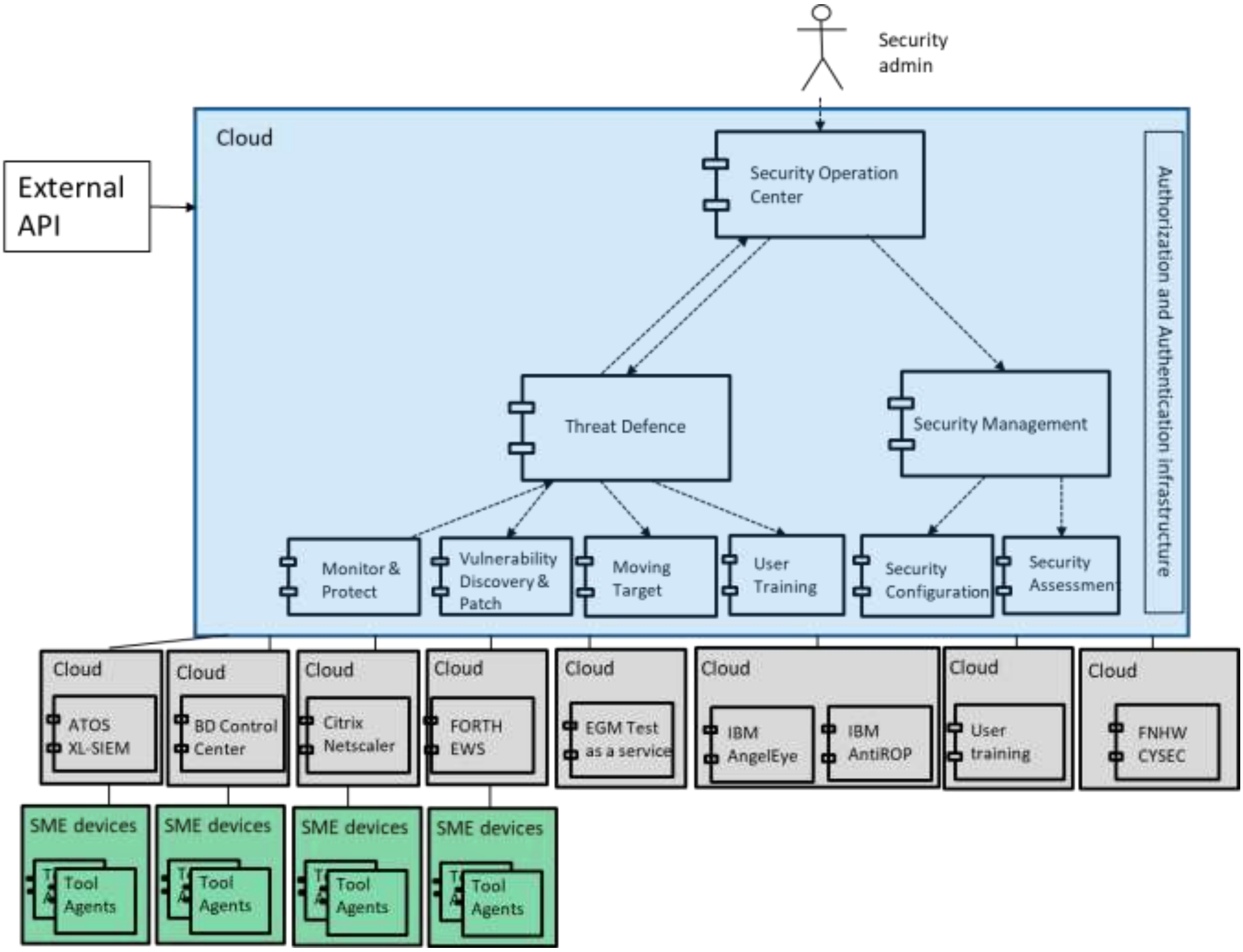


Figure 25: Tool integration

5.2 Modular integration into the proposed design

5.2.1 Modular integration plans

The road to reaching the above integration passes through a modular integration and development of the SMESEC Framework. In the first steps of the project we developed:

- The infrastructure of Authentication and Authorization - an essential step towards decentralized cloud deployment.
- The user interface module - an essential step towards communicating with SME users and receiving feedback.
- The security operation centre – the heart of SMESEC Framework where all innovation around orchestration will take place.
- A communication module – the SMESEC Framework API to all tools.

These are the essential modules to provide a minimal viable product (MVP) that we will evaluate with SMESEC use-case partners. We are developing these module with high degree of modularity in mind that will allow us to reuse code and advance towards the final integration. We are aware that the current integration does not allow many of the non-functional requirements we identified, but achieving the MVP is our top priority at this stage of the project.

5.2.2 Composition view of the integrated Framework

To support the different functionalities of the SMESEC Framework we are following a modular approach that facilitates the development and integration of SMESEC in new and existing systems. Figure 26 shows the different modules and their relations.

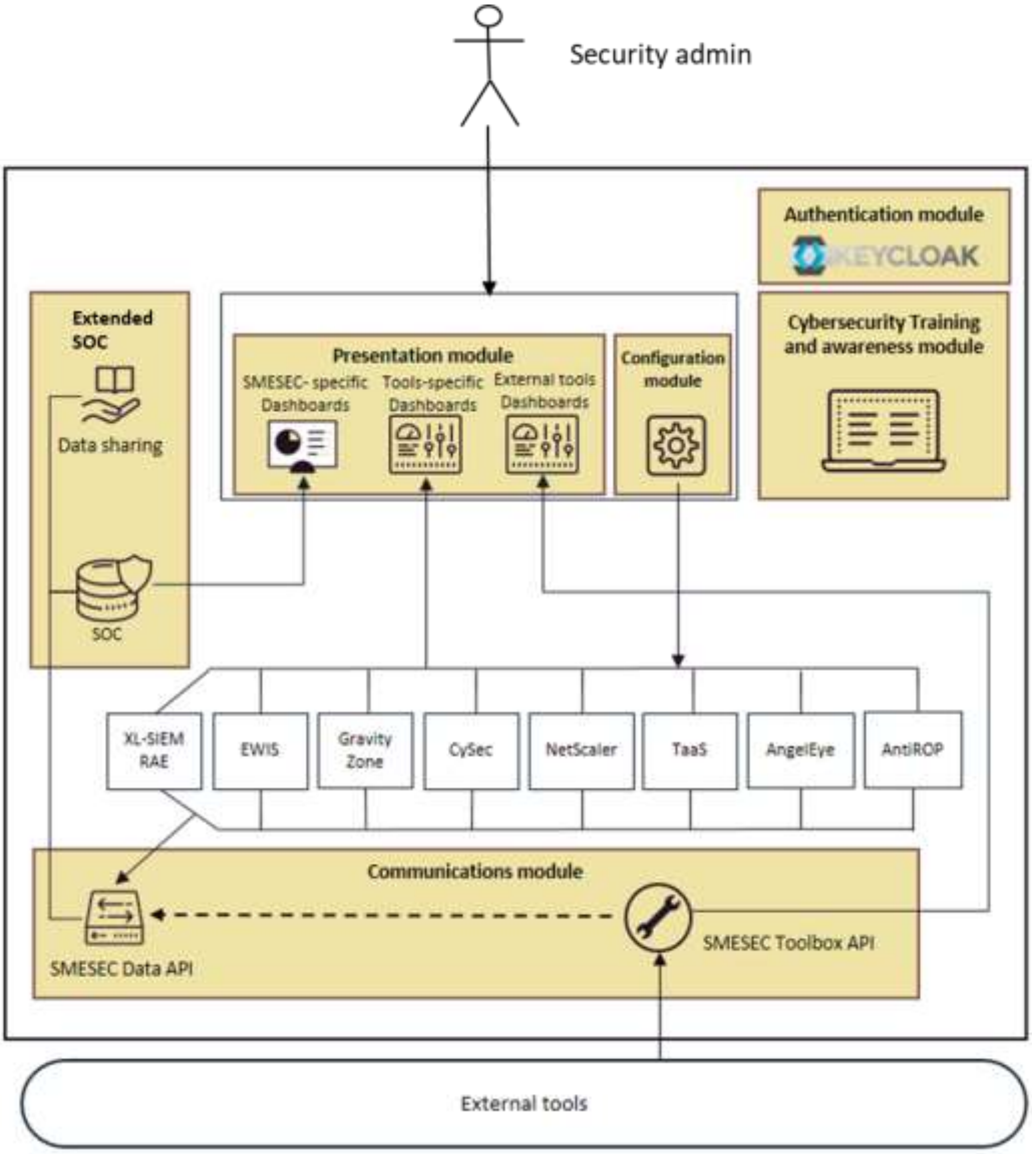


Figure 26: Integrated Framework composition diagram

Following we describe each of the modules and their objectives:

- **Authentication module:** This module handles all the authentication mechanisms present in SMESEC. This module relies on open source project Keycloak [17], configured with different roles for accessing the components present in SMESEC. These roles are already defined in section 4.1.1 of the deliverable.
- **Presentation module:** The presentation module contains different packages for showing information from the data that the solutions integrated in SMESEC provide. It uses different elements for reporting and visualization such as dashboards, alerts, graphs, etc. At this moment, this module allows the representation of the information provided by the tools offered in SMESEC and the data generated by the Security Operations Center.
- **Extended SOC module:** This module contains the Security Operations Center and the data sharing components. These components are in charge of store, analyze and orchestration of

information. The module can be extended with more components such as encryption, history analysis, etc. The output of the module is sent to the presentation module. Finally, this module could allow for information sharing capabilities by allowing input from cybersecurity databases or entities and, that way, improved the result of the protection of SMESEC or provide extra alarms or reports.

- **Communications module:** This module contains the different APIs that are used by SMESEC to communicate with cybersecurity solutions (both the ones extended and improved in SMESEC and third-party ones). The data of this module is exchanged with the intelligence one, in order to make additional data analysis and perform extra functionalities. In this module we provide two different APIs: (1) the SMESEC Data API is used by the SMESEC tools to deliver information to the Security Operations Center. (2) the SMESEC Toolbox API, provides an API to third-party tools for integration in SMESEC. This toolbox API also provides a way to integrate the third-party tools dashboards, in case they exist, into the SMESEC framework.
- **Configuration module:** This module contains the component that allows the user to change some configurations of the different tools present in the framework. These configurations are necessary for the integration of some tools (API keys of some tools, URLs for on premise installations, etc.) and can control also some specific behaviors of the tools and the framework.
- **Training and awareness module:** This module contains both the courses and material for training and a platform for performing courses. This module can be extended with additional elements (different tools or solutions for awareness and training) or even integrated in other elements (for example we are using this modular approach to integrate the training and awareness platform into the SMESEC hub).

5.2.3 Interface view of the integrated Framework

The communication in the SMESEC Framework covers two different elements: communication of the tools of SMESEC with the extended-SOC and presentation modules and the exchange of data of the SMESEC Framework with external tools or entities. These communications can be seen in high-level in the following UML diagram of Figure 27.

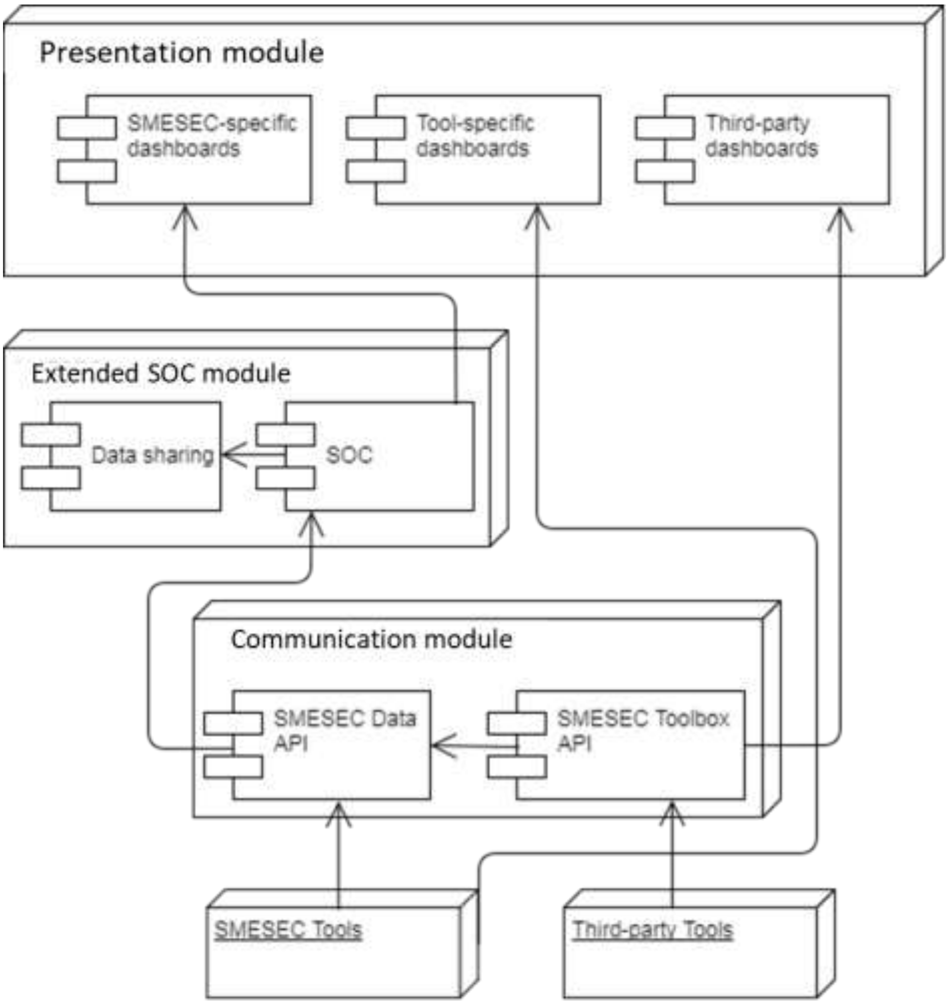


Figure 27: Integrated Framework interface diagram

Following we describe each of these communications at high-level and then the direct connections. The tools, both the ones of SMESEC and the external ones, communicate with the SMESEC Communication module through different APIs. This information is used as the general input for the SOC and uses the available APIs for all the tools. The SMESEC Tools communicate with the SMESEC Data API for exchanging data that will be send to the SOC. Additionally, this component interacts directly with the SMESEC tools-specific dashboards for showing the output of their functionalities. The Third-party Tools communicate with the SMESEC Toolbox API, which is the connection for external tools. This API communicates with the SMESEC Data API for data that could be used for the SOC (as the external tools could provide new functionalities or be used instead of the existing ones of SMESEC) and the Third-party dashboards for showing their direct output.

The SMESEC Communication module communicates with the SMESEC Extended SOC module and the SMESEC UI Module. Regarding the first one it provides the information of the tools to the SOC for use and information sharing through the data exchange module. Additionally, as commented before, the SMESEC Toolbox API communicates with the SMESEC UI Module for showing the output of the functionalities of the external tools.

Finally, the SMESEC UI Module receives information of the previous modules in order to present the output of the functionalities, being this of the SMESEC tools, external tools or SOC.

5.2.4 SMESEC Communication API

This section describes the current status of the creation of the API for external communications at the higher level of the SMESEC Framework.

5.2.4.1 Alert object

The API allows transformation of alert objects. The alerts follow the Malware Information Sharing Platform (MISP) standard. MISP is an EU founded project aiming to draw near threat intelligence information to any end user for free. The retrieved object will be in alert format. All the fields that the object has are explained in Table 5 below.

Table 5: Model for alert object

Id	Integer
title	string
	maxLength: 256
description	string
	maxLength: 256
recurrence	integer
	default: 1
resolved_at	string($date-time)
assigned_to	string
	maxLength: 64
updated_by	string
	maxLength: 64
resolved_by	string
	maxLength: 64
related_item_id	string
	maxLength: 32
related_item_type	string
	maxLength: 32
address	string
	maxLength: 256
meta_type	string
	maxLength: 32
type	string
	maxLength: 256
sub_type	string
	maxLength: 32

absolute_value	number($float)
absolute_difference	number($float)
score_value	number($float)
severity	integer
status	integer
	default: 0
operative_status	integer
	default: 0
created_at	string
	readOnly: true
updated_at	String
	readOnly: true

In the next sessions there is the description of the available options to extract information from the API. This is the current version up, running and tested.

5.2.4.2 GET

ALERTS

[GET/alerts] – Retrieves one or more alerts.

- Parameters: No parameters.
- Responses (if code 200)
  - Description: Array containing alert objects.
  - Content type: json/xml.
  - Links: No links.

ALERTS (With alert ID)

[GET/alerts{alertID}] – Retrieves one alert.

- Parameters:
  - Integer: Alert Id.
- Responses (if code 200)
  - Description: Array containing alert objects.
  - Content type: json/xml.
  - Links: No links.

5.2.4.3 POST

ALERTS

[POST/alerts] – Stores one or more alert.

- Parameters:
  - Object: Alert.

- Content type: json/xml.

- Responses (if code 201)
  - Description: Operation has been successful.

5.2.4.4 PUT

ALERTS (With alert ID)

[PUT/alerts{alertID}] – Replaces an alert.

- Parameters:
  - Integer: Alert Id.
- Responses (if code 200)
  - Description: Array containing alert objects.
  - Content type: json/xml.
  - Links: No links.

6 SMESEC Framework Functionalities

The SMESEC Framework aims to support SMEs in different ways:

- Providing cybersecurity solutions for the protection of their business and employees.
- Increasing awareness of employees with courses, training tools and material.
- Analyze information of the cybersecurity ecosystem and inform via alarms and notifications to SMEs about potential problems.

All these functionalities are supported by either the tools of SMESEC, which have been extended and enhanced in the project to cover the identified needs of SMEs, or by the SMESEC Framework. The SMESEC Framework, as presented in the previous sections has a modular architecture that allows the different modules to provide specific functionalities. Following we present a high-level description of the functionalities provided by the SMESEC Framework and then a more low-level definition with the properties and characteristics of the tools of SMESEC.

6.1 SMESEC Framework security operations center

We start by describing the functionalities made possible by the interconnection of the SMESEC tools and the security operations centre this Framework provides. These are functionalities provided and are beyond the collection of tools' functionalities that will be described in the following section.

The main added value of SMESEC Framework is delivered by the security operations centre (SOC) component that resides in the SMESEC Framework top layer. This component receives data from all other components of the SMESEC Framework and requests from the user-interface and orchestrates the later to provide monitoring, forensics and response functionality beyond the functionalities provided by each one of the SMESEC tools that can be accessed by the SMESEC Framework UI.

To enable the above functionalities, structured data of the alerts provided by the various tools is collected in the SOC component. The alerts provided follow the Malware Information Sharing Platform (MISP) standard. MISP is an EU founded project aiming to draw near threat intelligence information to any end user for free. The core format for the transmission is a JSON file that will allow the systems to communicate between each other. All the information regarding the data models for the information exchange can be found in [16].

Orchestrated monitoring functionality is provided by implementing rule based and machine learning analysis for incident detection using alerts' info. The rule engine will allow implementation of configurable rules that the user can edit, change and upload via UI. We will provide a default rule package and allow community development of this package in a public repository. Next, we will develop machine learning algorithms that will consume these alerts and implement anomaly detection algorithms that will automatically detect new incidents that escaped the rule-based engine detection.

This orchestrated monitoring will be able to detect kill chains and advanced persistent threats (APT) in the SME's system.

Forensics functionality is provided by implementing a set of queries over the alerts database that relate to an alert-under-investigation. These queries are predefined, configurable per alert, and can be executed from the UI. Results of these queries will be presented in the UI. Configuration of queries will be available from the SMESEC Framework UI. An example use case of the forensics functionality is: a user chose an alert for investigation, a set of investigation queries are offered for the user along with configuration options, the user choses a query for execution, and the SMESEC Framework returns the query result. An example configurable query is: Please provide all alerts for the same alert-type within last time-window, while time window is configurable, and the default is one-day.

Response functionality is provided by implementing a set of configurable processes that provide a response per alert. The response pre-defined processes cover the following areas:

- Security event notification and escalation – an automatic or semi-automatic process for notifying security admin of high risk alerts and automatic escalation of security configuration of all SMESEC security tools.
- Law enforcement involvement – a semi-automatic process for notification of law enforcement parties in adherence with incident response regulations.
- Public relations – a semi-automatic process for public relations notification and mitigation of damage to reputation with adherence to incident response regulations.
- Security device failure – an automatic or semi-automatic process for notifying security admin of failure of a security device.
- SMESEC tool provider involvement - an automatic or semi-automatic process for notifying SMESEC tool provider of an escaped attacks, false alerts, or failure of their device.

Additionally, the framework provides other functionalities that are useful for other features different of cybersecurity:

- Generation of cybersecurity intelligence for data sharing: the Security Operations Center allows the sharing of data (using anonymization and protection techniques) generated in the framework after the analysis of the cybersecurity status. This allows informing users of the SMESEC community of cybersecurity topics, last detected attacks and viruses, etc. or any other information gathered from the different systems running SMESEC. The information can also be shared with other entities such as CERTs to help protecting systems (e.g. ransomwares).
- Integration of external tools: SMESEC provides a API for integration of third-party tools in the framework and take advantage of them, either as stand-alone functionalities, integrated in the SOC for more complex functionalities or replacing one of the existing tools of the framework.

We are also researching solutions to following problems:

- 24x7 response – an automatic response outside of security admin work hours. We have identified the lack of constant monitoring (24-hour, 7-days a week) of the SMEs system by a security admin as an issue for SMEs. This issue arises from the combination of scarce staffing of the security admin role (if this role is staffed), and the requirement of constant availability of the SMEs system. We are researching solutions for this issue in directions of rules for automatic and configurable response process. Also, machine learning will be considered to solve this problem.

- Asset discovery and management – an automatic tool that discovers all assets in the SME's system.
- Vulnerability manager – an automatic tool that scans for known-vulnerabilities in the SME's system.

All the functionalities described here are work-in-progress and we plan to continue working in extending them and including new ones to support better the needs of SMEs. This will be evaluated both with the use case of the partners and the open call of the project. It will allow us to create more functionalities and increase the adoption of SMESEC in the market.

6.2 SMESEC tool-specific functionalities

The SMESEC tools provide a wide range of functionalities that are combined through a centralized offering and provide the following capabilities. A detailed list of the functionalities can be found in Table 6 describing functionality, provider and accessibility from the dashboard.

Table 6: Tool functionalities accessible from dashboard

Tool	Functionalities offered	Dashboard	Functionality
ATOS Risk Assesment Engine	• Risk assessment from business profile and vulnerability scan	Yes	Protection and reporting
IBM AngelEye	• Check binaries or source code for possible vulnerabilities	No	Discover
EGM TaaS	• Full test suites concerning security issues	Yes	Discover
IBM AntiROP	• Shuffles a binary file to avoid ROP attacks	No	Protection and reporting
BitDefender Total Security	• Quick scan: it scans only critical Windows and Linux system locations. It does not remove malware, to do that you need to do a full scan • Full Scan: Checks the entire system. • Memory Scan: This checks the programs that are running in the virtual machine memory. • Network scan: This allows scanning the network drives only if the BitDefender agent is installed on the target virtual machine. • Custom scan: Allows the user to create a scan with their preferences	Yes	Protection and reporting
CITRIX NetScaler	• Web Application Firewall • Secure Web Gateway • VPN	Yes	Monitoring
ATOS XL-SIEM	• Collects information about security events and alarms in real time • Priorization, filtering and normalization of the different data	Yes	Monitoring
FORTH EWIS	• Honeypot system for early detection of attacks	Yes	Monitoring
FHNW CySec	• Benchmark about product and SME maturity	Yes	Training,

Tool	Functionalities offered	Dashboard	Functionality
	level following the SMESEC maturity model developed by University of Utrecht. • Identification of missing gaps and proposals of measures to improve security. • Awareness about cyber threats and referral to relevant training and tools. • Guidance for capability improvement, including schedule-setting, reminders, and user feedback.		management
Training platform	• Training employees	Yes	Train

7 Conclusions

We have developed the unified architecture based on the system design that we have proposed earlier in "SMESEC System Design" (D3.1) [15]. We refined the requirement collection methodology documentation and updated the SMESEC requirements according to feedback we gathered so far. We have focused our effort around three areas: Further development of design views, integration of the SMESEC tools into the SMESEC Framework, and designing the functionalities of the SMESEC Framework beyond the collection of functionalities provided by the tools.

We have developed design views with in depth information and diagrams and added interaction and deployment views. We have added new use cases to the context view and updated composition and interface view accordingly. Further we updated the views to address new requirements of the SMESEC framework like allowing forensics capability and as-a-service deployment of the SMESEC Framework.

We have described our vision for integration of tools into SMESEC Framework and described the planned modular integration. We explained why this modular integration is the best integration choice and fastest path for creating a minimal viable product that will allow us to receive feedback from our use case partners in the next phase of the project.

We have described the collection of functionalities of the SMESEC tools and defined the functionalities of the SMESEC Framework beyond the tools' functionalities. We have identified orchestrated monitoring, forensics and automated response as the main functionalities provided by this Framework.

Further, we have developed the SMESEC user interface (UI) to answer usability requirements by multiple-persona of the SME's security admin. We developed this UI while keeping in mind that the use case persona if this framework is constantly evolving and acquiring more expertise in the field of security.

This document will serve as basis for "SMESEC Unified Architecture and the Initial Version of the SMESEC Framework prototype" (D3.3), and further development of design views and SMESEC innovation directions will reside in the "SMESEC Unified Architecture and the Initial Version of the SMESEC Framework prototype" (D3.3).

References

[1] "IEEE Standard for Information Technology-Systems Design- Software Design Descriptions, IEEE STD 1016-2009," 2009.

[2] SMESEC deliverable 2.1 “SMESEC security characteristics description, security and market analysis report”, George Oikonomou, 2017.

[3] SMESEC deliverable 2.2 “SMESEC security products unification report”, Ciprian OPRIȘA, 2017

[4] SMESEC deliverable 2.3 “Security Awareness Plan Report”, Samuel Fricker, 2017

[5] SMESEC deliverable 6.1 “Dissemination plan and market analysis”, Giunta Nicolas, 2017.

[6] H2020 Call Topic DS-02-2016, https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/ds-02-2016.html , 2018/02/06.

[7] Apache Storm, https://storm.apache.org , 2018/02/06.

[8] OSSIM: The Open Source SIEM | Alien Volt, https://www.alienvault.com/products/ossim , 2018/02/06.

[9] Bitdefender Advanced Threat Control, http://businessresources.bitdefender.com/hubfs/Bitdefender-Business-2015-SolutionPaper-ATC-93030-en_EN-web.pdf?adobe_mc=MCMID%3D31252819958915218863986580919594145170%7CMCORGID%3D0E920C0F53DA9E9B0A490D45%2540AdobeOrg%7CTS%3D1516630856 , 2018/02/06.

[10] Citrix NetScaler AppFirewall and Web App Service, https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-netscaler-application-firewall-datasheet.pdf , 2018/02/06.

[11] NetScaler Unified Gateway, https://www.citrix.com/products/netscaler-unified-gateway/ , 2018/02/06.

[12] SMESEC Grant Agreement no. 740787 – Annex I Description of the Action (Part B), April 2017.

[13] Spruit, M. CYSFAM, Cyber Security Focus Area Maturity Model, in publication.

[14] OWASP Top Ten Project, https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project, 2018/02/16

[15] SMESEC deliverable 3.1 “SMESEC System Design”, Fady Copty, 2018.

[16] MISP data models – MISP core format, MISP taxonomies, https://www.misp-project.org/datamodels, 2018/12/10

[17] Keycloack, https://www.keycloak.org/, 2018/12/10

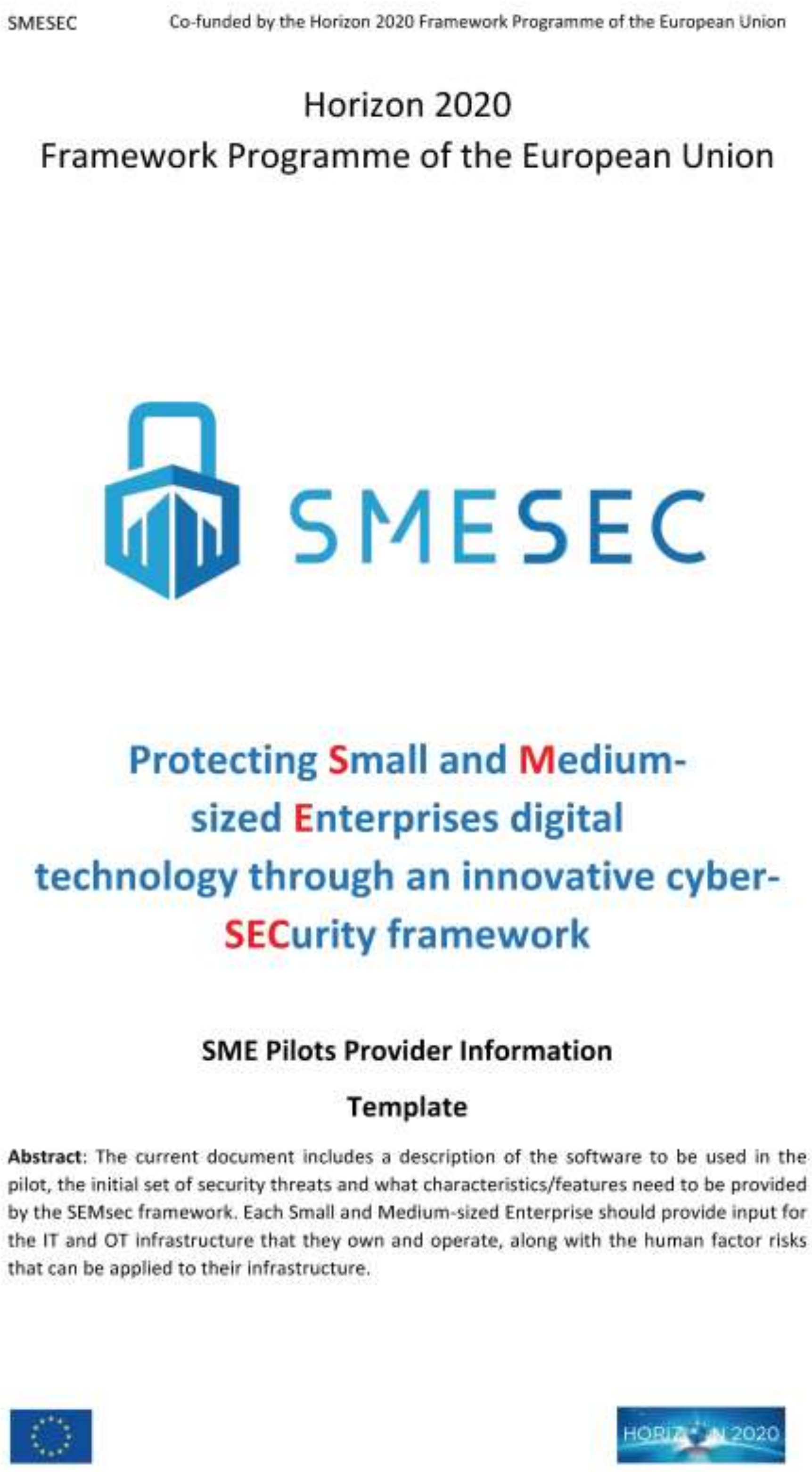
[18] SMESEC deliverable 3.4 “SMESEC products integration on the Unified Architecture”, Ciprian OPRIȘA, 2018

[19] SMESEC – Cybersecurity for SMEs, www.smesec.eu, 2018/12/10

[20] Presentation-Abstraction-Control – Wikipedia, https://en.wikipedia.org/wiki/Presentation%E2%80%93abstraction%E2%80%93control, 2018/12/14

[21] Persona (user experience) – Wikipedia, https://en.wikipedia.org/wiki/Persona_(user_experience), 2018/14/14

Annex A: Requirements Elicitation Template



SMESEC Co-funded by the Horizon 2020 Framework Programme of the European Union

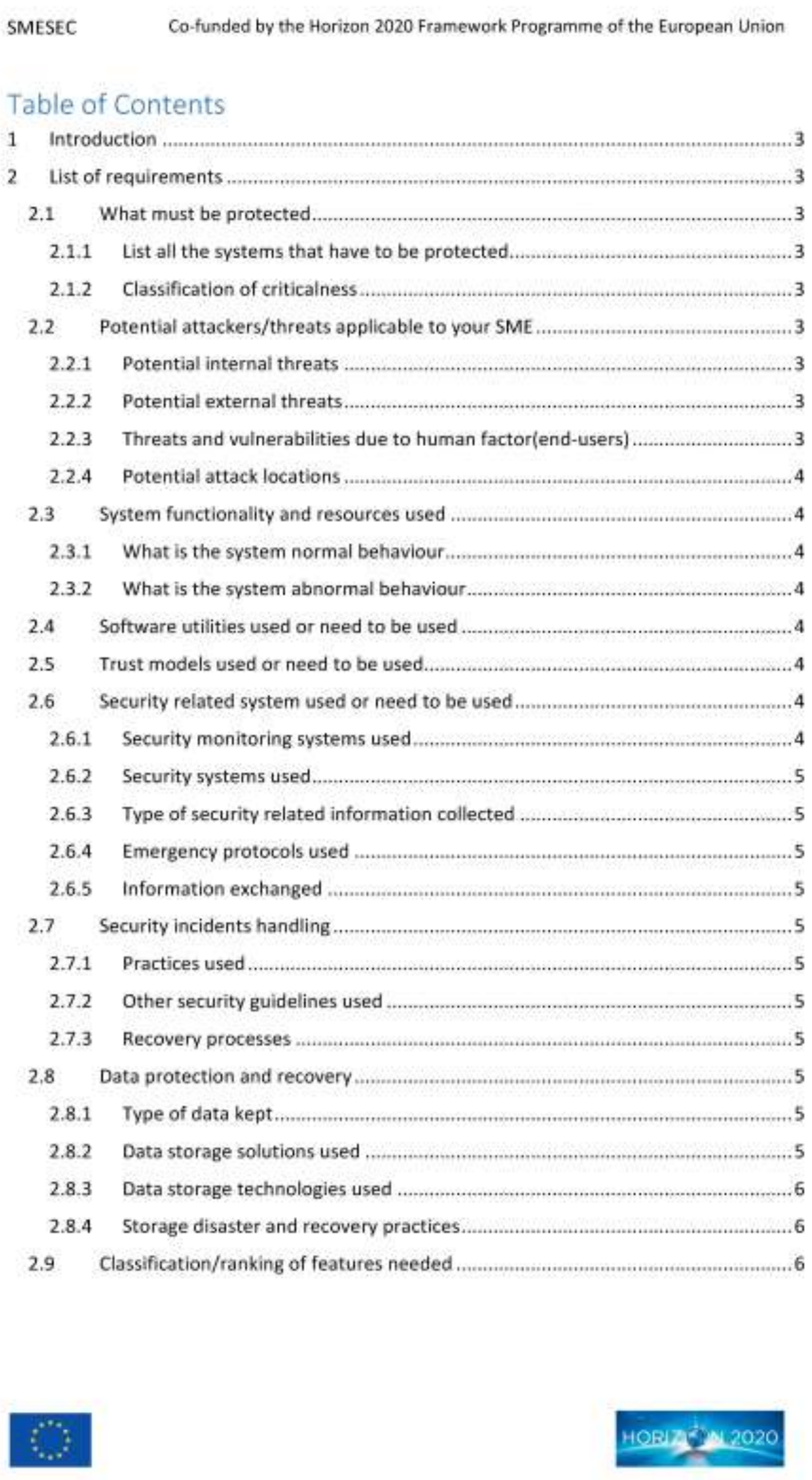
Horizon 2020
Framework Programme of the European Union

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

SME Pilots Provider Information

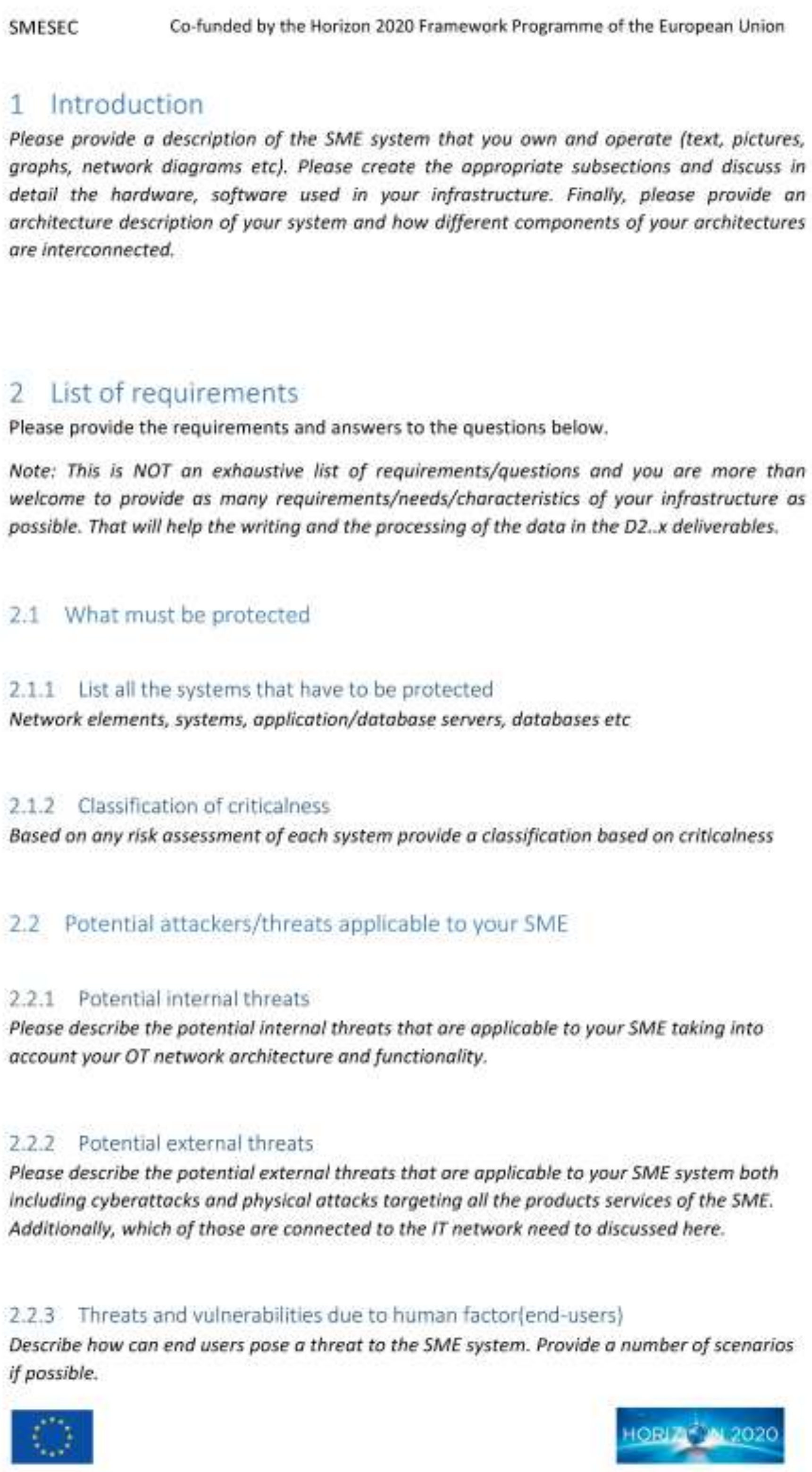
Template

Abstract: The current document includes a description of the software to be used in the pilot, the initial set of security threats and what characteristics/features need to be provided by the SEMsec framework. Each Small and Medium-sized Enterprise should provide input for the IT and OT infrastructure that they own and operate, along with the human factor risks that can be applied to their infrastructure.



SMESEC Co-funded by the Horizon 2020 Framework Programme of the European Union

Table of Contents



SMESEC Co-funded by the Horizon 2020 Framework Programme of the European Union

1 Introduction

Please provide a description of the SME system that you own and operate (text, pictures, graphs, network diagrams etc). Please create the appropriate subsections and discuss in detail the hardware, software used in your infrastructure. Finally, please provide an architecture description of your system and how different components of your architectures are interconnected.

2 List of requirements

Please provide the requirements and answers to the questions below.

Note: This is NOT an exhaustive list of requirements/questions and you are more than welcome to provide as many requirements/needs/characteristics of your infrastructure as possible. That will help the writing and the processing of the data in the D2..x deliverables.

2.1 What must be protected

2.1.1 List all the systems that have to be protected

Network elements, systems, application/database servers, databases etc

2.1.2 Classification of criticalness

Based on any risk assessment of each system provide a classification based on criticalness

2.2 Potential attackers/threats applicable to your SME

2.2.1 Potential internal threats

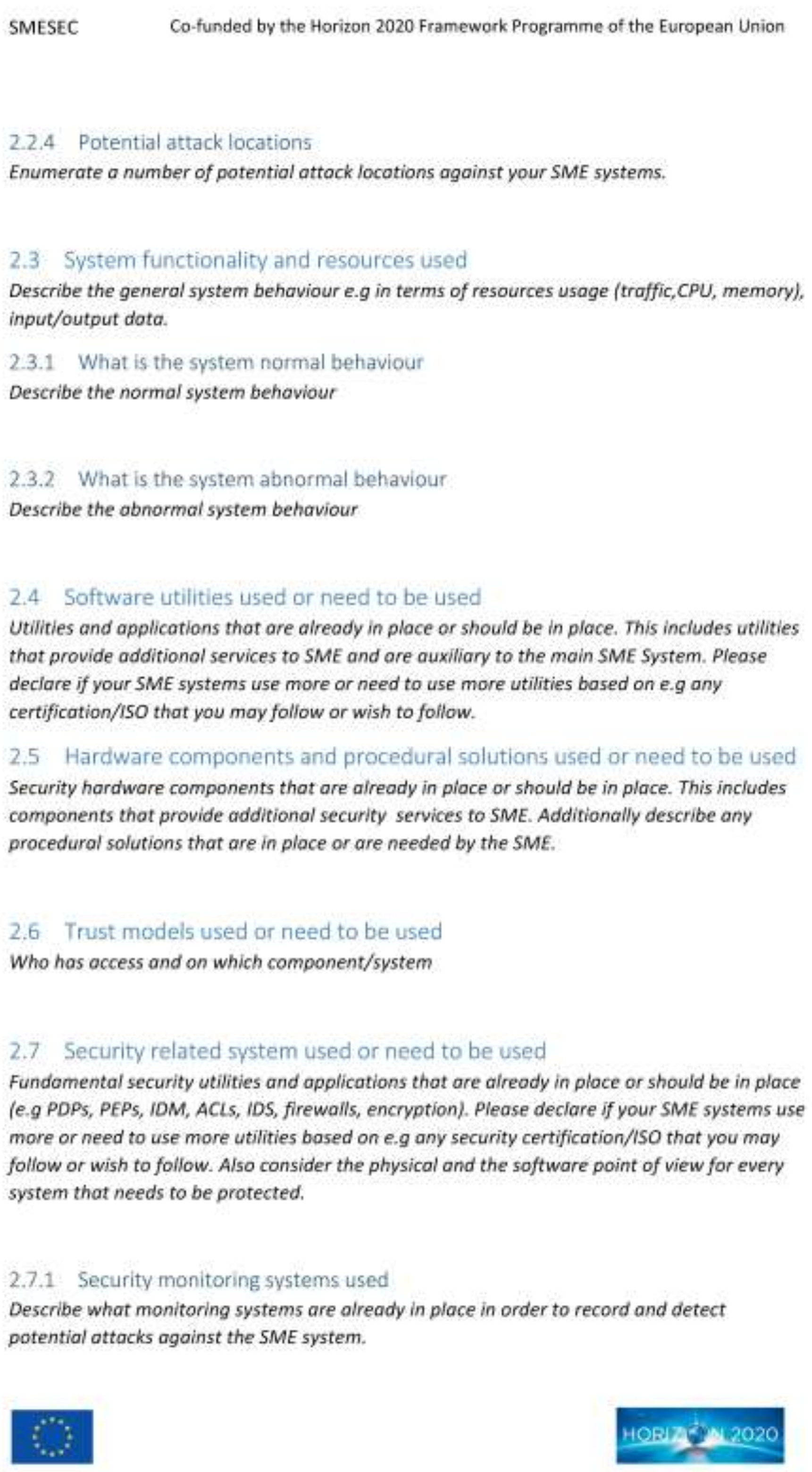
Please describe the potential internal threats that are applicable to your SME taking into account your OT network architecture and functionality.

2.2.2 Potential external threats

Please describe the potential external threats that are applicable to your SME system both including cyberattacks and physical attacks targeting all the products services of the SME. Additionally, which of those are connected to the IT network need to discussed here.

2.2.3 Threats and vulnerabilities due to human factor(end-users)

Describe how can end users pose a threat to the SME system. Provide a number of scenarios if possible.



SMESEC Co-funded by the Horizon 2020 Framework Programme of the European Union

2.2.4 Potential attack locations

Enumerate a number of potential attack locations against your SME systems.

2.3 System functionality and resources used

Describe the general system behaviour e.g in terms of resources usage (traffic,CPU, memory), input/output data.

2.3.1 What is the system normal behaviour

Describe the normal system behaviour

2.3.2 What is the system abnormal behaviour

Describe the abnormal system behaviour

2.4 Software utilities used or need to be used

Utilities and applications that are already in place or should be in place. This includes utilities that provide additional services to SME and are auxiliary to the main SME System. Please declare if your SME systems use more or need to use more utilities based on e.g any certification/ISO that you may follow or wish to follow.

2.5 Hardware components and procedural solutions used or need to be used

Security hardware components that are already in place or should be in place. This includes components that provide additional security services to SME. Additionally describe any procedural solutions that are in place or are needed by the SME.

2.6 Trust models used or need to be used

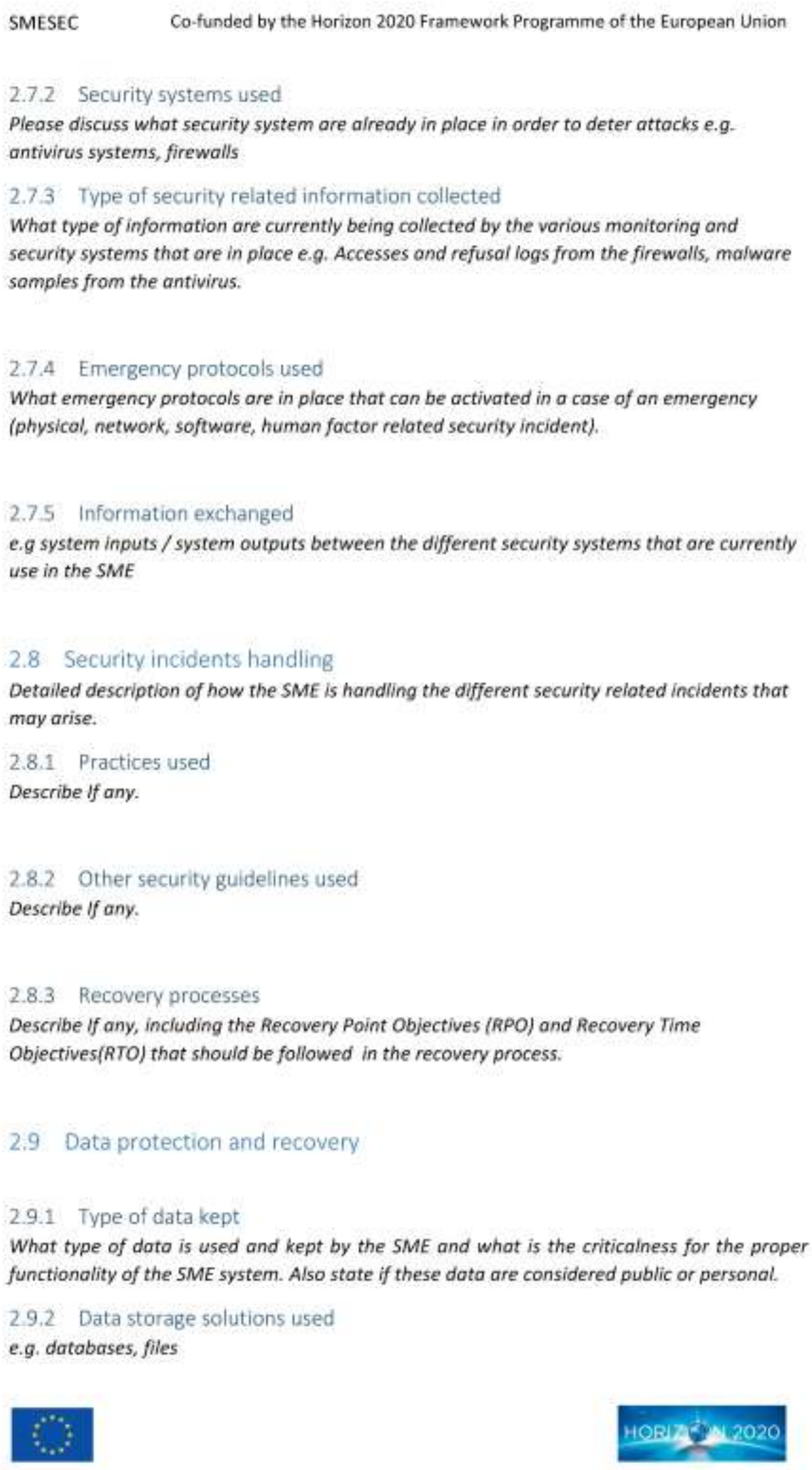
Who has access and on which component/system

2.7 Security related system used or need to be used

Fundamental security utilities and applications that are already in place or should be in place (e.g PDPs, PEPs, IDM, ACLs, IDS, firewalls, encryption). Please declare if your SME systems use more or need to use more utilities based on e.g any security certification/ISO that you may follow or wish to follow. Also consider the physical and the software point of view for every system that needs to be protected.

2.7.1 Security monitoring systems used

Describe what monitoring systems are already in place in order to record and detect potential attacks against the SME system.



SMESEC Co-funded by the Horizon 2020 Framework Programme of the European Union

2.7.2 Security systems used

Please discuss what security system are already in place in order to deter attacks e.g. antivirus systems, firewalls

2.7.3 Type of security related information collected

What type of information are currently being collected by the various monitoring and security systems that are in place e.g. Accesses and refusal logs from the firewalls, malware samples from the antivirus.

2.7.4 Emergency protocols used

What emergency protocols are in place that can be activated in a case of an emergency (physical, network, software, human factor related security incident).

2.7.5 Information exchanged

e.g system inputs / system outputs between the different security systems that are currently use in the SME

2.8 Security incidents handling

Detailed description of how the SME is handling the different security related incidents that may arise.

2.8.1 Practices used

Describe If any.

2.8.2 Other security guidelines used

Describe If any.

2.8.3 Recovery processes

Describe If any, including the Recovery Point Objectives (RPO) and Recovery Time Objectives(RTO) that should be followed in the recovery process.

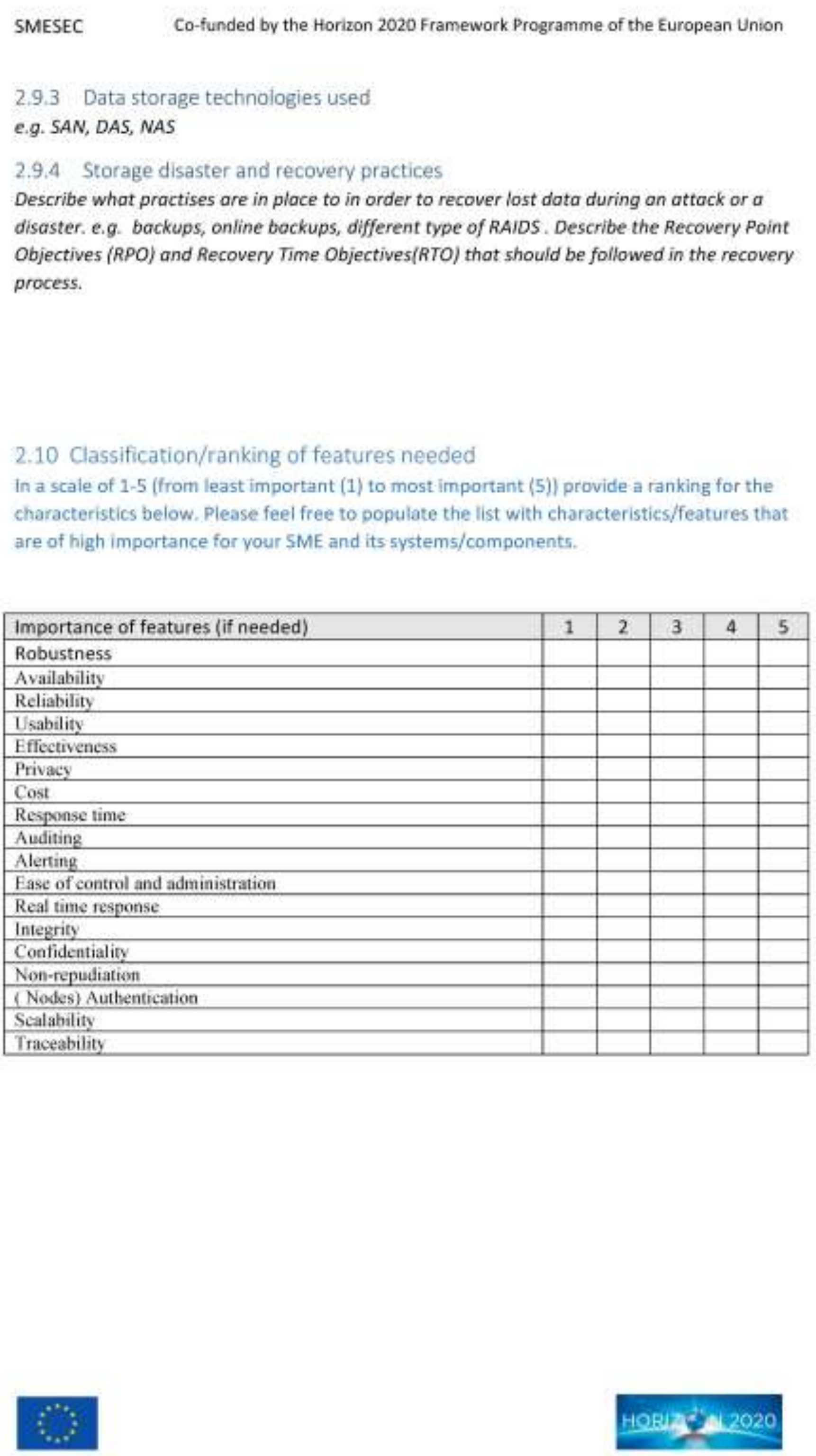
2.9 Data protection and recovery

2.9.1 Type of data kept

What type of data is used and kept by the SME and what is the criticalness for the proper functionality of the SME system. Also state if these data are considered public or personal.

2.9.2 Data storage solutions used

e.g. databases, files



SMESEC Co-funded by the Horizon 2020 Framework Programme of the European Union

2.9.3 Data storage technologies used

e.g. SAN, DAS, NAS

2.9.4 Storage disaster and recovery practices

Describe what practises are in place to in order to recover lost data during an attack or a disaster. e.g. backups, online backups, different type of RAIDS . Describe the Recovery Point Objectives (RPO) and Recovery Time Objectives(RTO) that should be followed in the recovery process.

2.10 Classification/ranking of features needed

In a scale of 1-5 (from least important (1) to most important (5)) provide a ranking for the characteristics below. Please feel free to populate the list with characteristics/features that are of high importance for your SME and its systems/components.

Importance of features (if needed)	1	2	3	4	5
Robustness					
Availability					
Reliability					
Usability					
Effectiveness					
Privacy					
Cost					
Response time					
Auditing					
Alerting					
Ease of control and administration					
Real time response					
Integrity					
Confidentiality					
Non-repudiation					
(Nodes) Authentication					
Scalability					
Traceability					