



SMESEC

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

D3.4 SMESEC products integration on the Unified Architecture

Document Identification			
Status	Final	Due Date	30/11/2018
Version	1.1	Submission Date	21/12/2018

Related WP	WP3	Document Reference	D3.4
Related Deliverable(s)	D2.1, D2.2, D3.2	Dissemination Level (*)	PU
Lead Organization	BD	Lead Author	Ciprian OPRIȘA
Contributors	ATOS, CITRIX, EGM, FHNW, FORTH, IBM	Reviewers	Christos Tselios, CITRIX
			Fady Copt, IBM

Keywords:
Innovations, extensions, market analysis, market benefits, integration

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

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

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

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

Document Information

List of Contributors	
Name	Partner
Jose Francisco RUIZ	ATOS
Ciprian OPRIȘA	BD
Ovidiu MIHĂILĂ	BD
Christos TSELIOS	CITRIX
Abbas AHMAD	EGM
Samuel FRICKER	FHNW
Martin GWERDER	FHNW
Manos ATHANATOS	FORTH
Christos PAPACHRISTOS	FORTH
Sotiris IOANNIDIS	FORTH
Fady COPTY	IBM

Document History			
Version	Date	Change editors	Changes
0.1	11/10/2018	Ciprian OPRIȘA BD	The 1 st draft of the deliverable.
0.2	20/11/2018	Ciprian OPRIȘA BD	Added contributions from BD, EGM, FORTH, FHNW
0.3	26/11/2018	Ciprian OPRIȘA BD	Added market benefits section
0.4	27/11/2018	Ciprian OPRIȘA BD	Added contributions from ATOS, CITRIX, IBM
0.5	06/12/2018	Ciprian OPRIȘA BD	Refined the document
1.0	20/12/2018	Ciprian OPRIȘA BD	Integrated the comments from the reviews.
1.1	21/12/2018	ATOS	Quality Review and Submission

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Ciprian Oprisa (BD)	21/12/2018
Technical manager	Christos Tselios (Citrix)	21/12/2018
Quality manager	Rosana Valle Soriano (Atos)	21/12/2018
Project Manager	Jose Fran. Ruíz (Atos)	21/12/2018

Document name:	D3.4 SMESEC products integration on the Unified Architecture	Page:	2 of 66
Reference:	D3.4	Dissemination:	PU
	Version:	1.1	Status:
			Final

Table of Contents

Document Information	2
Table of Contents	3
List of Tables.....	5
List of Figures	6
Executive Summary	7
1 Introduction.....	8
1.1 Purpose of the document	8
1.2 Relation to another project work	8
1.3 Structure of the document	8
2 Innovation Areas and Market Requirements.....	9
2.1 Overview	9
2.2 Lessons learned from the market requirement analysis.....	9
2.3 Proposed extensions summary	10
3 Product extensions	14
3.1 ATOS extensions.....	14
3.1.1 IoT Extension for XL-SIEM	14
3.1.2 Risk Assessment Engine - Indicators for SMEs about cybersecurity threats and attacks .	17
3.2 BD extensions.....	21
3.2.1 Integration of Bitdefender GravityZone with ATOS XL-SIEM	21
3.2.2 Improved ransomware protection.....	23
3.2.3 Outdated software detection	23
3.3 CITRIX extensions.....	24
3.3.1 Citrix ADC Platforms and Deployment Options.....	25
3.3.2 Features at a Glance.....	26
3.3.3 Citrix ADC extensions for seamless SMESEC framework integration	28
3.4 EGM extensions	34
3.4.1 ATOS collaboration.....	34
3.4.2 Keycloak related work.....	35
3.4.3 Architecture related work	36
3.5 FHNW extensions	37
3.5.1 CySeC integrated SAML2 and OAuth2 authentications for a unified framework.....	40

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	3 of 66		
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status:	Final

3.5.2	Development of the SMESEC common branding standards.....	40
3.5.3	CYSEC System Context, Users, and Use.....	41
3.5.4	Overview of Features	44
3.5.5	CYSEC.F01: Capability Improvement Dashboard	45
3.5.6	CYSEC.F02: Capability Improvement Journey	48
3.5.7	CYSEC.F03: Capability Improvement Specification.....	50
3.5.8	CYSEC.F04: Backlog and Reminder Management	52
3.5.9	Feature: Community Report.....	54
3.5.10	Hybrid Public-Cloud Multi-Tenant Service and On-Premise Deployment.....	56
3.5.11	Discussion	57
3.6	FORTH extensions	58
3.7	IBM extensions.....	60
3.7.1	IBM Anti-ROP Extensions.....	60
3.7.2	Testing platform Java script extension	61
3.7.3	AngelEye extensions	61
4	Market benefits brought by innovations.....	62
4.1	Context	62
5	SMEs struggle not only due to a lack of awareness, but also because they perceive cybersecurity as a costly endeavour.....	63
5.1	The SMESEC proposal	63
5.2	The SMESEC innovations and their market impact.....	63
6	Conclusions.....	65
7	Appendix 1.....	66
	Technical constraints of the IoT device of WorldSensing used in their use case.....	66

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	4 of 66	
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status: Final

List of Tables

Table 1: CYSEC features representing FHNW individual extensions..... 44

Table 2: Elements of the CYSEC Dashboard..... 46

Table 3: Elements of the backlog and reminder management 52

Document name:	D3.4 SMESEC products integration on the Unified Architecture				Page:	5 of 66
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status: Final

List of Figures

<i>Figure 1: High-level description of XL-SIEM agent</i>	16
<i>Figure 2: Memory consumed by XL-SIEM agent</i>	16
<i>Figure 3: Memory consumed by XL-SIEM IoT agent</i>	17
<i>Figure 4: Adding a target in Risk Assessment Engine (I)</i>	18
<i>Figure 5: Adding a target in Risk Assessment Engine (II)</i>	18
<i>Figure 6: Assets in Risk Assessment Engine</i>	19
<i>Figure 7: Selecting Models in Risk Assessment Engine</i>	19
<i>Figure 8: Qualitative Report of Risk Assessment Engine</i>	20
<i>Figure 9: Quantitative Report of Risk Assessment Engine</i>	20
<i>Figure 10: GravityZone configuration for syslog events</i>	22
<i>Figure 11: Enabling syslog notifications</i>	22
<i>Figure 12: Bitdefender Patch Management</i>	24
<i>Figure 13: Typical VPX in AWS deployment</i>	29
<i>Figure 14: Citrix ADC AppFirewall</i>	30
<i>Figure 15: Citrix Unified Gateway</i>	31
<i>Figure 16: Citrix NetScaler Secure Web Gateway</i>	32
<i>Figure 17: KeyCloak authentication page</i>	34
<i>Figure 18: TaaS frontend</i>	35
<i>Figure 19: Keycloak-js interfaces typed on keycloak.d.ts</i>	36
<i>Figure 20: TaaS adapted architecture</i>	37
<i>Figure 21: Excerpt from the branding document</i>	40
<i>Figure 22: CYSEC deployment scenario and external interfaces towards the users and the SMESEC framework</i>	42
<i>Figure 23: Question-answer loop of assessing SME capabilities and</i>	43
<i>Figure 24: capability improvement dashboard.</i>	45
<i>Figure 25: Example of a CYSEC question contained in a capability improvement journey.</i>	49
<i>Figure 26: Example of a successful conclusion of a capability improvement journey.</i>	50
<i>Figure 27: XSD of the CYSEC capability improvement specification.</i>	51
<i>Figure 28: Excerpt of an XML-based specification of a capability improvement journey.</i>	52
<i>Figure 29: Control loop of enabling self-adaptation based on (Cheng et al., 2009).</i>	55
<i>Figure 30: model of the data offered for analysis and community reporting.</i>	56
<i>Figure 31: Integrated FORTH EWIS Homepage, seen through SMESEC web application</i>	59

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	6 of 66		
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status:	Final

Executive Summary

This deliverable presents the work for extending the SMESEC products and integrating them into the SMESEC framework. This work was performed in Task 3.2, “Enhance SMESEC market products with the latest research innovations”.

After the market study in D2.1, some extensions and innovations were identified and proposed for each product. In Task 3.2, the product owners worked individually or collaboratively, in order to implement these extensions. Most of the work done in this task followed the proposal from D2.1, with only minor changes. Some SMESEC partners added more extensions, while other extensions were removed or replaced for incorporating more generic features.

The work was focused on implementing the extensions necessary for integrating the products into the SMESEC framework. The tools need the ability to share security data with other tools, make use of the data received from other tools or to integrate into the framework and be orchestrated by the Security Operations Centre. Besides the integration efforts, there were also efforts to improve the quality of each tool using the market analysis results and the pilot’s insights.

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	7 of 66		
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status:	Final

1 Introduction

1.1 Purpose of the document

The document is the 4th deliverable of WP3 “SMESEC security framework development for small-medium companies and organizations”. As the work package title states, it deals with the framework development. The current deliverable describes the product innovations and extensions, the main focus being the integration into the unified SMESEC framework.

1.2 Relation to another project work

D3.4 “SMESEC products integration on the Unified Architecture” covers the product extensions developed during Task 3.2. It has interdependencies with:

- D2.1 “SMESEC security characteristics description, security and market analysis report” – this deliverable contains a market analysis where the main security requirements were prioritized and proposed as potential extensions for the SMESEC products.
- D2.2 “SMESEC security products unification report” provides a technical understanding of the existing security products and states the basic principles for innovation.
- D3.2 “SMESEC Unified Architecture – First Internal Release” describes the unified architecture as a whole, while the current extensions focus on the efforts of the tool providers on the unification.

1.3 Structure of the document

The document is divided in 5 chapters, as follows:

Chapter 1 introduces the reader to the deliverable.

Chapter 2 follows the report from D2.1 and lists the main innovation areas and our proposed extensions.

Chapter 3 describes the details of the implemented extensions and innovations for each partner.

Chapter 4 discusses the market benefits brought by the innovations.

Chapter 5 provides the document conclusions.

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	8 of 66	
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status: Final

2 Innovation Areas and Market Requirements

2.1 Overview

The market analysis and the insights obtained from the pilots motivated the SMESEC consortium to innovate and to improve each product. In Task 3.2, each partner worked on several extensions, serving different purposes:

- Integration with other partner tools.
- Integration in the SMESEC framework.
- Improve existing security capabilities.
- Add new capabilities and cover new market sub segments.

The goal of WP3 is to develop the SMESEC framework and the main efforts of T3.2 were directed towards this goal. Some efforts were also directed for improving the individual features of the SMESEC tools.

We have divided the product extensions into collaborative and individual extensions. A collaborative extension is an extension for a specific SMESEC tool that was created in collaboration with other partners or for integration purposes. An individual extension improves the security capabilities of an individual tool and is not necessarily related to other SMESEC products.

2.2 Lessons learned from the market requirement analysis

The security market analysis was performed in D2.1, also some product extensions were proposed in the same deliverable.

Multiple market segments were analyzed, along with the competition products.

The following market segments were considered relevant for SMEs:

- Encryption.
- Governance, Risk Management and Compliance.
- Data Loss Prevention.
- Unified Threat Management.
- Security Information and Event Management.
- Intrusion Detection and Prevention Systems.
- Distributed Denial-of-Service mitigation.
- Business Continuity / Disaster recovery.
- Web Application Firewall.
- Endpoint Security.
- Application Security Testing.
- Security Awareness and Training.

There were also considered some emerging market segments:

- Deception technology.
- Endpoint Detection and Response.
- Cloud Access Security Brokers.

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	9 of 66	
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status: Final

- User Entity Behavior Analytics.
- Identity and Access Management.

While the SMESEC products already cover a wide spectrum of market segments, there are still new potential areas we can extend. The SMESEC architecture, designed in this work package allows extending SMESEC to different market segments.

2.3 Proposed extensions summary

Partner	ID	Short description	Working months	Other involved partners
ATOS	ATOS.PE01	Extension of indicators to cover cybersecurity threats and attacks for SMEs	M16-M18	-
ATOS	ATOS.PE02	Adaptation of XL-SIEM to IoT domain	M14-M18	-
Bitdefender	BD.PE01	Integration of Bitdefender GravityZone with ATOS XL-SIEM	M16-M18	ATOS
Bitdefender	BD.PE02	Improved ransomware protection	M13-M15	
Bitdefender	BD.PE03	Outdated software detection	M13-M16	
CITRIX	CITRIX.PE01	Extend Citrix Web App Firewall deployment mode to cloud, using the as-a-service mode	M24	
CITRIX	CITRIX.PE02	Integration of Citrix Web App Firewall with ATOS XL-SIEM	M16-M18	
CITRIX	CITRIX.PE03	Extend Citrix Unified Gateway deployment mode to the cloud, using the as-a-service mode	M24	
CITRIX	CITRIX.PE04	Integration of Citrix Unified Gateway with ATOS XL-SIEM	M16-M18	
CITRIX	CITRIX.PE05	Secure Web Gateway - Anti-malware protection	M16-M18	
CITRIX	CITRIX.PE06	Secure Web Gateway – Anti-bot protection	M16-M18	
CITRIX	CITRIX.PE07	Secure Web Gateway - Spam, malware, content filtering	M16-M18	

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	10 of 66
Reference:	D3.4	Dissemination:	PU	Version:	1.1
				Status:	Final

Partner	ID	Short description	Working months	Other involved partners
CITRIX	CITRIX.PE08	Extend Citrix Secure Web Gateway deployment mode to the cloud, using the as-a-service mode	M24	
CITRIX	CITRIX.PE09	Integration of Citrix Secure Web Gateway with ATOS XL-SIEM	M16-M18	
EGM	EGM.PE01	Integrate the keycloak to the TAAS	M7-M18	ATOS
EGM	EGM.PE02	Add the TAAS service to the SMESEC Framework Mockup	M7-M18	ATOS
EGM	EGM.PE03	Adapt the TAAS frontend component to the SMESEC requirements (change the callback management process).	M7-M18	
EGM	EGM.PE04	Outsource the user database (to the Keycloak server)	M7-M18	
FORTH	FORTH.PE01	Interconnection with other tools. Send or receive information and logs from other tools in the project.	M18	ATOS, CITRIX
FORTH	FORTH.PE06	Incorporate the single sign on technology. Use SSO technologies to access all the tools uniformly, using the same credentials and interface.	M22	ATOS, BD, CITRIX, FHNW
FORTH	FORTH.PE09	Correlate the events generated by DDOS tool with other tools in order to provide a homomorphic information to the system administrator.	M24	ATOS, BD, CITRIX, FHNW
FORTH	FORTH.PE01	Prioritize and send alerts to users	done-deprecated	
FORTH	FORTH.PE02	Defense of web and applications on the Cloud. Developing a research toolset that is able to detect inter-VM attacks for cloud-based applications	M24	

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	11 of 66
Reference:	D3.4	Dissemination:	PU	Version:	1.1
				Status:	Final

Partner	ID	Short description	Working months	Other involved partners
FORTH	FORTH.PE03	GPU for pattern matching. Converting a highly recognized research work, developed in FORTH, to a tool that can assist all pattern matching components of EWIS and cloud-based IDS system.	M24	
FORTH	FORTH.PE07	DDoS tool to be integrated into the EWIS system. Incorporate the functionality and the logs generated by the DDoS tool into the existing EWIS solution.	M18	
FORTH	FORTH.PE08	Incorporate more SME-oriented honeypot solutions. Configure, incorporated and focus on honeypots related to SMEs' needs.	M24	
FHNW	FHNW.PE01	Policy management: support commonly used policy templates	Dropped/integrated into the new SME-friendly approach	
FHNW	FHNW.PE02	Risk management: risk register	Dropped/integrated into the new SME-friendly approach	
FHNW	FHNW.PE03	Risk management: support for risk frameworks	Dropped/integrated into the new SME-friendly approach	
FHNW	FHNW.PE04	Risk management: Key Risk Indicator (KRI) library	Dropped/integrated into the new SME-friendly approach	
FHNW	FHNW.PE05b	Risk management: risk assessment questionnaires, implemented by the new SME coach concept	M18	
FHNW	FHNW.PE06b	Audit management: risk-based scoping, implemented by the new SME coach concept	M18	
FHNW	FHNW.PE07	Audit management: workpaper management	Dropped/integrated into the new SME-friendly approach	

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	12 of 66
Reference:	D3.4	Dissemination:	PU	Version:	1.1
				Status:	Final

Partner	ID	Short description	Working months	Other involved partners
FHNW	FHNW.PE08	Audit calendar management.	M30	
FHNW	FHNW.PE09	Threat and vulnerability management: integration with 3 rd party tools (patch management, vulnerability assessment) through an API definition with SMESEC partners' tools	M18	
FHNW	FHNW.PE10	Incidence management: data aggregation from multiple sources (SIEM, DLP, service desk) and business impact assessment (capability-specific KPIs recorded by the user or offered by integrated tools).	M24	
FHNW	FHNW.PE11	Platform capabilities: federated architecture	M24	
FHNW	FHNW.PE12	Platform capabilities: custom, role-based dashboards	M24 (questioned but not dropped)	
FHNW	FHNW.PE13	Platform capabilities: multilingual features to support local language	New, M30	

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	13 of 66
Reference:	D3.4	Dissemination:	PU	Version:	1.1
				Status:	Final

3 Product extensions

3.1 ATOS extensions

3.1.1 IoT Extension for XL-SIEM

IoT devices are a key market right now. They are used for a great diversity of tasks ranging from smart cities (e.g. detection of levels of contamination, number of vehicles going through a road, etc.) to agri-food (e.g. controlling temperature of the soil, heat, etc.). This way, many organizations use it for their businesses and depend on their security and stability. In that sense, a breach in the devices have a critical impact in both their financial and reputational aspects.

The tools provided by SMESEC aim to support SMEs in their day-to-day business covering their cybersecurity needs. One of the main risks of IoT is the lack of control of devices in uncontrolled/unknown environments. For this reason, the use of the XL-SIEM was seen as a very positive functionality as it could be used to monitor the security and safety of deployed devices. Still, one of the issues was from the technical point of view as the current specifications of the agents used for monitoring were not fitting for the technical capacities/requirements of the systems. The XL-SIEM agent provides several built-in capabilities for network and host vulnerability detection, using open source tools like OpenVAS or Suricata. Although this information is very valuable, the tools used for compiling it are usually resource consuming, representing a problem for its usage in IoT devices.

In order to achieve lower memory and disk footprints for the agent that makes it capable of being installed on IoT devices, we reworked several capabilities and reduce processing capabilities, keeping only the necessary functionality to communicate with the server and listening to the configured logs.

Therefore, the modifications of the agents were done to facilitate their deployment and use in IoT devices focusing in their limited capacity and performance. In order to achieve this, we analyzed the technical requirements of the IoT devices of the industrial use case of the project and worked with them for needs, expected behavior/functionality, etc. Following, we worked in reducing size of the agents and processing needs in order to reduce requirements. Then, we tested it with virtual machines of the devices using its specific characteristics for evaluating its performance and functionality. Some of the technical characteristics of the device are described in table below.

Type	Gateway Kerlink Wirnet Station 868
OS	Kernel 3.10.37-3.10.37-klk4, compiled for armv5tejl
Volatile memory	Low power DDRAM 128MB 10MB used for system firmware
Non-volatile memory	128MB NAND flash 40MB used for system firmware and autorecovery mechanism
Free space	150MB approximately

The work done in this task covers the needs of these devices, but we plan to continue refining the agents for supporting more types of devices and their needs. We plan to do this by evaluating other devices of the project coming from the use cases or SMEs of the open call.

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	14 of 66		
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status:	Final

This extension will help SMEs by allowing them to deploy more easily and effectively agents in their IoT devices. This way, they will be able to monitor the correct functionality and the safety of their data and systems. Additionally, we are working in facilitating the deployment and installation as much as possible by creating specific versions according to the different types of hardware and/or software. In its initial deployment with the WoS use case this new enhanced version of the agent has proved more useful than the normal one. We are still working in performance indicators, testing and in-depth evaluation but the experience so far is positive and useful.

Regarding the technical development, we have worked in reducing capabilities of various components of the agent. As we can see in Figure 1 the agent is composed of different components and communication agents that receive the information of monitoring of several applications, compile the information and send it to the server of the XL-SIEM for further processing. The work of this extension consisted in reducing the functionality of the agent by minimizing some of the inputs or the type of monitoring done in the system. Regarding the figure, the ones in blue are the components left in the lightweight version and the ones in gray the modified ones for reducing size and processing. More specifically, and as an example, we worked in the following components:

VAS Vulnerability Scanner: The VAS Vulnerability Scanner relies in an existing OpenVAS installation in the machine where the agent runs. In IoT devices, usually restricted in both memory and disk, the installation of this software is very resource consuming and, as we do not support this service in SMESEC we think it was a good option to make it optional. As a result, this functionality is not installed by default in the agent.

NMap: The XL-SIEM agent uses NMap¹ to scan the ports of the machine in which is installed, creating reports for the user about services installed in those ports, which ports are opened, etc. Although this information can be useful in some IoT devices, the technical needs of the instance of NMap installed on the device make it difficult to support low consumption IoT components. Finally, although the on-premises installation is no longer by default supported in the agent, being now optional, many of the information provided by the application can also be retrieved with NMap using an instance in an external machine. Therefore, this feature is removed in this version of the agent, liberating valuable resources.

WMI support: Windows Management Instrumentation (WMI²) is a Microsoft Windows technology for consolidating the management of devices and application in a network using Windows computing systems. Although in the latest version of Windows Core IoT³ it is supported WMI, the XL-SIEM agent does not support Windows systems yet. Therefore, we have decided to disable this capability and make it available for future versions if a need for Windows-compatible IoT devices is needed.

Unused parsers: The XL-SIEM agent contains parsers for obtaining the information from several different data sources. These sources include FTP, Snort⁴, SDEE, WMI, databases, local and remote log files, etc. In the IoT version of the agent only local and remote files parsing is allowed since the rest of them are not used in the IoT devices targeted by the agent or, as in the case of Snort, requires additional software to be installed. Therefore, we set as optional these parsers and will be available only when the IoT device where the agent run needs them.

¹ NMap. <https://nmap.org/>. Last visited on November 16th, 2018.

² WMI. <https://docs.microsoft.com/en-us/windows/desktop/wmisdk/wmi-start-page>. Last visited on November 16th, 2018.

³ Windows Core IoT. <https://developer.microsoft.com/en-us/windows/iot>. Last visited on November 26th

⁴ Snort. <https://www.snort.org/>. Last visited on November 16th, 2018.

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	15 of 66	
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status: Final

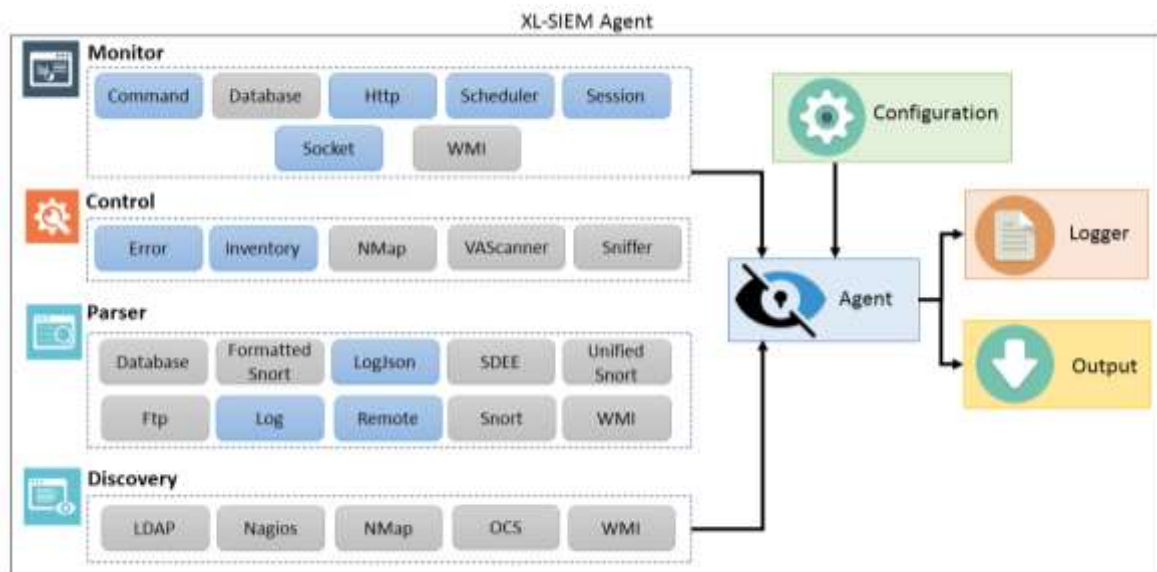


Figure 1: High-level description of XL-SIEM agent

The removal of those features makes the agent consume less memory and start faster, although the improvement is not enough to make it work in very small devices. As abovementioned, we used as basis the technical constraints of the industrial use case, but we plan to continue studying how we could improve the technical constraints and performance of the agents in IoT devices.

Another approach to make the agent lightweight is to provide a minimal set of plugins according to the specific needs of each target system/scenario. In the XL-SIEM agent, each activated plugin creates a new thread, increasing the memory footprint. In a typical installation, with 23 plugins activated, the agent consumes over 300 megabytes of memory, as can be seen in Figure 2

```
VmPeak: 327880 kB
VmSize: 325824 kB
```

Figure 2: Memory consumed by XL-SIEM agent

This memory measure is counting only the XL-SIEM agent process, without taking into account the required third-party software needed to run some of the plugins, as the beforehand mentioned software like Snort, OpenVAS, NMap, and others like Suricata, that can make the complete installation of the XL-SIEM agent consume more than 2 gigabytes of memory, making it completely useless on most of the IoT devices.

With that in mind, and given that IoT devices have several different purposes, we have decided to define the XL-SIEM IoT agent as a lightweight client that uses by default only the minimum set of plugins for communicating with the XL-SIEM, creating tailored ones for the use cases.

We performed several tests using this new IoT-oriented agent and the results have demonstrated to lower the memory footprints to approximately 60MB (being approximately 300MB the previous size), with no extra software required to be installed, making it able to run in many different IoT devices. This decrease of the memory usage is documented in Figure 3.

Document name:	D3.4 SMESEC products integration on the Unified Architecture	Page:	16 of 66
Reference:	D3.4	Dissemination:	PU
Version:	1.1	Status:	Final


```
VmPeak: 61312 kB
VmSize: 61312 kB
```

Figure 3: Memory consumed by XL-SIEM IoT agent

Another critical issue, together with size, in IoT devices is disk usage, especially when working with logs. IoT devices have usually a very reduced disk capacity and a high generation of logs could saturate the system, making it non-usable. Although the XL-SIEM agent can read and parse remote logs, giving the possibility to install it outside the IoT device, we have recognized that this approach is not possible in every situation and it needs a secure and trusted connection and environment. Nevertheless, there are cases in which regulations or business rules states that the company must keep the logs for some specific time. In order to reduce this issue of disk usage we have included in our infrastructure for the XL-SIEM the usage of Logrotate⁵ policies, including information for tweaking the Logrotate configuration. Using this application, the management of logs in the devices is easier, as it can be configured to compile logs in a specific time for reducing size, send them to by email, deleting them using some constraints, etc. Also, for cases that have severe limits on disk usage, the configuration can be changed to keep the minimal possible logs.

3.1.2 Risk Assessment Engine - Indicators for SMEs about cybersecurity threats and attacks

As described in the DoW we plan to integrate and use in SMESEC a Risk Assessment Engine (RAE) solution that evaluates, in near real-time, the risk that is faced by a company. This risk is calculated by executing a set of machine-readable risk assessment algorithms that analyze and compute the financial data of the organization and the cybersecurity status of the system. In order to perform this evaluation two different inputs are necessary from the target system:

- Financial data of the organization is provided by the employees of the organization using a series of questionnaires in order to transform high-level information to machine readable. The information compiled this way is the financial aspects of the business services, ICT components, etc. For example, it asks for the financial cost impact of losing a functionality of the business service or data storage system
- The cybersecurity information of the status can be provided by any monitoring tool deployed in the system. In our case, we use the XL-SIEM, also integrated in SMESEC, for providing this data. The integration of both components is done at data level using a specific communication channel and log formatting, specially designed for obtaining the precise information of the system.

Additionally, besides evaluating the risks it can propose mitigation measures.

In order to calculate the risk, the Risk Assessment Engine defines and uses different types of indicators retrieved from third party applications along with the assets that a company has. These indicators include business, vulnerabilities, network monitoring and application monitoring characteristics. They are aggregated and analyzed in the risk assessment algorithms, based on R⁶ and DEXi⁷ models. The assets

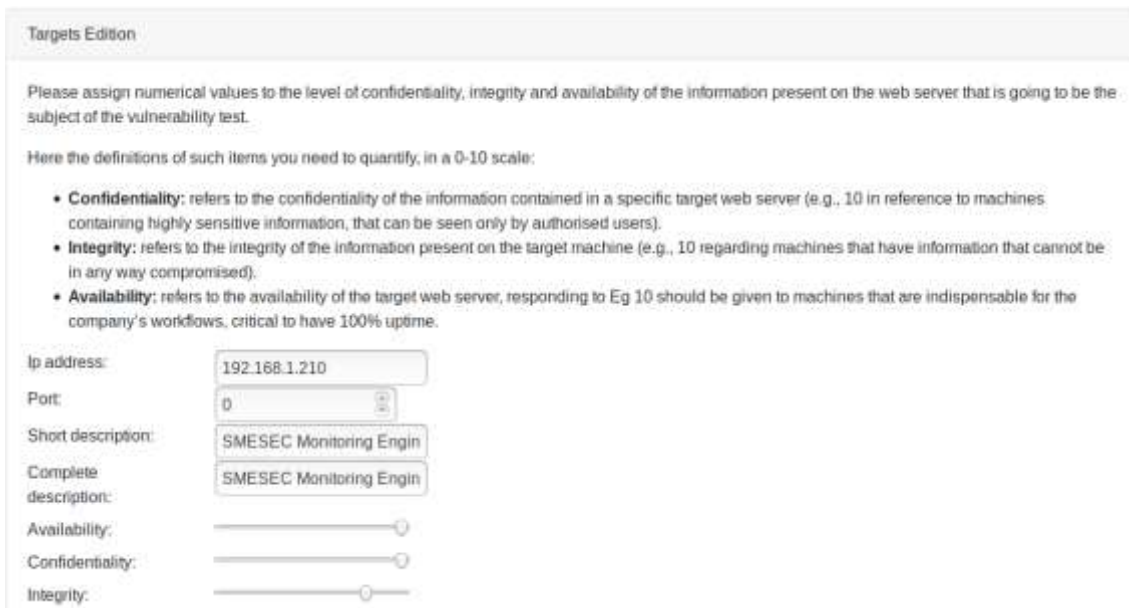
⁵ Logrotate. <https://linux.die.net/man/8/logrotate>. Last visited on November 16th, 2018.

⁶ The R Project for Statistical Computing. <https://www.r-project.org/>. Last visited on November 27th

⁷ DEXi: A program for multi-attribute decision making. <https://kt.ijs.si/MarkoBohanec/dexi.html>. Last visited on November 27th

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	17 of 66		
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status:	Final

of the company must be introduced in the interface of the Risk Assessment Engine, filling the fields as shown in the following Figure 4 and Figure 5.



Targets Edition

Please assign numerical values to the level of confidentiality, integrity and availability of the information present on the web server that is going to be the subject of the vulnerability test.

Here the definitions of such items you need to quantify, in a 0-10 scale:

- **Confidentiality:** refers to the confidentiality of the information contained in a specific target web server (e.g., 10 in reference to machines containing highly sensitive information, that can be seen only by authorised users).
- **Integrity:** refers to the integrity of the information present on the target machine (e.g., 10 regarding machines that have information that cannot be in any way compromised).
- **Availability:** refers to the availability of the target web server, responding to Eg 10 should be given to machines that are indispensable for the company's workflows, critical to have 100% uptime.

Ip address:

Port:

Short description:

Complete description:

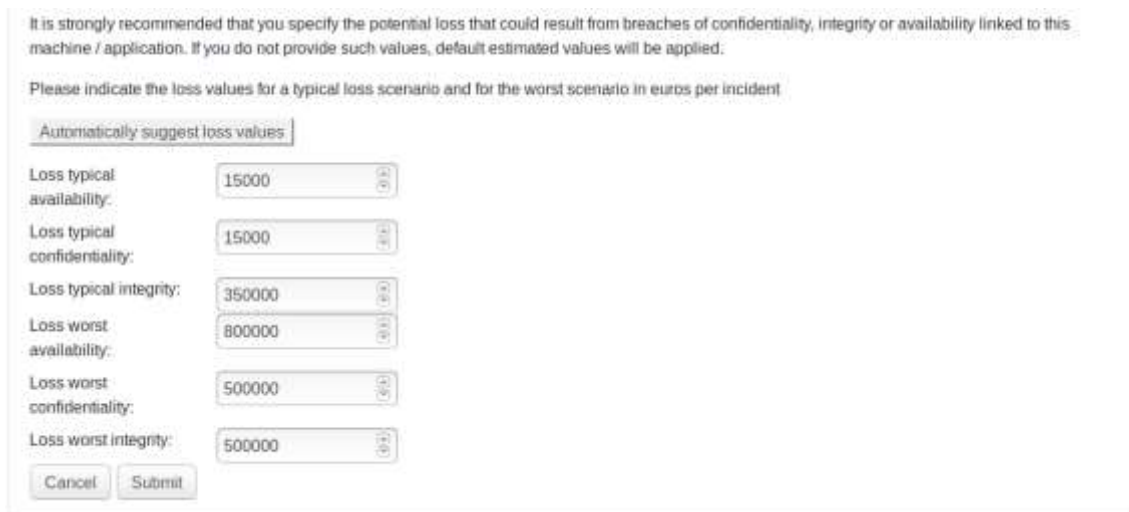
Availability:

Confidentiality:

Integrity:

Figure 4: Adding a target in Risk Assessment Engine (I)

As stated in the Risk Assessment Engine web interface, there is a strong recommendation to provide the values of potential losses. Although the system can apply default values based on availability, confidentiality and integrity values provided by the user, they won't be accurate since the system does not know the business details.



It is strongly recommended that you specify the potential loss that could result from breaches of confidentiality, integrity or availability linked to this machine / application. If you do not provide such values, default estimated values will be applied.

Please indicate the loss values for a typical loss scenario and for the worst scenario in euros per incident

Automatically suggest loss values

Loss typical availability:

Loss typical confidentiality:

Loss typical integrity:

Loss worst availability:


Loss worst confidentiality:

Loss worst integrity:

Figure 5: Adding a target in Risk Assessment Engine (II)

Once the user inserts all the assets of the company in the web interface, the Risk Assessment Engine shows all of them, as shown in Figure 6.

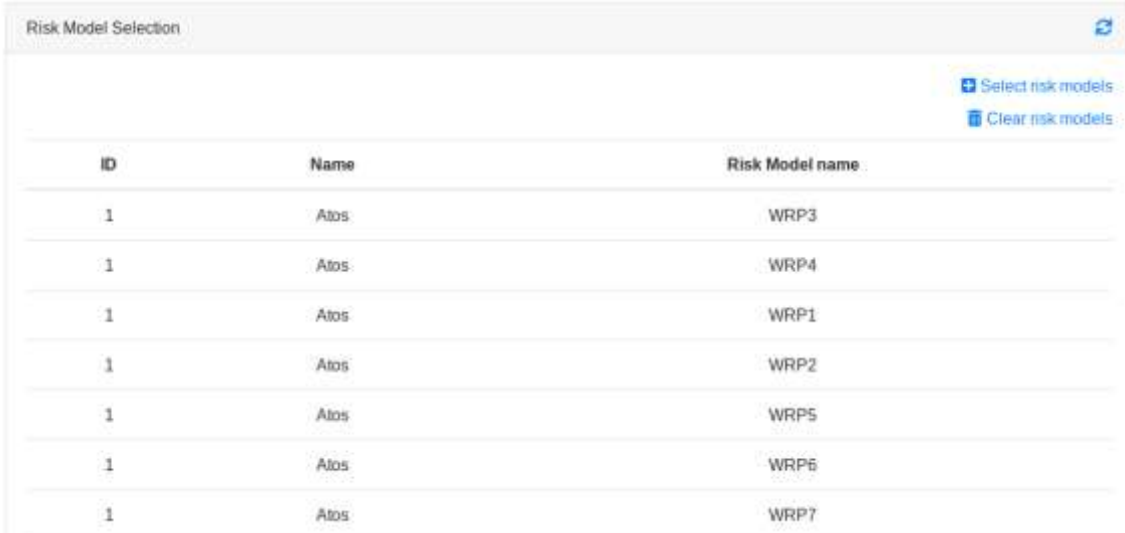
Document name:	D3.4 SMESEC products integration on the Unified Architecture	Page:	18 of 66	
Reference:	D3.4	Dissemination:	PU	
	Version:	1.1	Status:	Final



ID	Ip Address	Port	Short Description	Complete Description	Availability	Confidentiality	Integrity
71	192.168.1.210		SMESEC Monitoring Engine	SMESEC Monitoring Engine VM	10	10	8
74	0.0.0.0		Atos	Infrastructure as a whole	6	9	7
82	192.168.3.65		Test Machine	Test Machine	10	10	10

Figure 6: Assets in Risk Assessment Engine

Then, the user needs to select which of the existing risk models are valid for the assets of the company. This is also done in the web interface of the Risk Assessment Engine, as presented in Figure 7.



ID	Name	Risk Model name
1	Atos	WRP3
1	Atos	WRP4
1	Atos	WRP1
1	Atos	WRP2
1	Atos	WRP5
1	Atos	WRP6
1	Atos	WRP7

Figure 7: Selecting Models in Risk Assessment Engine

After these steps, the Risk Assessment Engine performs the analysis. Once it is completed, the Risk Assessment Engine will provide in its web interface two different reports, one for the qualitative results, shown in Figure 8, and another one with quantitative results, as presented in Figure 9. Both figures show incomplete results for clarity.

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	19 of 66		
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status:	Final

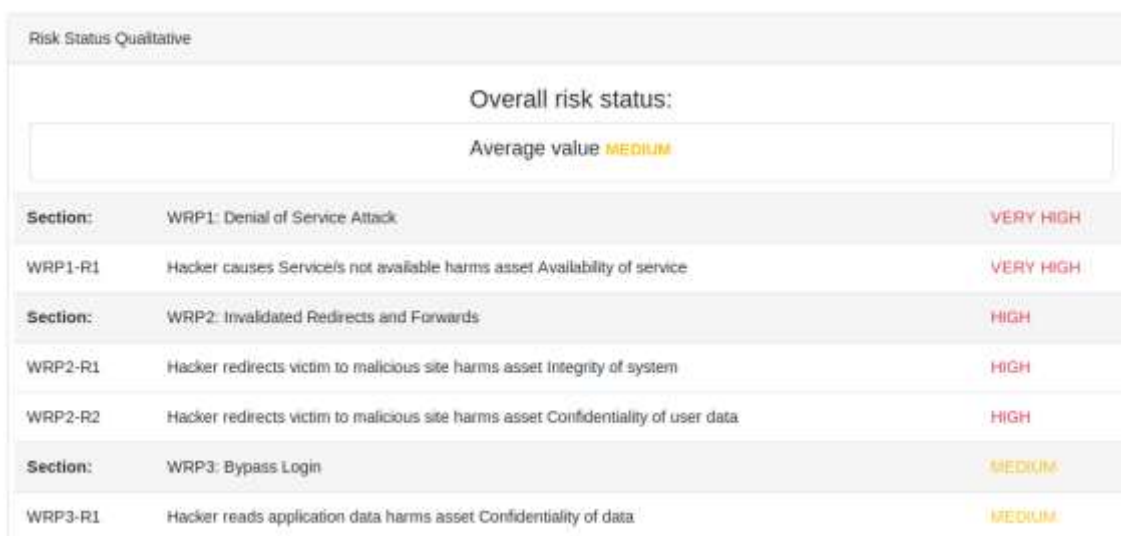


Figure 8: Qualitative Report of Risk Assessment Engine

After the first analysis is done, the Risk Assessment Engine monitors possible changes in the assets and the indicators, running a new analysis every time that detects a change. This way, the Risk Assessment Engine is able to provide information in near real-time about the company's risk.

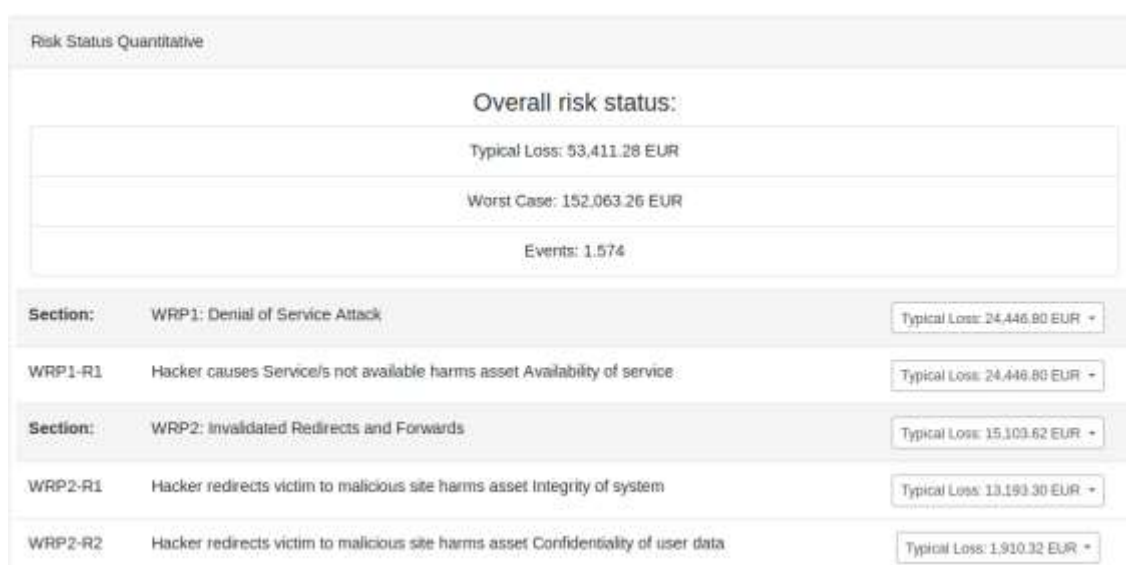


Figure 9: Quantitative Report of Risk Assessment Engine

Although these existing indicators cover many cybersecurity threats and scenarios they were designated specially for large organizations with characteristics very different from SMEs (or, at least, the assumptions used for their design and development) such as having cybersecurity expert employees, complex digital services and devices, other cybersecurity tools in the system, organized training in the organization, cybersecurity and privacy policies, etc. Therefore, we are currently working in SME-oriented indicators that cover all the specific needs and constraints of this type of organizations. We have had meetings with all the use case partners in order to analyze their requirements and what type of information is of more value to them. Thanks to this we are working in identifying the integrity of the

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	20 of 66		
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status:	Final

system (together with recommendations), availability of the different services, integrity of the services (for example physical constraints of the IoT devices used), etc. Finally, the information about risks detected will be sent to the Security Operations Centre, enhancing its functionality. We plan to evaluate these new indicators with the use cases and provide a list of updates and performance in the following deliverable of the framework, showing it together with the integration in the SMESEC Framework.

3.2 BD extensions

3.2.1 Integration of Bitdefender GravityZone with ATOS XL-SIEM

Bitdefender GravityZone is the anti-malware tool from the SMESEC framework. It has multiple endpoint protection tools, for various platforms (Windows, Linux, mobile, etc.). These Endpoint Security tools protect each device they are deployed on but can be also seen as agents collecting insights from those devices. These insights are sent to the GravityZone Control Center, using a proprietary protocol.

Deliverable 2.1 described, as part of the market analysis, the importance of Security Information and Events Management. The XL-SIEM, as part of the consortium tools was identified as appropriate for fulfilling this role. The extension BD.PE01 was implemented in order to make available the information collected by GravityZone to the XL-SIEM.

After an in-depth analysis of what type of information GravityZone can send, and what information can be used by XL-SIEM, we selected the following events types to be sent:

- Malware detection.
- Behavioural scanning.
- Disable behavioral scanning module.
- Phishing and fraud detection.
- Traffic blocked by firewall.
- Port scanning detected by firewall.
- Application control.
- Web control.
- Data protection.
- Authentication audit.
- Overloaded security server.

For each event, a JSON document is created and sent to XL-SIEM using the syslog protocol. This document contains actionable intelligence, collected by GravityZone, usually from the Endpoint Security agents. For instance, each event contains a computer name and IP, so the attack can be located by the system administrator. Some events contain specific information. For instance, a malware detection event will contain the malware name, the detected file path and the action performed by the Endpoint Security.

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	21 of 66	
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status: Final

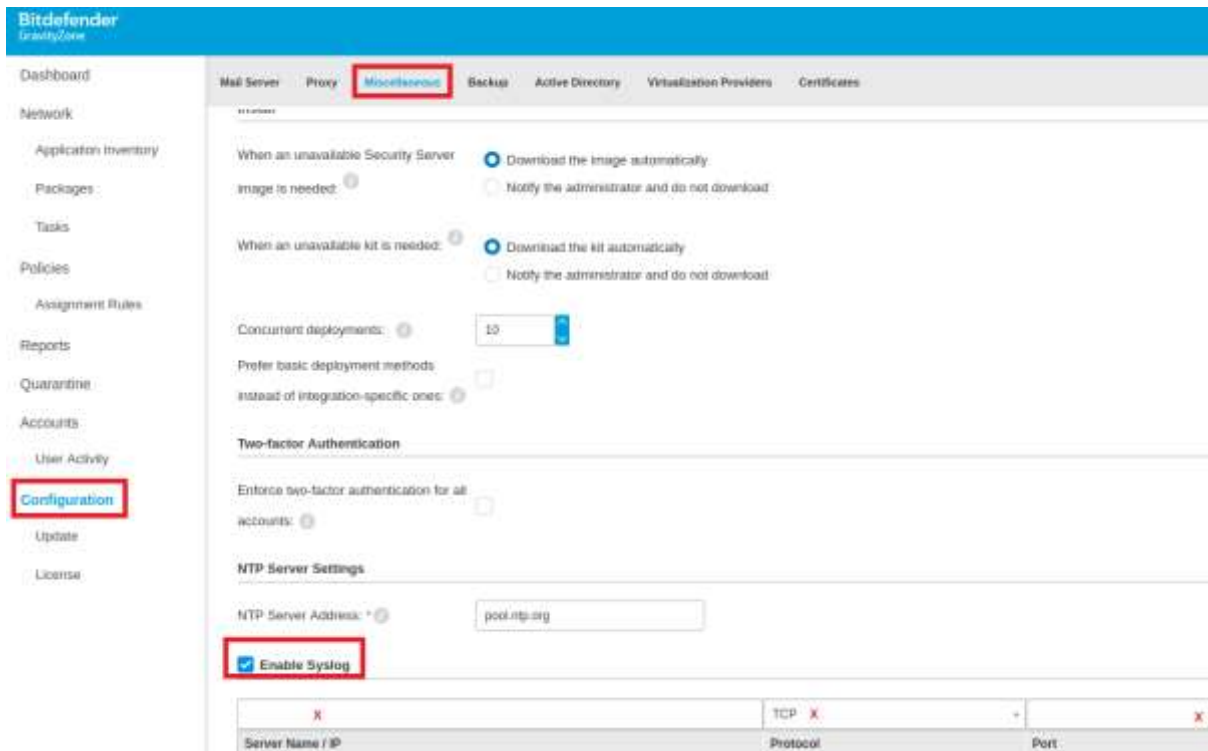


Figure 10: GravityZone configuration for syslog events

Figure 10 shows the configurations required to enable the syslog events and to set the syslog server. The user must click “Configuration” on the left menu, then “Miscellaneous” on the upper menu. The “Enable Syslog” should be checked, and the Server Name, Protocol (TCP or UDP) and Port should be filled.

To control which events are getting sent, the user must click on the notification settings (upper right corner) in order to open the Notification settings dialog box. Each desired notification should be selected and the “Log to syslog server” option should be checked, as in Figure 11.

Enable notifications

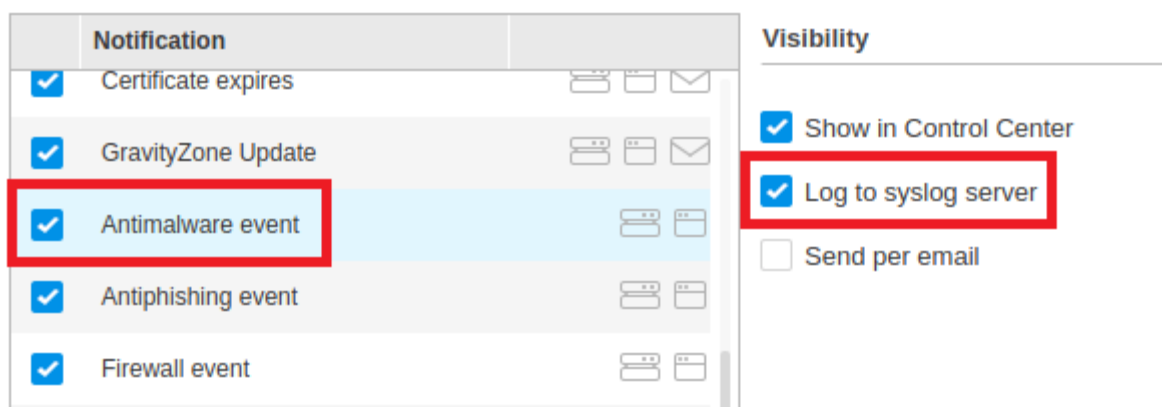


Figure 11: Enabling syslog notifications

Document name:	D3.4 SMESEC products integration on the Unified Architecture	Page:	22 of 66
Reference:	D3.4	Dissemination:	PU
	Version:	1.1	Status: Final

The integration has been tested by several pilots.

There are at least two benefits for SMEs enabled by this extension. First of all, the important security insights obtained by GravityZone will be displayed in the XL-SIEM dashboard, along with events collected from other tools. It will be easier for the system administrator, even if he isn't a security expert to monitor the security of the network, as a whole. Secondly, events correlated from multiple sources may enable the XL-SIEM to provide better security overall.

3.2.2 Improved ransomware protection

As the anti-malware component of the SMESEC framework, GravityZone should protect against all kinds of malware threats. A particular worrisome type of malware is ransomware, a type of malware that restricts the SME's access to some of the computer's resources or even the whole system in order to extort money. There are two main ransomware categories, the screen lockers and the file encryptors. Recent years have shown an increase in the number of ransomware attacks, like CTB-Locker, Locky, Petya and TeslaCrypt.

There are three areas where Bitdefender protects against ransomware:

- Prevention.
- Early detection.
- Remediation.

The prevention stage involves training machine learning models on millions of existing ransomware samples, in order to learn common features and be able to detect 0-day samples. Bitdefender also protects against exploits, a common attack vector in ransomware infections. A particular innovative approach, that was started before Task 3.2 but was refined in this period is the anti-ransomware vaccine. This method is based on the fact that most ransomware won't infect a system twice, by looking for some specific markers. The Bitdefender team analyzed these markers and added them to the protected systems, thus preventing real infections.

The early detection is another technique that was improved, by monitoring running processes, files and registry keys modifications. Monitoring these entities will allow the anti-malware tool to detect encryption actions in the early phase and to block them and roll back the changes.

The remediation actions involve termination of the ransomware processes and rolling back the file system modifications. Bitdefender Labs also offer free decryption tools for some ransomware families. In order to enable these extensions, no special actions are required from the users. All they need to do is keep the anti-malware up to date.

Protection against ransomware greatly benefits SMEs, as Cybersecurity Ventures predicts that the ransomware cost will reach 11.5 billion USD by 2019. A ransomware data encrypts an SMEs data will disrupt the normal operations and may cause irremediable damage.

3.2.3 Outdated software detection

Outdated software remains the number one cause for exploits, especially for SMEs where, 0-day exploits are not commonly used. It is very important to train the users and system administrators to keep their

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	23 of 66		
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status:	Final

software up to date, but Bitdefender takes a step further by warning the customers about outdated software and even automatically updating some software on its own.

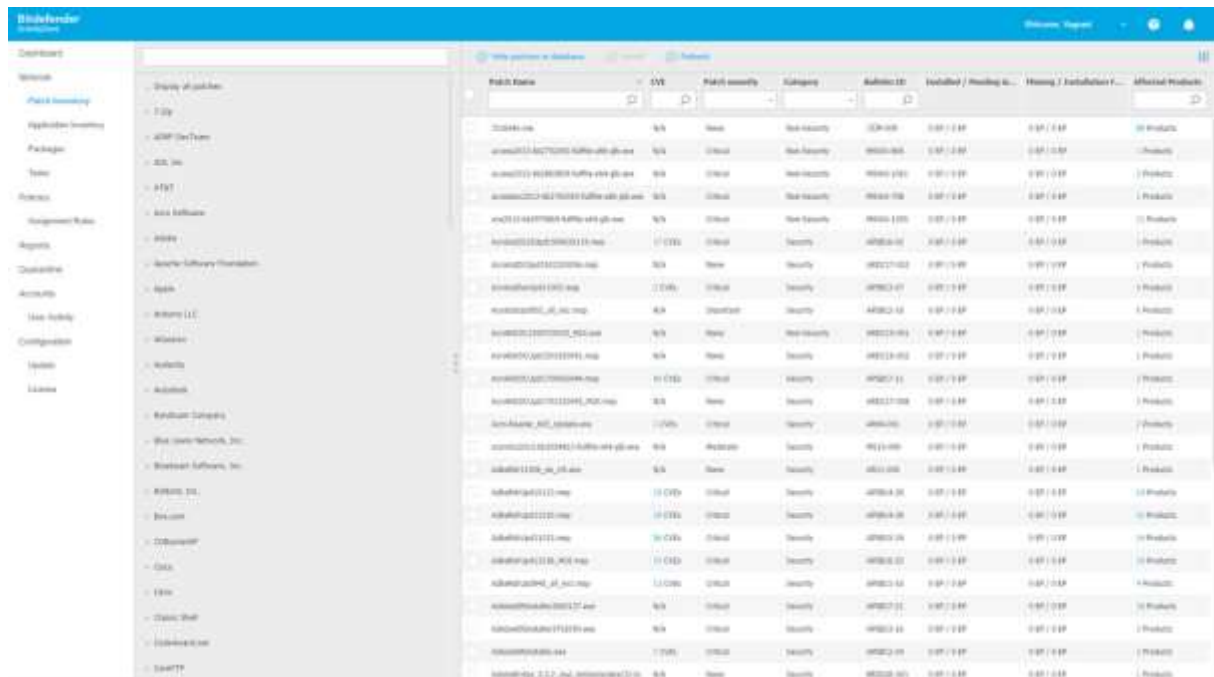


Figure 12: Bitdefender Patch Management

Figure 12 shows the interface for Bitdefender Patch Management, that comes as a plugin for Bitdefender GravityZone.

The main features of Bitdefender Patch Management are:

- Patching for OS and the largest collection of software applications.
- Automatic and manual patching.
- Detailed information centering patches - CVE, Bulletin ID, Patch Severity, Patch Category.
- Ability to set different schedules for security and non-security patches.
- Quick deployment of missing patches.
- The ability to distribute patches from the relay, reducing network traffic.
- Patch specific reports that help companies demonstrate compliance.
- Automatically notify IT administrator when security/non-security patches are missing.

3.3 CITRIX extensions

Citrix ADC (formerly NetScaler ADC) is an application delivery controller that performs application-specific traffic analysis to intelligently distribute, optimize, and secure Layer 4-Layer 7 (L4 - L7) network traffic for web applications, provides flexible delivery services for traditional, containerized and microservice applications and delivers enhanced cybersecurity features. Its feature set consists of switching features, security and protection features, and server-farm optimization features.

Document name:	D3.4 SMESEC products integration on the Unified Architecture				Page:	24 of 66
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status: Final

3.3.1 Citrix ADC Platforms and Deployment Options

There are various platforms on which Citrix ADC can be delivered, with the dominant ones being listed in the following paragraphs. It is essential to comprehend that all features of Citrix ADC are enabled on top of these baseline deployments via a dedicated licensing scheme which is later initiated.

MPX/SDX (Hardware)

Citrix ADC MPX (hence referred as MPX) is a hardware-based application delivery appliance which delivers stellar performance ranging between 500Mbps and 200Gbps traffic.

MPX is suitable for managing web applications with multiple gigabits of traffic, offering load balancing for small enterprises and ultra-high performance in cybersecurity applications.

Citrix ADC SDX (hence referred as SDX) is a hardware-based appliance with enhanced virtualization capabilities enabled-out-of-the-box towards consolidating up to 115 independently-managed Citrix ADC instances. SDX is suitable for consolidating multiple physical load balancers, provide flexible multi-tenancy and is clearly targeted to service providers which require fully isolated tenants. The integrated isolation capability it encompasses greatly simplifies application rollouts from staging and development environments.

Citrix ADC VPX (hence referred as VPX) is a software-based virtual appliance running on widely deployed hypervisors such as KVM, Xen, Hyper-V and ESXi. VPX is a perfect match for architecting hybrid cloud infrastructures as well as deliver cloud-native application load balancing for public cloud environments. It was primarily designed to replace hardware-based load balancing solutions and deploy the majority of Citrix ADC features using the as-a-Service paradigm, in order to accommodate use cases related to actions in development, testing and production environments. VPX is suitable for architecting scalable, multi-tenant infrastructures and offers several attractive application delivery options for telco, enterprises and small businesses.

Citrix ADC CPX (hence referred as CPX) is a Docker containerized load balancer that can be supported on-premise and in multi-cloud environments. CPX is suitable for supporting containerized applications and provide developers and DevOps teams with a robust load balancing solution early in the development cycle. A single CPX instance deployed in a Docker host provides throughput of up to 1 Gbps thus facilitating migration to a microservices architecture. In addition, CPX allows to deliver exceptional application performance with multi-core CPX as an ingress device to handle North-South traffic for popular cluster orchestrators such as Kubernetes. CPX Express, a free developer version of CPX supports up to 20Mbps traffic and 250SSL connections and can be downloaded from <https://www.citrix.com/products/citrix-adc/cpx-express.html#download>.

As mentioned, Citrix ADC is available in both VM (aka VPX) and Docker container forms (aka CPX). However, only VPX supports the full set of capabilities. VPX images are available for KVM, XenServer, VMware (ESX) and Hyper-V, a dedicated version of the product can also be deployed in AWS environment.

It should be stated here that any Citrix ADC software image contains all the following features (and more) – however, they are activated by different licensing scheme, each available for a different premium:

- SSL/TLS termination and web server load balancing.
- I&AM (in conjunction with relevant AAA backends).

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	25 of 66		
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status:	Final

- Web Application Firewall (aka Citrix Web App Firewall).
- VPN Gateway (aka Citrix Unified Gateway).
- Secure Web Gateway (aka Citrix Secure Web Gateway).

Additional information about the licensing can be found in a following section of this document.

For managing a fleet of Citrix ADC nodes and support certain advanced reporting functions, an additional node needs to be deployed, the NetScaler Management & Analytics System (NetScaler MAS). However, such advanced functionality is probably out of scope for any SMESEC use case.

For accommodating use cases where high availability is required, two Citrix ADC instances can be deployed as a synchronized HA pair.

3.3.2 Features at a Glance

Citrix ADC features can be configured independently or in combinations to address specific needs. Although some features fit more than one category, the numerous Citrix ADC features can generally be categorized as application switching and traffic management features, application acceleration features, and application security and firewall features, and an application visibility feature.

3.3.2.1 Denial of service (DoS) attack defense

Detects and stops malicious distributed denial-of-service (DDoS) attacks and other types of malicious attacks before they reach your servers, preventing them from affecting network and application performance. The Citrix ADC appliance identifies legitimate clients and elevates their priority, leaving suspect clients unable to consume a disproportionate percentage of resources and cripple your site. The appliance provides application-level protection from the following types of malicious attacks:

- SYN flood attacks.
- Pipeline attacks.
- Teardrop attacks.
- Land attacks.
- Fraggle attacks.
- Zombie connection attacks.

The appliance aggressively defends against these types of attacks by preventing the allocation of server resources for these connections. This insulates servers from the overwhelming flood of packets associated with these events.

The appliance also protects network resources from ICMP based attacks by using ICMP rate limiting and aggressive ICMP packet inspection. It performs strong IP reassembly, drops a variety of suspicious and malformed packets, and applies Access Control Lists (ACLs) to site traffic for further protection.

3.3.2.2 Content Filtering

Provides protection from malicious attacks for web sites at the Layer 7 level. The appliance inspects each incoming request according to user-configured rules based on HTTP headers and performs the action the user configured. Actions can include resetting the connection, dropping the request, or sending

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	26 of 66		
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status:	Final

an error message to the user's browser. This allows the appliance to screen unwanted requests and reduces your servers' exposure to attacks.

This feature can also analyze HTTP GET and POST requests and filter out known bad signatures, allowing it to defend your servers against HTTP-based attacks.

3.3.2.3 Responder

Functions like an advanced filter and can be used to generate responses from the appliance to the client. Some common uses of this feature are generation of redirect responses, user defined responses, and resets.

3.3.2.4 Rewrite

Modifies HTTP headers and body text. It is possible to use the rewrite feature to add HTTP headers to an HTTP request or response, make modifications to individual HTTP headers, or delete HTTP headers. It also enables users to modify the HTTP body in requests and responses.

When the appliance receives a request, or issues a response, it checks for rewrite rules, and if applicable rules exist, it applies them to the request or response before passing it on to the web server or client computer.

3.3.2.5 Priority Queuing

Prioritizes user requests to ensure that the most important traffic is serviced first during surges in request volume. It is possible to establish priority based on request URLs, cookies, or a variety of other factors. The appliance places requests in a three-tier queue based on their configured priority, enabling business-critical transactions to flow smoothly even during surges or site attacks.

3.3.2.6 Surge Protection

Regulates the flow of user requests to servers and controls the number of users that can simultaneously access the resources on the servers, queuing any additional requests once servers have reached their full capacity. By controlling the rate at which connections can be established, the appliance blocks surges in requests from being passed on to your servers, thus preventing site overload.

3.3.2.7 Citrix Unified Gateway

Citrix Unified Gateway consolidates remote access infrastructure to provide single sign-on across all applications whether in a datacenter, in a cloud, or delivered as SaaS. It allows people to access any app, from any device, through a single URL. Citrix Unified Gateway is easy to deploy and simple to administer. The most typical deployment configuration is to locate the Citrix Unified Gateway appliance inside the so called DMZ. It is possible to install multiple Citrix Unified Gateway appliances in the network for more complex deployments. More information regarding the Citrix Unified Gateway and its suitability for SMESEC can be found in a following section of this deliverable.

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	27 of 66		
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status:	Final

3.3.2.8 Web Application Firewall

Citrix Web App Firewall protects applications from misuse by hackers and malware, such as cross site scripting attacks, buffer overflow attacks, SQL injection attacks, and forceful browsing, by filtering traffic between each protected web server and users that connect to any web site on that web server. The application firewall examines all traffic for evidence of attacks on web server security or misuse of web server resources and takes the appropriate action to prevent these attacks from succeeding. More information regarding the Citrix Web App Firewall and its utilization in SMESEC can be found in a following section of this deliverable.

3.3.3 Citrix ADC extensions for seamless SMESEC framework integration

In D2.1 the following potential extensions have been identified:

Citrix Web App Firewall (former NetScaler AppFirewall)

ID	Category	Potential extension
CITRIX.PE01	Deployment Options	Deploy to cloud in as-a-service mode
CITRIX.PE02	Integrations	Integration with SIEM

Citrix Unified Gateway (former NetScaler Gateway)

ID	Category	Potential extension
CITRIX.PE03	Deployment Options	Deploy to cloud in as-a-service mode
CITRIX.PE04	Integrations	Integration with SIEM

NetScaler Secure Web Gateway

ID	Category	Potential extension
CITRIX.PE05	Threat protection	Anti-malware protection
CITRIX.PE06	Threat protection	Anti-bot protection
CITRIX.PE07	Email security	Spam, malware, content filtering
CITRIX.PE08	Deployment Options	Deploy to cloud in as-a-service mode
CITRIX.PE09	Integrations	Integration with SIEM

3.3.3.1 Cloud Deployment of Citrix ADC

For addressing CITRIX.PE01, CITRIX.PE03 and CITRIX.PE08 extensions identified in D2.1, Citrix enabled the deployment of Citrix Web Application Firewall, Citrix Unified Gateway and Citrix Secure Web Gateway services in the cloud, by integrating all their distinct characteristics into the overall Citrix ADC bundle and enable them via proper licensing. This approach allows each service to become available in the cloud once a Citrix ADC instance is properly deployed and configured.

Citrix ADC in its VPX flavour is available as an Amazon Machine Image (AMI) in AWS marketplace and enables customers to leverage AWS Cloud computing capabilities and use Citrix ADC load

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	28 of 66		
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status:	Final

balancing and traffic management features for their business needs. In addition, for enabling deployment over on-premise, cloud infrastructure, Citrix offers a dedicated package of Citrix ADC in QCOW2 format. Such images can be deployed in Openstack or native KVM virtualization environments thus enabling all necessary features inside a privately-owned datacenter. Citrix ADC on AWS supports all the traffic management features of a physical Citrix ADC appliance. Citrix ADC instances running in AWS can be deployed as standalone instances or in HA pairs.

The Citrix ADC VPX AMI is packaged as an EC2 instance that is launched within an AWS VPC. The VPX AMI instance requires a minimum of 2 virtual CPUs and 2 GB of memory. An EC2 instance launched within an AWS VPC can also provide the multiple interfaces, multiple IP addresses per interface, and public and private IP addresses needed for VPX configuration. Currently, on Amazon AWS, VPX can be launched only within a VPC, because each VPX instance requires at least three IP addresses. (Although VPX on AWS can be implemented with one or two elastic network interfaces, Citrix recommends three network interfaces for a standard VPX on AWS installation). AWS currently makes multi-IP functionality available only to instances running within an AWS VPC. A VPX instance in a VPC can be used amongst others to load balance servers running in EC2 instances.

Figure 13 illustrates a typical VPX on AWS deployment. The AWS VPC has (i) a single internet gateway to route traffic in and out of the VPC; (ii) established network connectivity between the internet gateway and the internet; (iii) three different subnets, each for management, client and server; (iv) network connectivity between the internet gateway and the two subnets (management and client); (v) a single Citrix ADC VPX deployed within the VPC. In addition, the VPX instance has three Elastic Network Interfaces (ENIs) marked in yellow, one attached to each subnet.

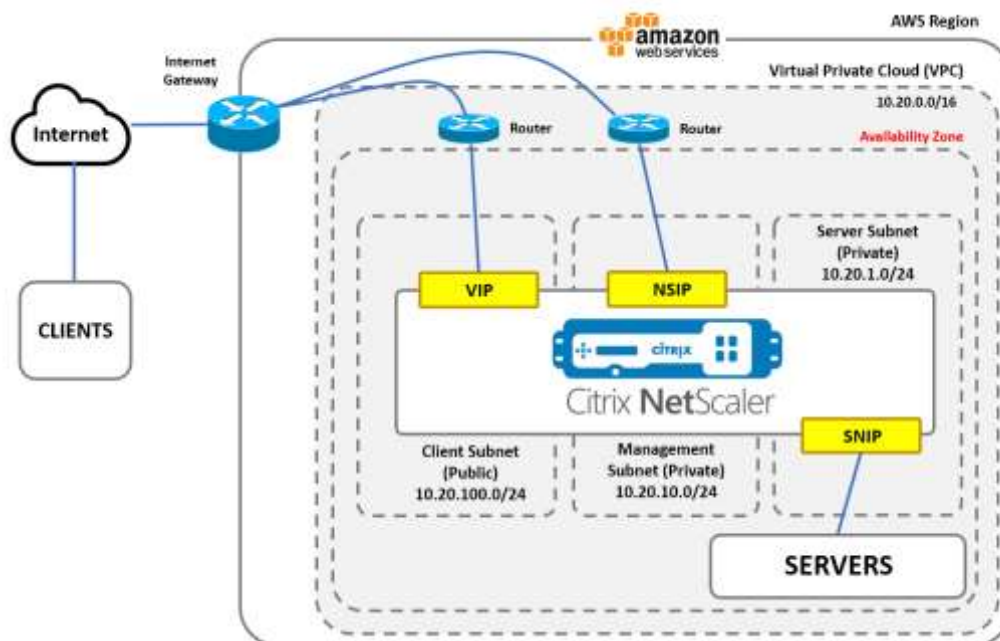


Figure 13: Typical VPX in AWS deployment

It is possible to deploy a Citrix ADC VPX standalone instance on AWS using three options:

(i) AWS web console; (ii) Citrix-authored CloudFormation template; (iii) the AWS CLI. Under the auspices of SMESEC, VPX will be deployed in AWS using the AWS web console only, a process described in the following steps.

Document name:	D3.4 SMESEC products integration on the Unified Architecture	Page:	29 of 66	
Reference:	D3.4	Dissemination:	PU	
	Version:	1.1	Status:	Final

It should be stated here that to ensure the optimal functionality of every Citrix ADC VPX instance, the node must be co-located with the servers it protects, as shown in the previous Figure. If this requirement is not met, potential service quality degradation must be expected.

3.3.3.2 Citrix Web App Firewall (former NetScaler AppFirewall)

As already described in SMESEC Deliverable D3.1 “System Design”, Section 6.1.3, Citrix Web App Firewall is a Web Application Firewall solution which protects web applications and sites from common and contemporary malicious attacks, including every application-layer and zero-day threats.

Citrix Web App Firewall introduces deep-packet inspection of HTTP, HTTPS and XML, as well as protection against OWASP Top 10. The overall protection features it supports includes (i) countermeasures against SQL injection and cross-site scripting attacks along with cookie tampering, (ii) HTTP and XML reply and request format validation and more generic form validation and protection schemes (iii) JSON payload inspection, (iv) signature and behaviour-based protection together with protection from Denial of Service , (v) support for data loss prevention (DLP), authentication, authorization and auditing paired with advanced reporting capabilities. The service can analyze traffic in the upper layers of the OSI model, as illustrated in Figure 14.

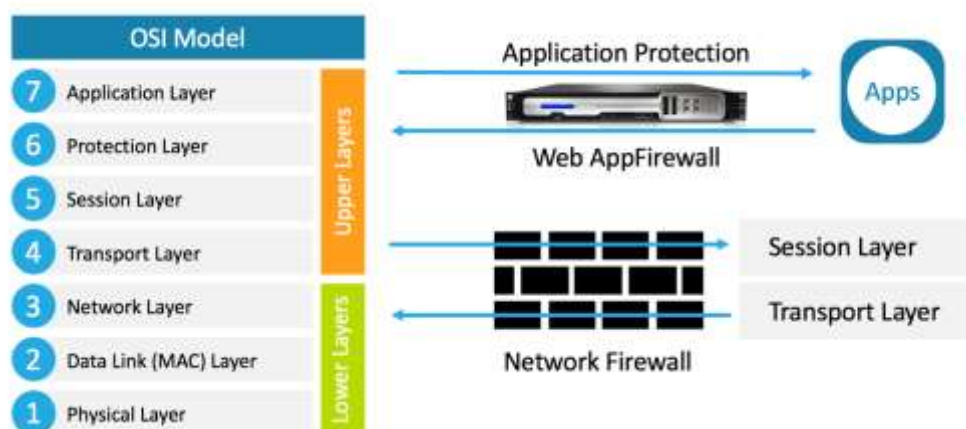


Figure 14: Citrix ADC AppFirewall

The Citrix Web App Firewall offers easy to configure options to meet a wide range of application security requirements. Web App Firewall profiles, which consist of sets of security checks, can be used to protect both the requests and the responses by providing deep packet-level inspections. Each profile includes an option to select basic protections or advanced protections. Some protections might require use of other files.

The profiles can also use other files, such as signatures or error objects. These files can be added locally, or they can be imported ahead of time and saved on the appliance for future use. They can be shared by multiple profiles.

Profiles work in conjunction with the Web App Firewall policies. Each policy identifies a type of traffic, and that traffic is inspected for the security check violations specified in the profile that is associated with the policy. The policies can have different bind points, which determine the scope of the policy. For example, a policy that is bound to a specific virtual server is invoked and evaluated for only the

Document name:	D3.4 SMESEC products integration on the Unified Architecture	Page:	30 of 66
Reference:	D3.4	Dissemination:	PU
	Version:	1.1	Status: Final

traffic flowing through that virtual server. The policies are evaluated in the order of their designated priorities, and the first one that matches the request or response is applied.

For allowing proper feature integration of the Citrix Web Application Firewall with the SIEM module of SMESEC, as described in CITRIX.PE02, it is important to increase the underlying Citrix ADC log level and obtain the necessary messages using the universally acclaimed SYSLOG format. This integration is currently under test.

3.3.3.3 Citrix Unified Gateway (former NetScaler Gateway)

As mentioned in SMESEC Deliverable D3.1 “System Design”, Section 6.1.4, Citrix Unified Gateway consolidates remote access infrastructure to provide single sign-on (SSO) across all applications regardless if they reside in a data center, in a cloud, or delivered using the SaaS paradigm. This feature allows users to access any app, from any device, through a single URL. Some additional features of Unified Gateway include but are not limited to multi-factor authentication, end-to-end monitoring across all application traffic and contextual access control across on-premise VDI, web, cloud and SaaS applications. In a nutshell, the service helps reduce costs, simplify management, and significantly improve the overall user experience. Figure 15 illustrates the variety of devices able to access all available destination applications through Citrix Unified Gateway.

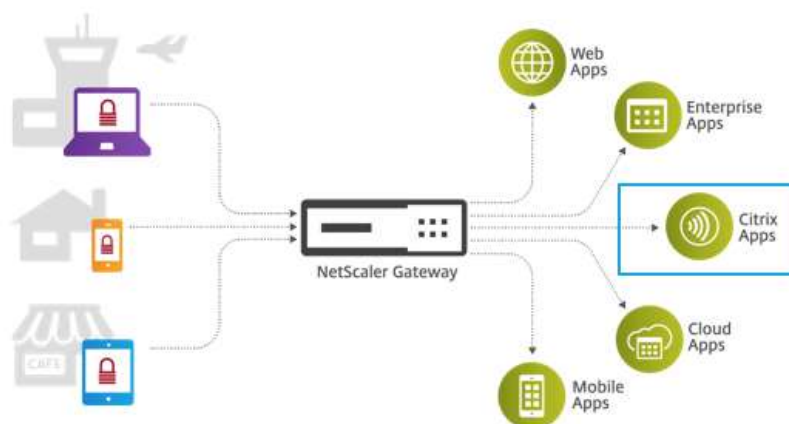


Figure 15: Citrix Unified Gateway

Similar to the Citrix Web Application Firewall, for allowing proper feature integration of Citrix Unified Gateway the with the SIEM module of SMESEC, as described in CITRIX.PE04, it is important to increase the underlying Citrix ADC log level and obtain the necessary messages using the universally acclaimed SYSLOG format. This integration is currently under test.

Document name:	D3.4 SMESEC products integration on the Unified Architecture	Page:	31 of 66
Reference:	D3.4	Dissemination:	PU
	Version:	1.1	Status: Final

3.3.3.4 Citrix Secure Web Gateway

Encryption, without a doubt, protects the privacy and integrity of data. However, there are cases where it also creates blind spots that attackers can exploit to evade security controls. Since over half of all internet traffic today is encrypted, there is a rather large security gap that exposes businesses and increases vulnerability and risk. As mentioned in SMESEC Deliverable D3.1 “System Design”, Section 6.1.5, Citrix Secure Web Gateway (SWG) enforces company security and compliance policies and gets insights into user behaviour through an advanced SSL decryption mechanism. This process cost-effectively eliminates blind spots in the business environment and strengthens the security posture. SWG uses a cloud-based service paired with a local cache to check for URL reputation and category. It addresses zero-day attacks up to 10 times faster than other forward proxies that need to download a full or partial database. Through this, enforces company security policies on all outgoing web traffic, while blocking access to inappropriate sites on a per user/group basis. Figure 16 illustrates the positioning of SWG in the network, along with an overview of the services it supports.

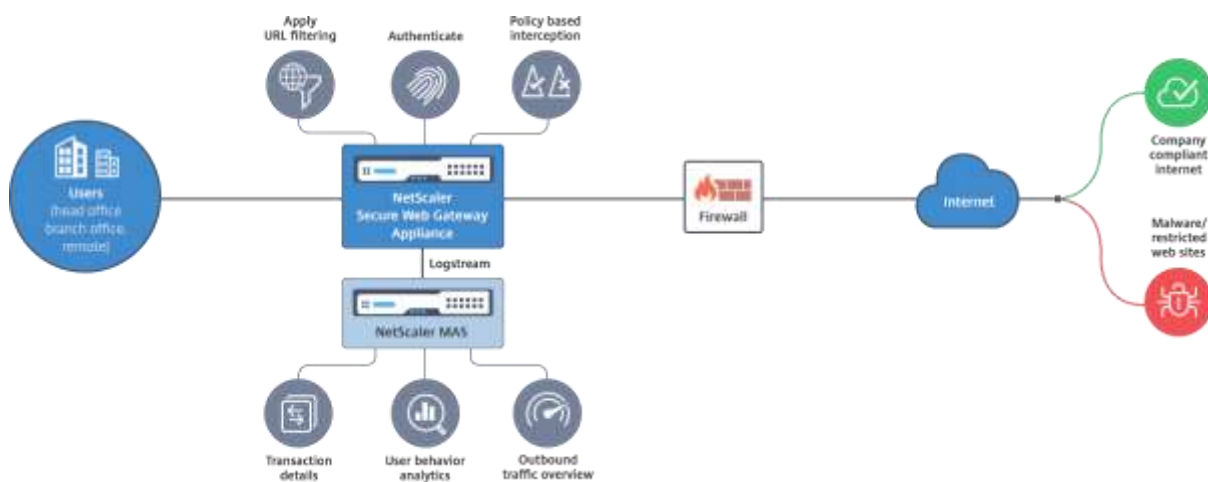


Figure 16: Citrix NetScaler Secure Web Gateway

Traffic flows through the enterprise network from the head office, branch offices, data center, and remote employees. A Citrix ADC appliance at the edge of the network acts a proxy. The appliance can operate in transparent proxy mode or explicit proxy mode and offers controls to intercept internet traffic, including HTTPS. Policies configured on the appliance determine whether it intercepts, bypasses, or blocks a particular request. Access to restricted sites can be blocked by using URL filtering, thus partially satisfying CITRIX.PE05, CITRIX.PE06 and CITRIX.PE07. A user is authenticated before logging on to the enterprise network. All requests and responses are tagged to identify the user, and internet-site access is categorized. User activity is logged and used to generate reports. If a breach occurs, administrators can isolate the infected system, determine whether the devices of any other users who visited that web site are compromised, and take appropriate action. When you integrate the NetScaler Management and Analytics System (MAS) with a Citrix SWG appliance, the logged user activity and the subsequent records in the appliance are exported to NetScaler MAS by using log stream. NetScaler MAS collates and presents information about the activities of users, from websites visited to the time spent online. It also provides information about bandwidth use and detected threats, such as malware and phishing sites. These key metrics can be used for network monitoring and consequently engage

Document name:	D3.4 SMESEC products integration on the Unified Architecture	Page:	32 of 66
Reference:	D3.4	Dissemination:	PU
	Version:	1.1	Status: Final

Citrix SWG appliance to take corrective actions, once again thus partially satisfying CITRIX.PE05, CITRIX.PE06 and CITRIX.PE07. It should be stated here that a Citrix SWG appliance can be physical or virtual (deployed in VPX flavour).

In a nutshell, Citrix SWG enables IT directors to

- Gain visibility into the otherwise bypassed secure traffic.
- Block access to malicious or unknown sites and avoid infecting users within the enterprise.
- Control access to some websites, such as personal mail, social networking, and job search websites, from the enterprise network.

Apply intelligent content control policies to ensure maximum user productivity.

SSL interception in SWG

A Citrix Secure Web Gateway (SWG) appliance configured for SSL interception acts as a proxy. It can intercept and decrypt SSL/TLS traffic to inspect the unencrypted request and enable a company to enforce compliance rules and security checks, thus partially satisfying elements and requirements related with CITRIX.PE05, CITRIX.PE06 and CITRIX.PE07. SSL Interception uses a policy that specifies which traffic to intercept, block, or allow. For example, traffic to and from financial web sites, such as banks, must not be intercepted, but other traffic can be intercepted, and blacklisted sites can be identified and blocked. Citrix recommends that configuring one generic policy to intercept traffic and more specific policies to bypass some traffic.

The client and the Citrix SWG proxy establish an HTTPS/TLS handshake. The SWG proxy establishes another HTTPS/TLS handshake with the server and receives the server certificate. The proxy verifies the server certificate on behalf of the client, and also checks the validity of the server certificate by using Online Certificate Status Protocol (OCSP). It regenerates the server certificate, signs it by using the key of the CA certificate installed on the appliance and presents it to the client. Therefore, one certificate is used between the client and the Citrix ADC appliance, and another certificate between the appliance and the back-end server.

For intercepted HTTPS traffic, the SWG proxy server decrypts the outbound traffic, accesses the clear text HTTP request, and can use any Layer 7 application to process the traffic, such as by looking into the plain text URL and allowing or blocking access on the basis of the corporate policy and URL reputation. If the policy decision is to allow access to the origin server, the proxy server forwards the re-encrypted request to the destination service (on the origin server). The proxy decrypts the response from the origin server, accesses the clear text HTTP response, and optionally applies any policies to the response. The proxy then re-encrypts the response and forwards it to the client. If the policy decision is to block the request to the origin server, the proxy can send an error response, such as HTTP 403, to the client.

To perform SSL interception, in addition to the proxy server configured earlier, the following features must be configured in SWG appliance:

- SSL profile
- SSL policy
- CA certificate store
- SSL-error autolearning and caching

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	33 of 66		
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status:	Final

3.4 EGM extensions

The goal of TaaS (Test as a Service) is extend the SMESEC framework capabilities to verify and validate the potentiality of different vulnerabilities related to oneM2M and LoRa security requirements. Our motivation to add this extension is to meet the market requirements related to sensors and IoT platforms domain listed in D2.1 in section 2.5. For instance, we investigate potential security vulnerabilities in LoRa. In particular, we analyze the LoRa network stack and discuss the possible susceptibility of LoRa devices to different types of attacks using commercial-off-the-shelf hardware and try to generate the appropriate security test cases. The TaaS enable to SMEs and companies to develop standards based interoperable and secure products with a shorter time-to-market and significantly lowered engineering and financial overhead.

3.4.1 ATOS collaboration

EGM worked with ATOS to integrate the extension into the SMESEC Framework, we have proceeded as the following:

3.4.1.1 Keycloak Integration

Let's list out the points what we would like to achieve for a production ready Keycloak Angular application as the TaaS use Angular as a frontend technology. The full project is available on the gitlab of the project. We collaborate with ATOS to fill keycloak.json (our keycloak configuration file) with ATOS keycloak server configuration and add a link to your keycloak.js file in index.html.

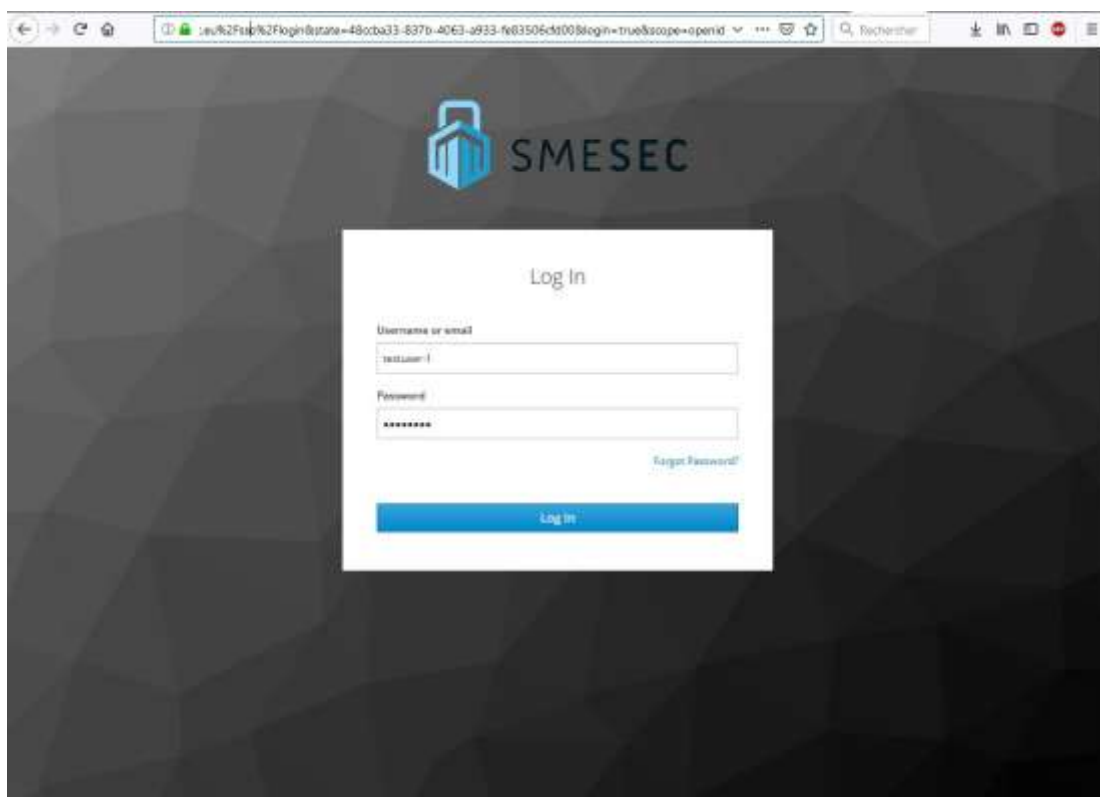


Figure 17: KeyCloak authentication page

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	34 of 66		
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status:	Final

3.4.1.2 TaaS integration:

After the integration of the Keycloak, the service is now ready for the integration into the SMESEC frontend mock-up. For that we collaborated with ATOS to include our index.html main page into a iframe that call our backend services.

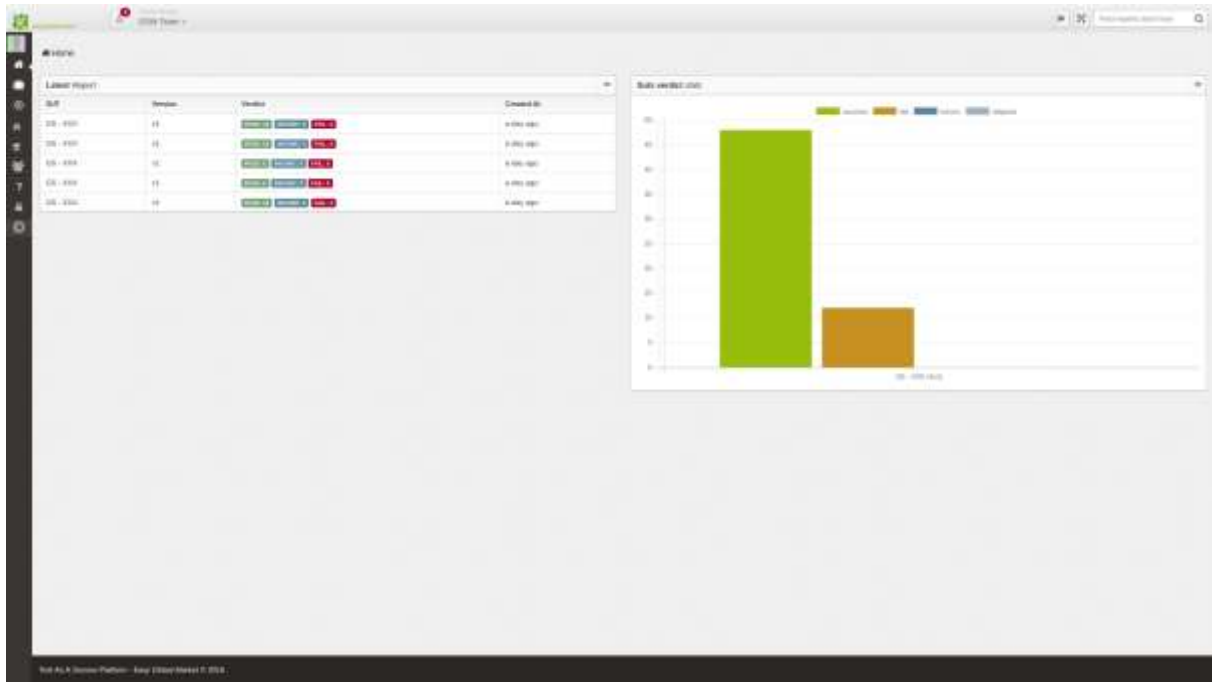


Figure 18: TaaS frontend

To integrate the extension into the SMESEC Framework, we have proceeded as the following:

3.4.2 Keycloak related work

The TaaS use Angular 2 framework (which is based on typescript) as a frontend technology. The keycloak from the other side support only the native javascript, so as a first contribution, we did the typing that will allow “keycloak-js” to be imported as an angular service.

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	35 of 66	
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status: Final

```

declare namespace Keycloak {
  type KeycloakAdapterName = 'cordova' | 'cordova-native' | 'default' | any;
  type KeycloakOnLoad = 'login-required' | 'check-ssso';
  type KeycloakResponseMode = 'query' | 'fragment';
  type KeycloakResponseType = 'code' | 'id_token token' | 'code id_token token';
  type KeycloakFlow = 'standard' | 'implicit' | 'hybrid';

  interface KeycloakInitOptions {
    /**
     * @private Undocumented.
     */
    useNonce?: boolean;

    /**
     * Allows to use different adapter:
     *
     * - {string} default - using browser api for redirects
     * - {string} cordova - using cordova plugins
     * - {function} - allows to provide custom function as adapter.
     */
    adapter?: KeycloakAdapterName;

    /**
     * Specifies an action to do on load.
     */
    onLoad?: KeycloakOnLoad;

    /**
     * Set an initial value for the token.
     */
    token?: string;

    /**
     * Set an initial value for the refresh token.
     */
    refreshToken?: string;
  }
}

```

Figure 19: Keycloak-js interfaces typed on keycloak.d.ts

The second action is configure the Keycloak with the same configuration as the ATOS server.

3.4.3 Architecture related work

One of the SMESEC requirements (see D2.1) is to have a common dataset of users, in this perspective we changed the TaaS architecture to source out our user dataset and handle the user roles based on the keycloak token. The figure bellow shows these changes:

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	36 of 66		
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status:	Final

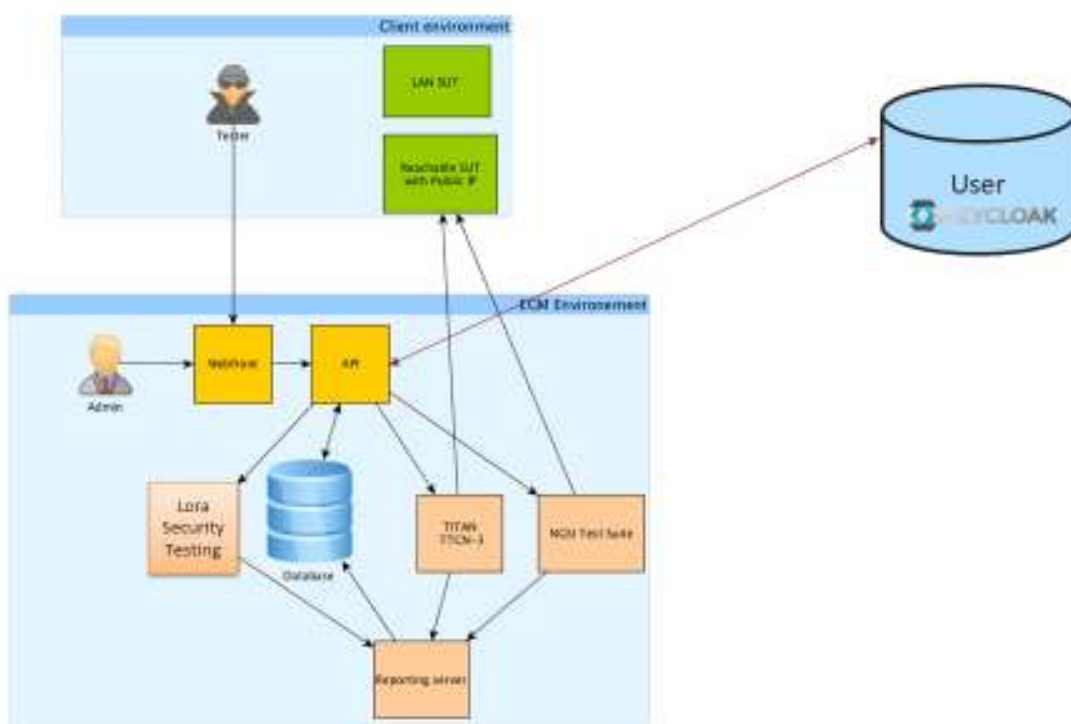


Figure 20: TaaS adapted architecture

3.5 FHNW extensions

In D2.1 the following potential extensions have been identified:

ID	Category	Potential extension
FHNW.PE01	Policy Management	Support commonly used policy templates
FHNW.PE02	Risk Management	Risk register
FHNW.PE03	Risk Management	Support for Risk Frameworks
FHNW.PE04	Risk Management	KRI (Key Risk Indicator) Library
FHNW.PE05	Risk Management	Risk Assessment Questionnaires
FHNW.PE06	Audit Management	Risk-based scoping
FHNW.PE07	Audit Management	Workpaper management
FHNW.PE08	Audit Management	Audit Calendar Management
FHNW.PE09	Threat & Vulnerability Management	Integration with 3 rd party tools (patch management, vulnerability assessment, etc.) through an API definition with SMESEC partners' tools

Document name:	D3.4 SMESEC products integration on the Unified Architecture	Page:	37 of 66
Reference:	D3.4	Dissemination:	PU
	Version:	1.1	Status: Final

FHNW.PE10	Incidence management	Data aggregation from multiple sources (SIEM, DLP, service desk, etc.) Business impact assessment (Both features above, though capability specific KPIs recorded by the user or offered by integrated tools)
FHNW.PE11	Platform capabilities	Federated architecture
FHNW.PE12	Platform capabilities	Custom role-based dashboards

The first chosen approach to implement the CYSFAM framework without adoption has proven to be ineffective and complicated. While being a useful framework for large enterprises, CYSFAM showed to be too complicated for SMEs. As a result, the potential extensions FHNW.PE01, FHNW.PE02, FHNW.PE03, FHNW.PE04 and FHNW.PE07 have been dropped and instead a methodology based on CYSFAM and tailored to the needs of SMEs was developed in collaboration with the University of Utrecht. This updated methodology is being implemented in the FHNW CYSEC tool (see the section about the FHNW individual extension).

The support for Risk assessment questionnaire (FHNW.PE06) has been extended to the concept of an interactive coach providing expert knowledge to SMEs without cybersecurity experts.

Audit Calendar management (FHNW.PE08) is believed to be a valuable extension and is planned to be integrated towards the end of the SMESEC project (current plan: November 2019).

Interfaces for integration of 3rd party tools (FHNW.PE09) are now available through the new design following FHNW.PE06. Although they are not yet used throughout the SMESEC framework, it is still believed to become handy as the framework matures and grows towards FHNW.PE10.

Federated architecture (FHNW.PE11) has shown to be useful to address privacy needs and security concerns regarding the data managed by CYSEC. Local instances of CYSEC will be available to the general public as part of the open call evaluation.

Currently the use of FHNW.PE12 (custom, role-based dashboards) is under discussion and questioned. Analysis showed that customisation possibilities are welcome but add the threat of rendering a system too complicated. While it has not been dropped yet, it is currently questioned.

Furthermore, the following new extension has been added upon feedback from the reviewer from the EU commission:

ID	Category	Potential extension
FHNW.PE13	Platform capabilities	Support multilingual features to support local languages

While this extension makes sense and implementation started, results show that the platform can sustain a multilingual environment. The development of specific cybersecurity coaches has proved to be much more complicated due to the interactivity and the interconnecting nature of a CySeC coach. It is always possible to use multiple unlinked coaches in different languages. However, developing multilingual coaches will remain a challenge.

The following table summarises the current status of the extensions:

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	38 of 66		
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status:	Final

ID	Category	Potential extension	Status
FHNW.PE01	Policy Management	Support commonly used policy templates	Dropped/integrated into the new SME-friendly approach
FHNW.PE02	Risk Management	Risk register	Dropped/integrated into the new SME-friendly approach
FHNW.PE03	Risk Management	Support for Risk Frameworks	Dropped/integrated into the new SME-friendly approach
FHNW.PE04	Risk Management	KRI (Key Risk Indicator) Library	Dropped/integrated into the new SME-friendly approach
FHNW.PE05	Risk Management	Risk Assessment Questionnaires	Implemented by the new SME coach concept (done)
FHNW.PE06	Audit Management	Risk-based scoping	Implemented by the new SME coach concept (done)
FHNW.PE07	Audit Management	Workpaper management	Dropped/integrated into the new SME-like approach
FHNW.PE08	Audit Management	Audit Calendar Management	Planned November 2019
FHNW.PE09	Threat & Vulnerability Management	Integration with 3 rd party tools (patch management, vulnerability assessment, etc.) through an API definition with SMESEC partners' tools	Implemented but not yet in use
FHNW.PE10	Incidence management	Data aggregation from multiple sources (SIEM, DLP, service desk, etc.) Business impact assessment (Both features above, though capability specific KPIs recorded by the user or offered by integrated tools)	Planned but no date available
FHNW.PE11	Platform capabilities	Federated architecture	Under development (Planned June 2019)
FHNW.PE12	Platform capabilities	Custom role-based dashboards	Questioned but not dropped
FHNW.PE13	Platform capabilities	Support multilingual features to support local languages	New; Under development

In addition to the aforementioned extension, the following parts have been contributed by FHNW to the collaborative parts up until now:

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	39 of 66		
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status:	Final

3.5.1 CySeC integrated SAML2 and OAuth2 authentications for a unified framework

To work in a common framework the CySeC tool (developed for SMESEC) had to be able to use external, delegatable authentication so that users do only have to log in once during the use of the SMESEC-Framework (see FHNW.PE09). For this, SAML2 has been integrated into the tool. Unfortunately, the authentication provider chosen for the SMESEC framework (Keycloak) was unable despite the previous analysis unable to provide the necessary features required for a delegated login. We had to switch strategy from the former standard SAML2 to a new standard OAuth providing all the means for a delegated login. Implementation of OAuth is now in the testing phase.

3.5.2 Development of the SMESEC common branding standards

To have a joint branding, FHNW developed a common minimum branding standard. The essence of this branding standard may be found under SMESEC\Templates\Logo in the SMESEC owncloud. The SMESEC common branding standards reflect those recommended for and adopted by the SMESEC.EU webpage.

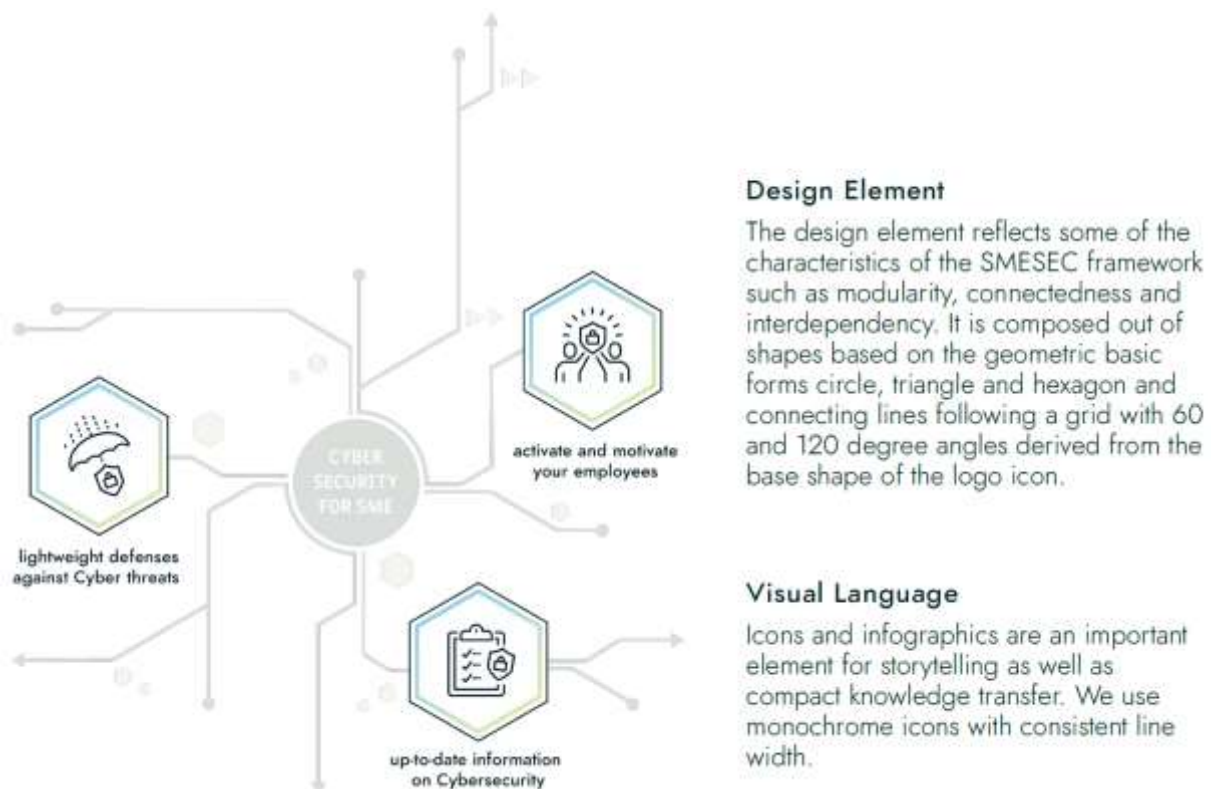


Figure 21: Excerpt from the branding document

Most people find Cyber Security boring, too complicated or just not relevant to them. This attitude makes it necessary to convince users that Cyber Security can be interesting, not too complicated and relevant to everyone. This change in opinion is encouraged by CYSEC with a good user experience (UX) and gamification. The gamification and well-elaborated explanations, which are not too

Document name:	D3.4 SMESEC products integration on the Unified Architecture	Page:	40 of 66	
Reference:	D3.4	Dissemination:	PU	
	Version:	1.1	Status:	Final

complicated (for users without previous knowledge) but also not too easy (for users who already have experience) will avoid that Cyber Security is perceived as boring.

Applications in the area of cybersecurity are often very complicated and very technically designed. In CYSEC, the user interface (UI) is attractively designed and clearly structured. This approach allows the user easy access to the topic and reduces fears. Personalised recommendations, understandable explanations and progress indicators show the user that Cyber Security is relevant for everyone. An additional problem is that to be effective in cybersecurity, you have to stay tuned. Through gamification and personalised recommendations, we motivate the user to continually work on security.

In summary, the main objectives of CYSEC, which are achieved through user experience and gamification, are the following:

- Creating awareness of the dangers of Cyber Security.
- To sensitise and motivate SMEs to cybersecurity topics.
- Provide references to training resources and products (including SMESEC's).
- Help to increase personal security permanently.
- Provide a regularly updated assessment of your security level.

FHNW contributes to the SMESEC framework with the Cybersecurity Coach CYSEC. CYSEC allows the SME end-users to assess their cybersecurity capabilities and improve them according to the SMESEC values of easily do-it-yourself. The FHNW solution consists of a web application that guides the end user (or enterprises) through the process of becoming more secure. The application evaluates answers to questions, offers pointers to training resources and products (including SMESEC ones), and keeping track of the improvement backlog and reminders for helping to achieve the SME's security goals.

This section describes the context and scope of CYSEC and offers an overview of its features, including a description of their design to enable do-it-yourself cybersecurity assessment and improvement.

3.5.3 CYSEC System Context, Users, and Use

CYSEC is used by two types of users, the person responsible for cybersecurity in the SME ("SME Employee") and the reference person for judging the state of SMEs in the cybersecurity community ("Community Reference Person"). CYSEC offers a graphical user interface for the SME employee and a logger that allows the community reference person to analyse a stream of observations as the SME is undertaking capability improvements. CYSEC may be used as a service offered by the SMESEC Cloud or deployed on the SME's premise as a separate stand-alone application.

The following figure describes the deployment scenario, the external interfaces towards other components of the SMESEC framework, and the interfaces offered to users.

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	41 of 66		
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status:	Final

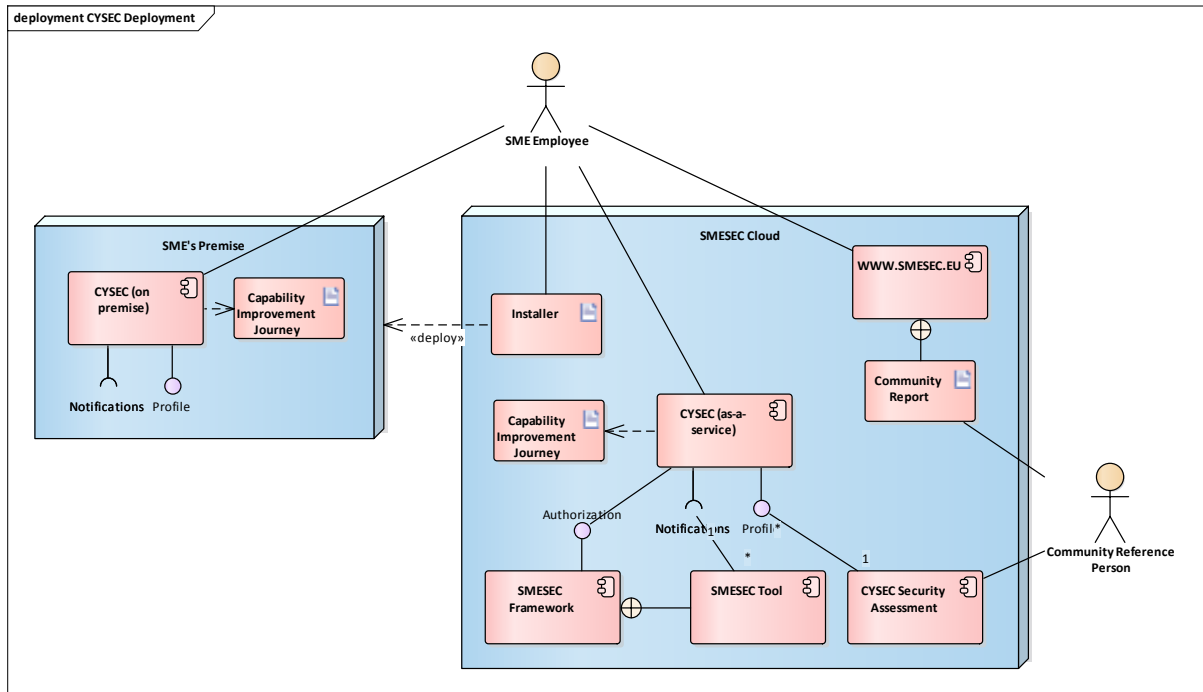


Figure 22: CYSEC deployment scenario and external interfaces towards the users and the SMESEC framework

CYSEC offers interfaces for receiving notifications about cybersecurity-related events from SMESEC tools and for sharing the capability profile and insights about cybersecurity adoption and adherence. SMESEC uses the common interface for user authorisation offered by the SMESEC framework.

An SME employee uses CYSEC along a journey of capability improvement steps. CYSEC offers a capability improvement cockpit that allows the user to choose the journey to work on. To support decision-making, CYSEC recommends the top journeys and provides reminders about capabilities to be worked on. These recommendations are influenced by the end users progress of capability improvement and notifications about cybersecurity-related events captured by the SMESEC tools.

CYSEC serves the user journey for capability improvement with a step-wise series of questions that the user is answering. Within a journey, the first question is the most fundamental easy capability to work on, and with each step, the capabilities become more advanced and challenging to implement. The user always has the possibility to stop working on a journey with the confidence of having made the most fundamental improvements. A sufficiently completed journey is associated with a badge reflecting an endorsement or certification of SMESEC that the capability area is implemented at the level indicated by the badge. Badges correspond to threat types that the SME can effectively address and standards that are fulfilled by the SME's cybersecurity capabilities.

Each question is associated with background information that motivates the question, offers facts about the question's topic and links to further information, tools, videos, and online training. The background information is thus a place to provide awareness and access to education and tools that help the company to build cybersecurity capabilities.

Each question is also associated with a set of answers that reflect how much the cybersecurity capability underlying the question has been implemented. Partial or inexistent implementation is recorded by

Document name:	D3.4 SMESEC products integration on the Unified Architecture	Page:	42 of 66	
Reference:	D3.4	Dissemination:	PU	
	Version:	1.1	Status:	Final

CYSEC and recommendations of actions recommended, including the setting of reminders and contact with members of the SME whose contributions are needed to implement the capability.

The following figure illustrates the interaction between the CYSEC user journey interface with the SME employee’s answering of questions while getting educated and building the company’s cybersecurity capabilities.

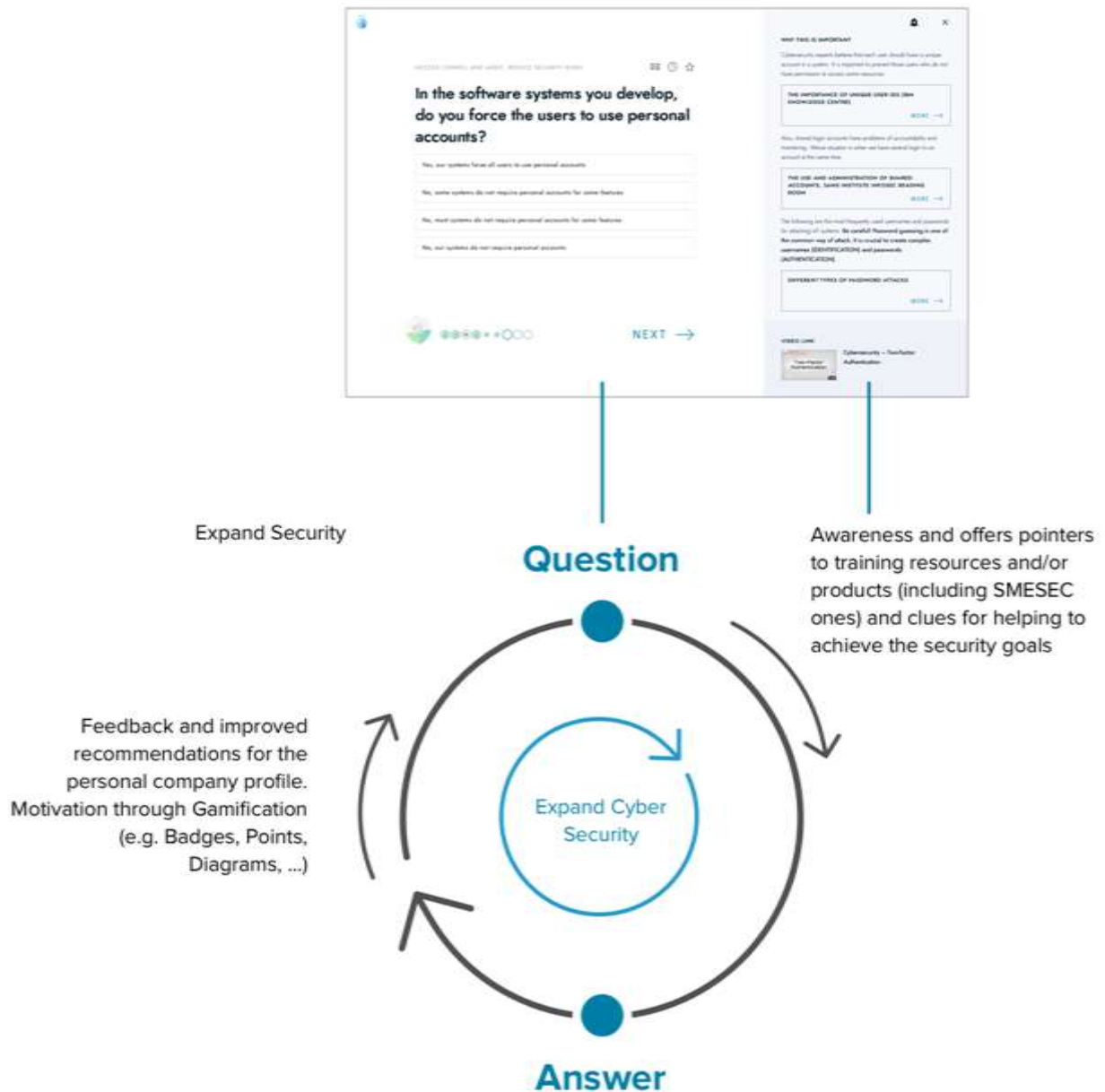


Figure 23: Question-answer loop of assessing SME capabilities and offering awareness of cybersecurity knowledge, end-user training, and SMESEC tool capabilities.

CYSEC is configurable to adapt to different types of SMEs, to markets (incl. language), and to evolve with new capabilities such as cybersecurity knowledge for addressing previously unsupported threats

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	43 of 66	
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status: Final

and artificial intelligence to improve the self-adaption of the coach. It is configured with an XML file that specifies capability improvement journeys, captures the SME's state of following that journey, and captures the behaviour of the cybersecurity coach.

3.5.4 Overview of Features

The following table offers an overview of the CYSEC features that are built as individual extensions of FHNW. Each feature is specified in more detail in the subsequent sub-chapters. The following table gives an overview of the functional features CYSEC.F01-F05.

Table 1: CYSEC features representing FHNW individual extensions.

Feature	Functionality, Benefit, and Implementation
CYSEC.F01 Capability Improvement Dashboard	The capability improvement dashboard gives an overview of capability improvement achievements and improvement recommendations for all supported cybersecurity capability areas. The feature allows the SME employee to understand how mature the organisation is and offers the ability to decide what the next-best actions are to be pursued. The capability improvement dashboard is implemented as an information display and recommended based on the improvement journey status, notifications obtained from SMESEC tools, and knowledge of SME behaviour.
CYSEC.F02 Capability Improvement Journey	The capability improvement journeys offer a series of questions, background information, facts, and recommendations for training videos and tools for a user-selected capability area. The feature allows the SME employee to understand cybersecurity and build cybersecurity capabilities in the organisation. The capability improvement journey is implemented as a configurable questionnaire with an information display for facts and recommendations.
CYSEC.F03 Capability Improvement Specification	The capability improvement specification is used to parametrise a capability improvement journey. It is used by a community reference person to specify recommended capabilities, offering a flexible, loose coupling between the CYSEC tool and the corresponding cybersecurity expertise. The specification is implemented with an XML structured according to a suitable schema. The XML includes a definition of the journey steps, questionnaires, background information, recommendations, how far the SME is in fulfilling the journey, and coach behaviour.
CYSEC.F04 Backlog Management and Reminders	Backlog management and reminders offer the cues needed to build cybersecurity capabilities that require effort and calendar time to be implemented or that reoccur. The prompts are generated in cooperation with the user while answering the questions of the capability improvement journey and help to return to cybersecurity while compensating a potential lack of discipline. The backlog management and reminders may be visible on the capability improvement dashboard or be exported to state-of-the-art backlog management and reminder tools.

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	44 of 66
Reference:	D3.4	Dissemination:	PU	Version:	1.1
				Status:	Final

Feature	Functionality, Benefit, and Implementation
CYSEC.F05 Community Report	The community report offers insights into the state of cybersecurity capability-building in the SME. The insights support the assessment of the state of cybersecurity in the SME community and offer decision-support for recommendations of how to evolve cybersecurity technology. It is implemented as a log of changing context information and observations that can be subscribed to with a publish/subscribe interface. The log is offered as structured data that may be researched with advanced analysis tools.

3.5.5 CYSEC.F01: Capability Improvement Dashboard

The capability improvement dashboard is the start page of the CYSEC tool. It provides the SME employee with the ability to obtain a quick overview of available questionnaires, personalised recommendations, progress and successes.

The following figure shows a screenshot of the capability improvement dashboard.

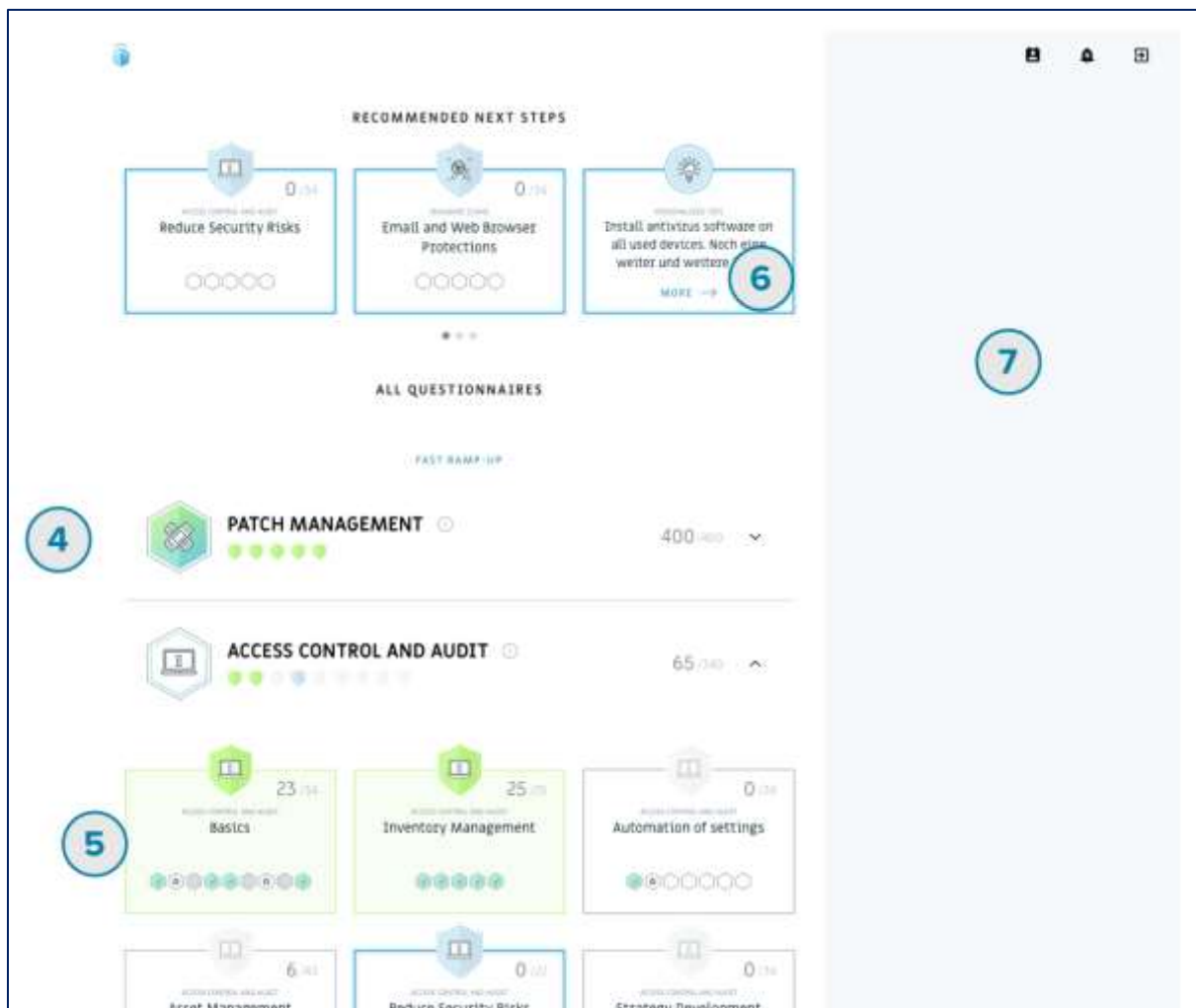



Figure 24: capability improvement dashboard.

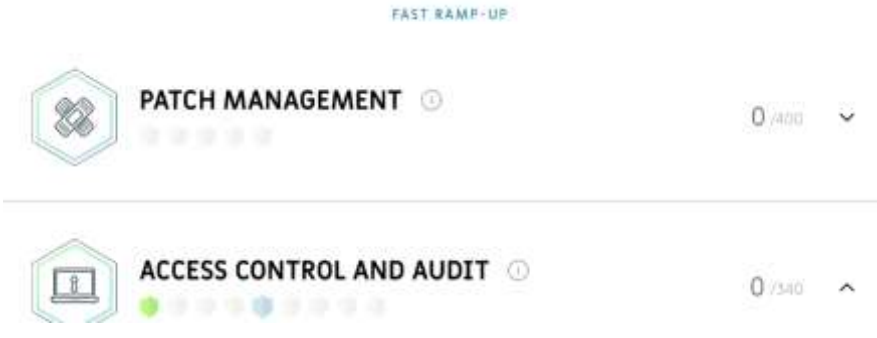

Document name:	D3.4 SMESEC products integration on the Unified Architecture	Page:	45 of 66	
Reference:	D3.4	Dissemination:	PU	
	Version:	1.1	Status:	Final

The dashboard contains the elements specified in the following table. The numbers refer to the figure above.


Table 2: Elements of the CYSEC Dashboard

ID and Name	Description
6 CYSEC.F01.E01 Recommendations	<p>By answering questions, a company profile is created and updated in the background. CYSEC recognises which questionnaires are relevant for the user and recommends these. With these recommendations placed at the top of the dashboard, CYSEC actively influences the user's capability improvements. By following these recommendations, the user moves forward in the capability improvement successfully and quickly.</p>  <p>The top-three recommendations are immediately visible. More suggestions are offered to the user upon demand. Each recommendation is rendered as follows:</p> <ul style="list-style-type: none"> - Recommended work on a capability: badge in the form of a shield, name of the capability area, and an indication of already achieved progress. - Recommended work on a task: a circle with the name of the action. The name may be autogenerated or have been entered by the user when the backlog item was being created. <p>The recommendations are based on a score calculated using the partial ordering of capabilities defined in the incremental capability maturity model offered by the University of Utrecht, expiry times of tasks, and successful implementation orders that CYSEC observed with other SMEs. In the example above, the user is recommended to create personal accounts as part of the access control and audit capability area, work on the reducing security risks in the capability area of malware scans, and assess improvements of access control and audit.</p>
4 CYSEC.F01.E02 Capability areas	<p>The questions are divided into thematic blocks, each corresponding to a capability area. Each capability area is rendered with its name, an icon indicating the meaning of the area, and visual and numeric indicators of implementation progress within the capability area.</p>

Document name:	D3.4 SMESEC products integration on the Unified Architecture	Page:	46 of 66				
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status:	Final

		 <p>The capability areas are ordered according to the partial ordering of capabilities defined in the incremental capability maturity model offered by the University of Utrecht and the implementation progress achieved within the capability areas.</p> <p>In the example above, the fast ramp-up capability area of patch management is placed at the top as the SME has not made any progress in it yet. It is followed by access control and audit for which some progress has been made.</p>
5	CYSEC.F01.E03 Questionnaires Blocks /	<p>Each capability area may be opened for getting access to the included capabilities. Such a capability is reflected as a sequence of questions that the user answers while learning about the capability and implementing it in the company.</p>  <p>Each capability is rendered as a block with an icon and name communicating the meaning of the block and with a graphical progress bar and points indicating the progress achieved within the block. Capabilities that are sufficiently completed, respectively are recommended as a next step are highlighted with colour-coding.</p> <p>In the example above, the basics of access control and audit have been sufficiently implemented according to the maturity model of the University</p>

Document name:	D3.4 SMESEC products integration on the Unified Architecture	Page:	47 of 66				
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status:	Final

		of Utrecht, asset management has been started, and the reduction of security risks has been recommended to be worked on as a next capability.
7	CYSEC.F01.E04 Progress and achievements	<p>In the side panel on the right-hand side of the dashboard, diagrams and badges show the progress and the achievements. The badges are gamification elements that show the user that the effort is worth it and that progress is becoming visible. A badge may correspond to a capability area that has been entirely implemented, a threat that the company can address, or a standard that the company fulfils. These badges may be used as a basis for certification used by the company to demonstrate its maturity in cybersecurity.</p>  <p>The visualisations above show the contents shown to indicate progress and achievements to the users. Left-hand side: badges reflecting achievements. Middle: collected improvement points over time. Right-hand side: recently implemented capabilities.</p>

3.5.6 CYSEC.F02: Capability Improvement Journey

Each CYSEC capability area is constructed as a series of questions, the capability improvement journey, regarding cybersecurity awareness factors and relevant content. The content part encompasses statements about cyber threats and instructions on how to avoid those threats to provide effective security communication with SMEs.

The figure below shows an example of a question screen.

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	48 of 66		
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status:	Final

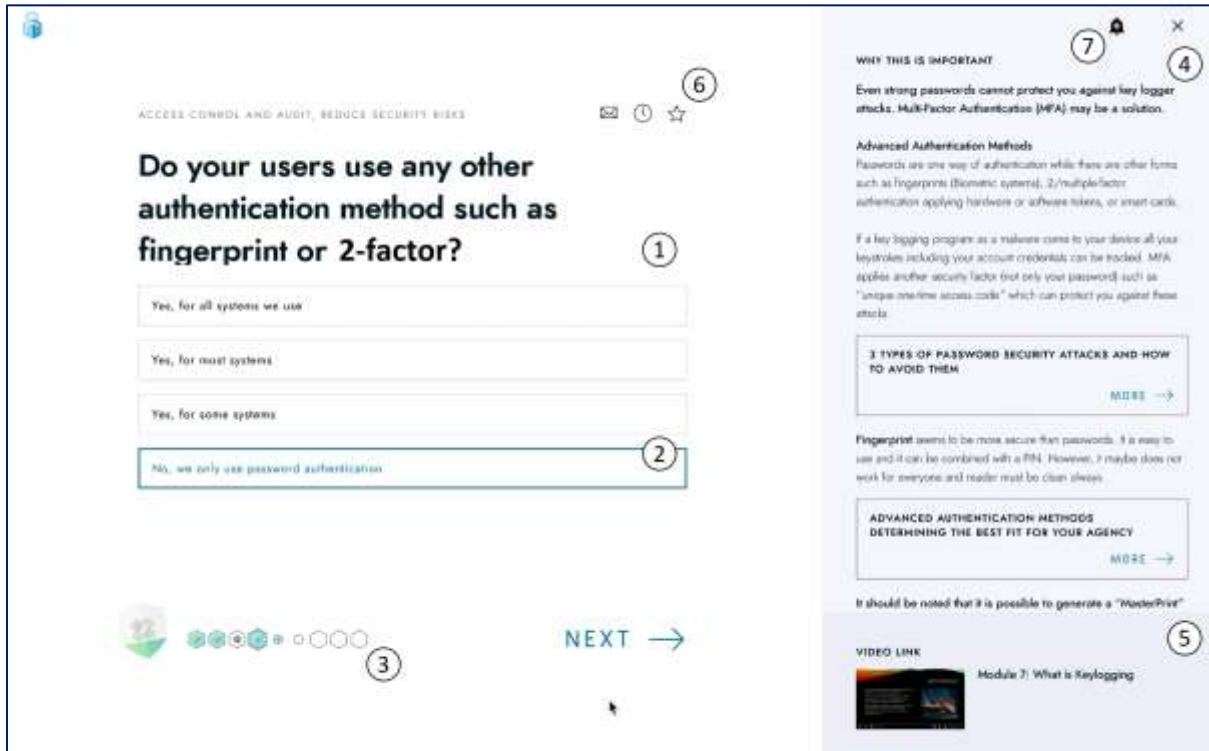


Figure 25: Example of a CYSEC question contained in a capability improvement journey.

(1) shows the question that the user is answering. (2) offers a choice of answers, here with the 4th answer being selected. Each answer indicates the degree of implementation of the practice underlying the question, from full implementation to completely absent implementation. CYSEC memorises the answer and associates actions for capability improvement that eventually lead to improved answers. (3) indicates the implementation progress within the ongoing improvement journey. (4) offers background information, facts, and recommended practices, training, and tools related to the question that the user is answering. (5) offers a link to a video or online-training as an alternative medium to understand the background, facts, and recommendations related to the question. (4) and (5) together offer step-wise learning support for educating the user in cybersecurity. (6) allows the user to manage the implementation of the capability by sending notifications to other users, setting reminders, or starring the question. (7) offers feedback to the user about the CYSEC activities, including observations that are being recorded and action recommendations being added to the improvement backlog for the SME.

The aim of (4) is to improve both users' understanding of the security threats and the ability of the SME to perform the desired behaviour. Therefore, the design of content is based on three parts:

- **What:** short explanation of the cyber threat. This part aims to improve the awareness of what the SME should do.
- **Why:** the necessity and importance of protection against the defined threats to motivate SMEs to follow the instructions. This part may include relevant videos, statistics, or links to further reading. This part aims to improve the threat appraisal ability of the SME.
- **How:** clear instructions to provide relevant steps which can be applied in the real world. Imperative statements are applied to minimize the complexity of the content. This part aims to improve the self-efficacy of the SME.

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	49 of 66		
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status:	Final

The following figure illustrates the successful conclusion of a capability improvement journey. The screen is designed to confirm a feeling of achievement and invite the SME employee to accept the next “challenge,” i.e. the next most-important capability improvement journey according to the CYSEC recommendation.

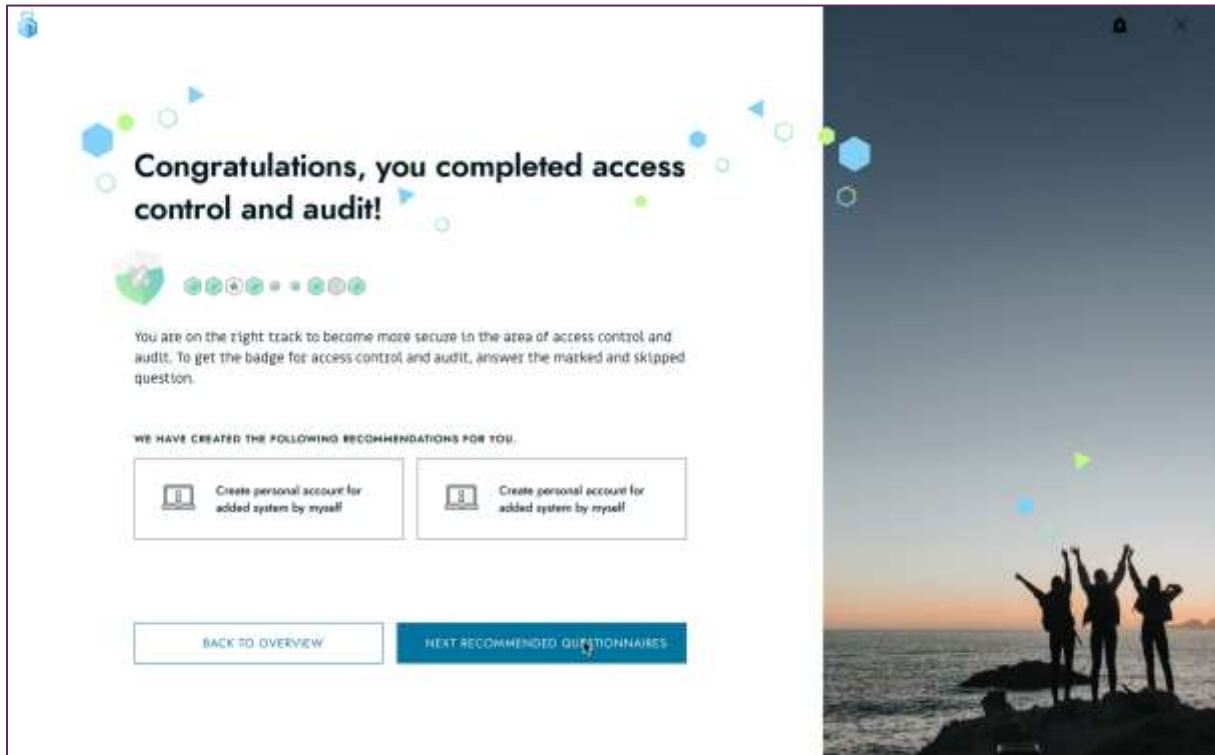


Figure 26: Example of a successful conclusion of a capability improvement journey.

3.5.7 CYSEC.F03: Capability Improvement Specification

CYSEC is configured with an XML file that specifies the capability improvement journeys with questionnaires and recommendations, captures the adoption of cybersecurity practices with the answers provided by the SME employee to these questionnaires, and records context information such as the company, authorised users, and settings of the SME’s CYSEC instance. The XML also embodies behaviour of the CYSEC tool, making it possible to deploy and update CYSEC with an update of parts of the XML. The benefit of this chosen specification approach is the decoupling of CYSEC with the capability improvement journey specifications, giving flexibility for extensions and adaptations of CYSEC recommendations that reflect evolving cyber threats and cybersecurity knowledge as well as supports internationalisation with questions and recommendations translated to new languages.

The following figure gives an overview of the XSD for CYSEC. Visible is the structuring of the SME company in questionnaires and users. The questionnaires are specified with questions, recorded answers, blocks with recommendations, libraries with CYSEC behaviour code, and metadata about the questionnaire. The settings are recorded as attributes at the respective node of the XSD instance.

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	50 of 66
Reference:	D3.4	Dissemination:	PU	Version:	1.1
				Status:	Final

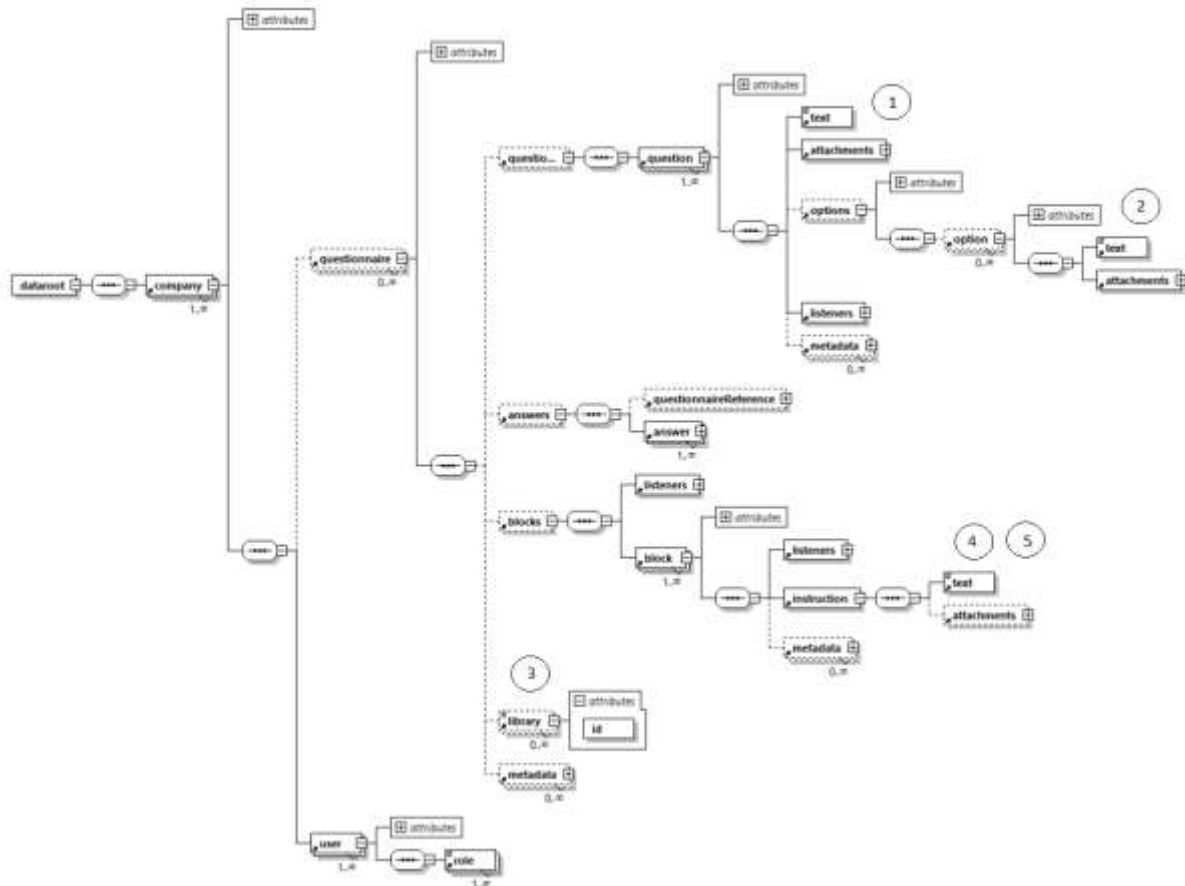

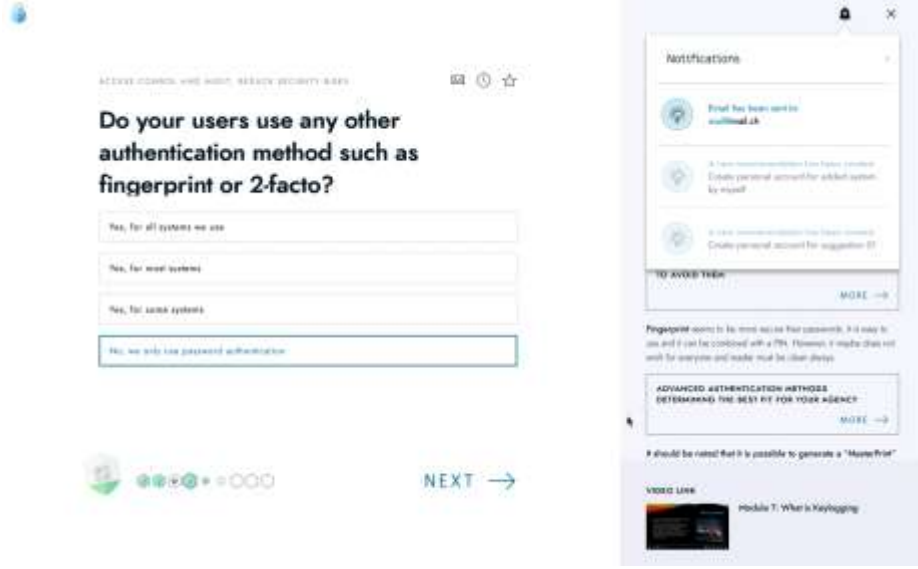





Figure 27: XSD of the CYSEC capability improvement specification.

The following figure shows an excerpt of a CYSEC XSD-compliant specification. It corresponds to the scenario shown in the section of CYSEC.F02, the capability improvement journey.

Document name:	D3.4 SMESEC products integration on the Unified Architecture	Page:	51 of 66	
Reference:	D3.4	Dissemination:	PU	
	Version:	1.1	Status:	Final

	<p>The following figure illustrates the default mail sending screen for mail sending.</p>  <p>The following figure illustrates how CYSEC offers feedback about such user-initiated action with a notification.</p>  <p>The mail is sent to the recipient and added to the recipient's capability improvement dashboard as a recommended next step.</p>
<p>CYSEC.F04.E02 Reminder</p>	<p>The SME employee may postpone the answering of a question or of an associated task to a convenient time. For example, end-user training may be planned to be prepared and held at a later time.</p>

Document name:	D3.4 SMESEC products integration on the Unified Architecture	Page:	53 of 66
Reference:	D3.4	Dissemination:	PU
Version:	1.1	Status:	Final

	<p>CYSEC offers a reminder service, as well as an iCal integration with common calendar tools. On the selected day, the user receives a notification, and the reminder is being shown in the capability improvement dashboard as a recommended next step. The calendar tool integration allows the reminder to be received even if the CYSEC application is not open.</p> <p>The following figure shows the user interface element used for giving access to the SME employee’s backlog.</p> 
<p>CYSEC.F04.E03 Mark</p> 	<p>The SME employee may star questions to be reviewed or filled in later, so they do not get forgotten. For example, the employee may want to investigate the password status of the SME’s devices and, once done, find the concerned question rapidly again.</p> <p>CYSEC handles the starred questions similar to the reminded questions but without an expiry date. For example, these questions are added to the SME employee’s backlog and the recommended next steps of the capability improvement dashboard.</p>

3.5.9 Feature: Community Report

For the cybersecurity community, CYSEC is intended as a tool to collect data about the SMEs’ cybersecurity behaviour and feedback about the practices, training, and tools. The collected data is intended to support empirical research about cybersecurity for SMEs and improve the cybersecurity technology offered to that target group to maximise the likelihood of adoption and adherence.

Document name:	D3.4 SMESEC products integration on the Unified Architecture	Page:	54 of 66
Reference:	D3.4	Dissemination:	PU
Version:	1.1	Status:	Final

A researcher, respectively expert-in-the-loop approach is used to assess and improve cybersecurity technology for SMEs. The approach is an application of the control loop of self-adaptive systems proposed by Cheng et al.⁸ shown in the figure below.

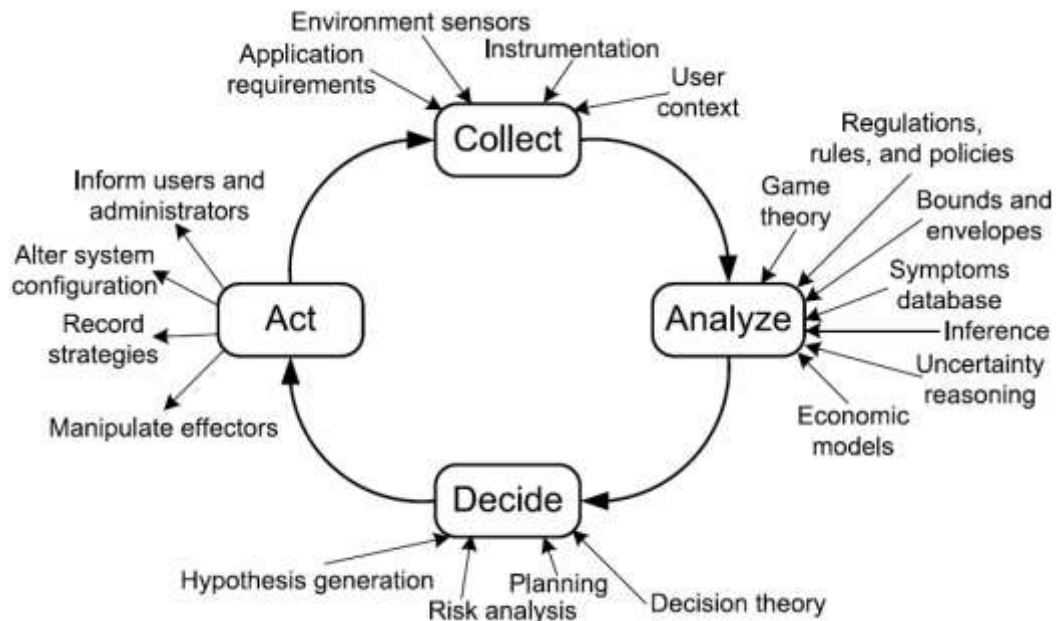


Figure 29: Control loop of enabling self-adaptation based on (Cheng et al., 2009).

Collect: CYSEC is used as a tool to record the progressing user journeys, including when which questions are being answered positively by the SME. If permitted by the SME employee, that event data is offered to the CYSEC Security Assessment tool (CSA) through an Orion context broker publish/subscribe interface.

The following figure gives an overview of the data that, if opted in, is offered on the publish/subscribe interface. Each time the SME employee answers a question on the capability improvement journey, the extent of the practice is reported with a time stamp. Each time a SMESEC tool notifies CYSEC, that event is reported with a time stamp. When data is available, the reported events and practices are connected to the context it applies to, i.e. products, services, or systems of the SME.

⁸ Cheng, B. H., Lemos, R. d., Giese, H., Inverardi, P., Magee, J., & et al. (2009). Software Engineering for Self-Adaptive Systems: A Research Roadmap. In *LNCS 5525 - Software Engineering for Self-Adaptive Systems* (pp. 1-26). Berlin, Heidelberg: Springer.

Document name:	D3.4 SMESEC products integration on the Unified Architecture	Page:	55 of 66
Reference:	D3.4	Dissemination:	PU
	Version:	1.1	Status: Final

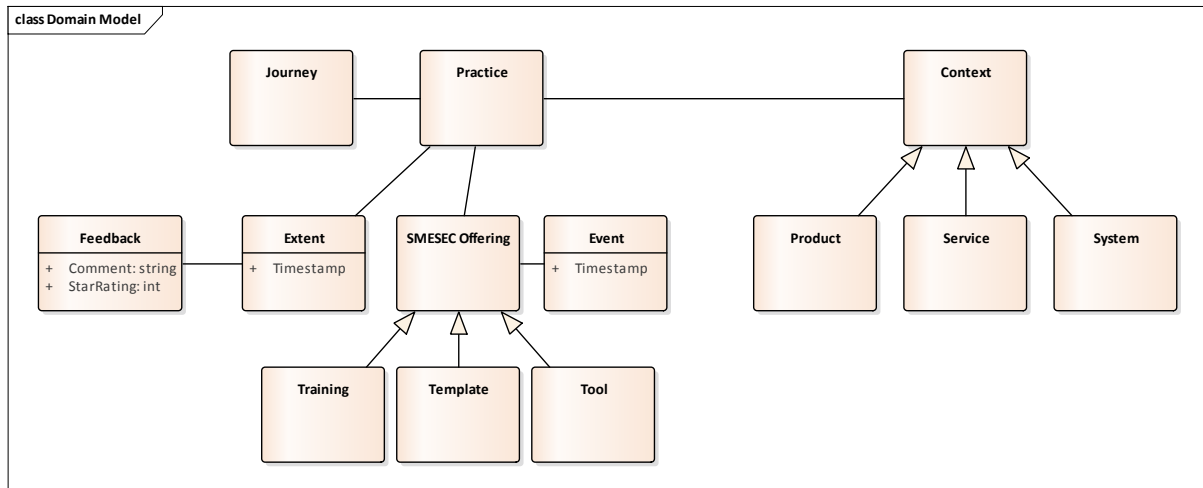


Figure 30: model of the data offered for analysis and community reporting.

Analyse: The CSA anonymises and aggregates these data across SMEs to provide the cybersecurity community reference person with the ability to answer research questions and create reports about the state-of-cybersecurity for SME. No user interface is provided. Instead, the aggregated data is offered in a structured format that allows import into spreadsheet tools, like Microsoft Excel, or advanced analysis tools, like IBM SPSS.

The community reference person is responsible for analysis of the aggregated data and transforms it into decision support by the cybersecurity community as a whole or by specific members. The former may be addressed through research papers or white papers like the community report produced by the SMESEC consortium and described in D3.5. The latter may be offered as a dedicated research service.

Questions that may be answered with the data offered by CYSEC include: a) *how common is a practice in use among the SME*, b) *how much do SME appreciate a given practice*, c) *why do SME not adopt a given practice*, c) *how long time does an SME need to complete a given journey*, and d) *does the use of a given practice correlate with a given incident*. The analysis of the data performed by the authorized cybersecurity reference person and reported in the community report or a research paper.

Decide and Act: With the help of the papers, reports, or research services, members of the community can then act and offer improved practice recommendations, training, and tools that make it easier for SME to be secure for the evolving cyber threats to which they are exposed.

3.5.10 Hybrid Public-Cloud Multi-Tenant Service and On-Premise Deployment

CYSEC provides the SME employee with the ability to use CYSEC as-a-service on the SMESEC cloud (SaaS) or have a local installation deployed on the company premises. The SaaS option offers convenience and does not require installation. The local option offers isolation and the associated confidence that the company profile may not be leaked to third-parties. For both options, however, sharing of the SME’s cybersecurity profile is under the control of the SME employee in an opt-in fashion.

The localized version is lightweight and runs in a small virtual machine. The virtual machine is based on Debian Linux running a Tomcat and Apache environment. The localised version is so light that it

Document name:	D3.4 SMESEC products integration on the Unified Architecture	Page:	56 of 66	
Reference:	D3.4	Dissemination:	PU	
	Version:	1.1	Status:	Final

may even run on a small system such as RaspberryPi, enabling CYSEC to be delivered as a physical box and the associated business models and to be used as a demonstrator at conferences and events. The localised setup of CYSEC is performed with the Debian Advanced Package Tool (APT). An apt-get action is used to install CYSEC and apt-update to update CYSEC.

In environments where a local IT is available, an external authentication mechanism may be used in place of the internal user management. Current user management capabilities are:

- In Application user management.
- User Management through external OAuth provider. If the SMESEC framework is installed, the CYSEC is preconfigured to use the OAuth provider of the framework.
- User Management through an external SAML provider.
- An LDAP support to accommodate user management through a Microsoft Active Directory.

When offered as-a-service, CYSEC provides a self-management system for the SME employees. Each new company created when the first user subscribes himself to the system gets this user as an admin. Each subsequent user may be accepted or declined by the first user. At any time, the application guarantees that there is at least one user with the role administrator. If a new user tries to subscribe to the company administrator users are notified of their request enabling them to accept or deny the request.

Upon SME employee approval, all or selected data contained in the improvement journeys is shared in an easy automated way with the SMESEC cloud. These data include the SME's capability profile and improvement observations needed to create the community report. Security Updates of the platform and improved coaches are available and even possible if not sharing data SMESEC. The SME employee can define these settings through the graphical user interface provided by CYSEC.

3.5.11 Discussion

This section has described the CYSEC, an automated approach to helping SME to learn about cybersecurity and build cybersecurity capabilities by adopting practices recommended by the SMESEC consortium. CYSEC provides the SME employee with the ability to learn, track, plan, and involve his colleagues in improving cybersecurity. To encourage adoption and adherence to cybersecurity practice, CYSEC offers elements of gamification and tailors recommendation to the progressing cybersecurity profile of the SME and the actions performed by the SME employee. CYSEC provides authorised community reference persons to subscribe to updates to evaluate the state-of-the-cybersecurity-practice in SME and perform data-driven research to improve cybersecurity technology. The data is offered in a structured format to allow flexible analysis as part of community reporting and empirical research.

CYSEC is integrated into the SMESEC use case SMEs in the tasks T4.1-5 and validated and refined in collaboration with these SMEs in T5.1-3. The results will be reported in D4.2, D4.4, D4.6, D4.8, and D4.9, respectively in D5.1-3. CYSEC will be evaluated with third-party SMEs in T5.4-5. The results will be reported in D5.4-5.

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	57 of 66	
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status: Final

3.6 FORTH extensions

Concerning extension FORTH.PE01, in SMESEC we are using the ATOS XL-SIEM for real time collection and prioritization, filtering of the attack events. Thus, we need to integrate and facilitate the connection between our EWIS platform with the XL-SIEM. We have achieved that goal, by changing the logging capabilities of our tools and creating a unified logging schema to send the logs to the XL-SIEM. There all the logs from the different tools are gathered, processed and correlated to present the aggregated information to the system administrator. Furthermore, we have worked into synergizing CITRIX NetScaler with FORTH's EWIS in the case of the e-voting pilot using the following setup: When an external connection arrives, it is firstly examined by NetScaler, then, based on ruleset created for the e-voting pilot, if it is not a valid request it is forwarded to the honeypot, for further examination and interaction with the potential attacker. If it a valid request it is forwarded to the e-voting production system. We are performing tests and adjust the configuration between the two systems in order to achieve the correct interplay of the two.

In order to address the proposed collaborative extension FORTH.PE06 we have completely revamped and redesigned the visualization part of the EWIS system to look and feel exactly like the SMESEC framework visualization interface. Moreover, in order to achieve the Single Sign On we have incorporated into our system the Keycloak authentication mechanism and we are able to exchange authentication tokens with the SMESEC Framework web application. We have also created the appropriate APIs to send/receive user information from the SMESEC main application once the user is authenticated successfully.

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	58 of 66		
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status:	Final

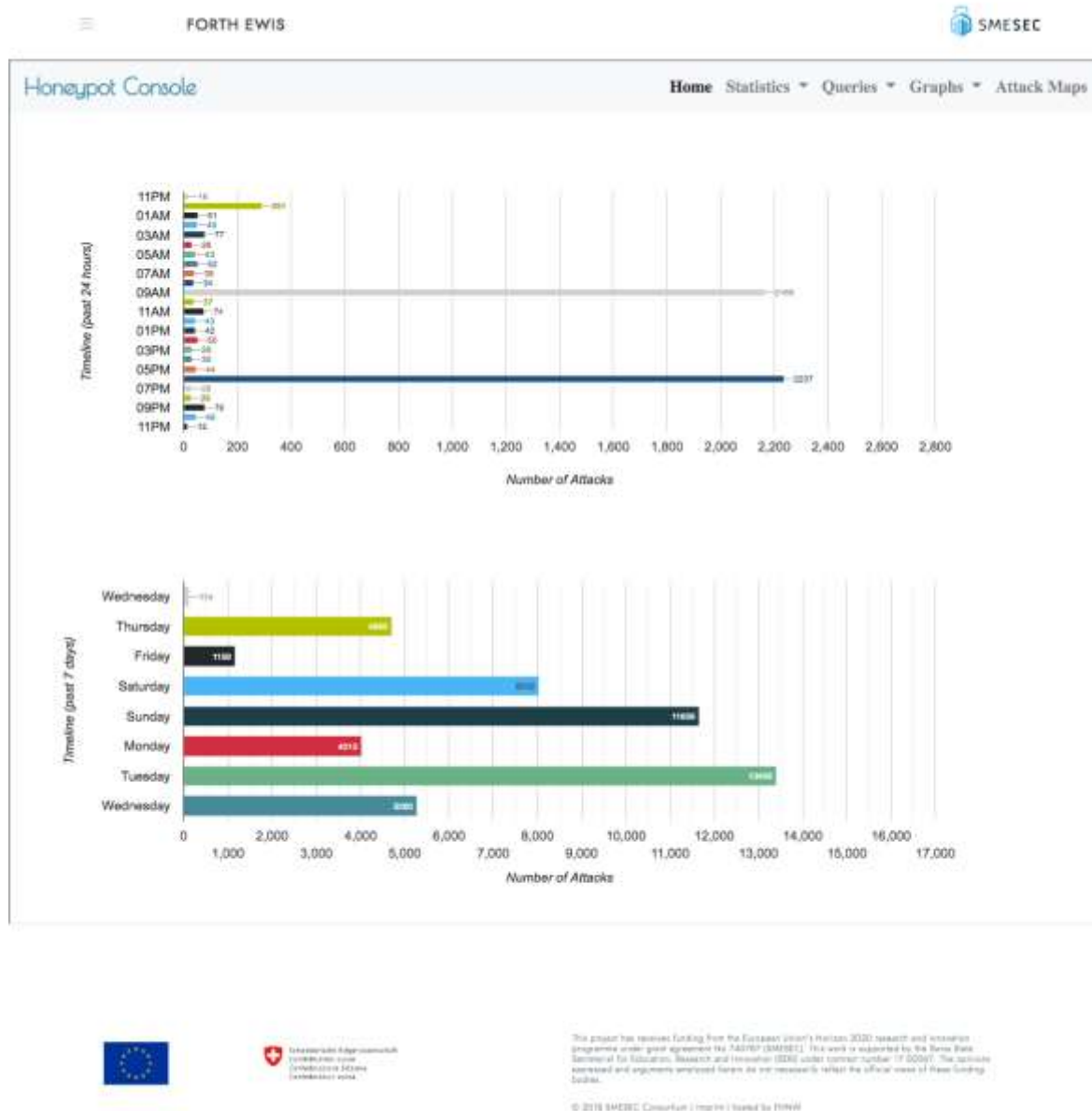


Figure 31: Integrated FORTH EWIS Homepage, seen through SMESEC web application

Finally, concerning collaborative extension FORTH.PE09, we have already, incorporated the DDOS tool into the EWIS solution and is able to send the logs and events to the XL-SIEM and to log them and visualize them through the FORTH EWIS dashboard which has been incorporated into the SMESEC framework.

Document name:	D3.4 SMESEC products integration on the Unified Architecture	Page:	59 of 66	
Reference:	D3.4	Dissemination:	PU	
	Version:	1.1	Status:	Final

3.7 IBM extensions

3.7.1 IBM Anti-ROP Extensions

Almost 90 percent of exploit-based software attacks use hostile Return Oriented Programming (ROP) techniques in their attack chain. Return Oriented Programming is an attack that hijacks the control flow of a program to allow remote code execution by an attacker. Over the years, much work has been done to break this control flow hijack phase of the attack chain and prevent remote code execution of malicious code. So far, the available techniques have had limited success, and have introduced a significant performance burden on the protected devices.

Return Oriented Programming (ROP) is the most common control flow hijack exploit technique that allows an attacker to take control of a program flow. This is done by smashing the call stack and redirecting it to execute attacker instruction sequences. The attacker carries out this exploit by borrowing gadgets, or small pieces of code, from the hijacked program and redirects the control flow to execute these gadgets. The attacker malicious code is compiled of a sequence of these gadgets.

Compiling a ROP attack requires an offline phase where attackers read the target program binary, find the desired gadgets in the target program, and create a list of entry points to execute these gadgets. Each one of these gadgets ends with a return instruction and the attacker hijacks the control flow by controlling the return address of these gadgets, hence the name return-oriented-programing.

Cybercriminals use ROP because it can easily bypass data execution prevention (DEP), a technology implemented in hardware and software to prevent execution of data sections. One of the many techniques developed to prevent ROP attacks is address space layout randomization (ASLR), a process implemented in almost all operating systems. ASLR randomizes the address bases of the sections, forcing the attacker to guess the location of the gadgets. Attackers building a ROP attack assume that the gadgets they need are in absolute addresses or shifted by constant bytes. If they can detect the shift of one gadget, they can detect the shifts of all gadgets.

This is where the IBM Anti-ROP solution comes in. Given a source code of a program and a randomization seed we compile the source code with randomization of: the order of the functions, the alignment of functions, and the linking order of the objects. For every deployment of the program on an IoT device we compile a new unique copy of the program.

Our solution challenges the attacker to guess all address locations of the gadgets. Unlike in ASLR technology, finding a gadget in one block does not reveal the addresses of the other gadgets. This results in a new situation where every IoT device is created in a unique manner and renders the attacker guessing of gadget addresses impossible.

The IBM Anti-ROP Extension doesn't modify the functionality of the SME's IoT software but makes it a lot harder for attackers to successfully exploit vulnerabilities in its code.

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	60 of 66		
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status:	Final

3.7.2 Testing platform Java script extension

JavaScript is one of the most popular programming languages in the world. Only in GitHub there are more than 2.3 million unique projects written in JavaScript. Amongst other applications, JavaScript is used for server-side development using the NodeJS infrastructure.

Statistics collected by Snyk show that 77% of sites use at least one vulnerable JavaScript library. This is an alarming situation that can lead to compromise of business in general, and SMEs in particular.

Nowadays, there are some static analysis tools that alert developers of bad, or potentially vulnerable places in their code. These tools mainly focus on better coding style, and trivial best practices for secure development. Currently, there is no solution for more complex vulnerability analysis of server-side JavaScript code. This issue we aim to address.

We introduce a pluggable fuzzing infrastructure by uplifting a state-of-the-art fuzzing paradigm (AFL) into a high-level, interpreted, dynamic, and weakly typed language (JS). We focus on server-side JavaScript code (NodeJS) to detect vulnerabilities, find attack vectors and exploits, and discover various bugs. This infrastructure can be used as a standalone tool, as part of a larger testing platform, or be deployed as part of a software development life cycle. Even though the infrastructure is highly pluggable and versatile, one can start and run it within minutes with little technical training, or no training at all.

3.7.3 AngelEye extensions

Many applications have security vulnerabilities that can be exploited. It is practically impossible to find all of them due to the NP-complete nature of the testing problem. Security solutions provide defenses against these attacks through continuous application testing, fast-patching of vulnerabilities, automatic deployment of patches, and virtual patching detection techniques deployed in network and endpoint security tools. These techniques are limited by the need to find vulnerabilities before the ‘black hats’.

We propose an innovative technique to virtually patch vulnerabilities before they are found. We leverage testing techniques for supervised-learning data generation and use artificial intelligence techniques to create predictive deep neural-network models that read an application’s input and predict in real-time whether it is a potential malicious input.

Our technique was tested on an ahead-of-threat experiment in which we generated data on old versions of an application, and then evaluated the predictive model accuracy on vulnerabilities found years later. Our experiments show ahead-of-threat detection on LibXML2 and LibTIFF vulnerabilities with 91.3% and 93.7% accuracy, respectively.

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	61 of 66		
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status:	Final

4 Market benefits brought by innovations

4.1 Context

Although the new digitization era offers huge economic and social opportunities, it also changes the nature and magnitude of cyber risks and creates new vulnerabilities cyber attackers seek to exploit. European countries and in particular the Small Medium Enterprises (SMEs) are targeted more and more often – according to the 2017 Global State of Information Security Survey, at least 80% of companies in Europe have experienced at minimum one cybersecurity incident over the last year. While the risk of targeted, sophisticated cyber-attacks is growing, most European companies are still unprepared and / or unaware of the risks, as almost 70% of European SMEs do not understand the impact and consequences of their exposure to cyber risks.

Looking across the treat categories, the most prevalent are:

1. Malware and phishing – the most common type of threat encountered; the cost of such incident is relatively low in comparison to other types of attacks; the high rate of occurrence makes it the costliest attack vector.
2. Distributed Denial of Service (DDoS) – the fast adoption of IoT triggered numerous, sophisticated and frequent DDoS attacks.
3. Data breaches – sensitive personal information, such as financial and health records, remains the key focus of cyber-attacks.

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	62 of 66	
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status: Final

5 SMEs struggle not only due to a lack of awareness, but also because they perceive cybersecurity as a costly endeavour.

5.1 The SMESEC proposal

The SMESEC partners are proposing to develop a cost-effective suite of cyber-security tools. The suite supports SMEs in managing network information security risks and threats and identifying opportunities for implementing secure, innovative technologies for the digital market. As a benefit, the framework shall allow SMEs not only look at cyber-security as an obstacle but also as an opportunity for business.

5.2 The SMESEC innovations and their market impact

As an important part of the project activities, the SMESEC tool providers are working on advancing their solutions and proposing new innovations. The innovations road-map is designed on a two-fold level: either is a consequence of the dynamics of targeted market (this side was covered within the SMESEC Project by Deliverable 2.1) , which evolves, either is an internal strategy of focusing on constant technological advancements or is a combination of both.

This is why, the project partners are working on developing and implementing individual and collaborative innovative extensions, aiming to gain significant market impact.

Impacts:

- 1) New technical differentiators – as an example, the integration of Bitdefender GravityZone with ATOS XL-SIEM is a collaborative innovation whose scope is to make available the information collected by GravityZone to the XL-SIEM. This joint integration is a market differentiator proposed by SMESEC unified framework as it facilitates the access to information. Even a non-security expert will be able to monitor the security of the network, as a whole, within a short timeframe. On top, events correlated from multiple sources may enable the XL-SIEM to provide better security overall. Market wise this translates to consistent USPs which could attract more customers.
- 2) Clients satisfaction – as for their requirements SMESEC is proposing new technical solutions for an easier, better and safer online business presence.
- 3) Increased competitiveness – determined by the new extensions.
- 4) Improved brand recognition and value – among the project partners are businesses with very successful and proven track-record. Although their brand consistency is already important, by jointly working on innovative extensions and deploying those as part of SMESEC, their brand recognition and value are expected to grow.
- 5) New partnerships – as a result of the technical collaborative work, the commercial teams are working together to identify new and profitable business cases.
- 6) Increased turnover and improved profitability – One of the pilots within SMESEC may recommend to their clients the SMESEC solutions which lead to new sales channels.

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	63 of 66	
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status: Final

Since SMESEC activities are still in progress is yet difficult to accurately assess the market impact of the implemented innovative extensions. Nonetheless, there are some clear benefits impacting both the project partners (more competitive solutions, improved brand recognition, growing sales etc.) and the targeted customers (access to latest technology, access to integrated solutions, lower acquisition costs etc.).

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	64 of 66		
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status:	Final

6 Conclusions

This report contains a summary of the work performed in Task3.2 for extending the SMESEC products and integrating them into the SMESEC framework. The product extensions were proposed in D2.1, upon a comprehensive market analysis.

The integration into the SMESEC framework was a challenging problem, as we wanted to keep each product an individual entity while working together to provide security as a whole. On one hand, there were efforts to provide security events and manage them into the SIEM product, the ATOS XL-SIEM. The SMEs adopting SMESEC will also need a unified view of the framework, so we also worked on providing a unified dashboard.

For extending the coverage on the market segments analyzed in D2.1, most partners also extended their tools with individual innovations, meant to strengthen their market position.

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

For collaborative extensions, Bitdefender worked on the integrating 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.

The work on the product extensions at the time of delivery of this document is mainly complete, some refinements will follow in Task 3.4.

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	65 of 66		
Reference:	D3.4	Dissemination:	PU	Version:	1.1	Status:	Final

7 Appendix 1

Technical constraints of the IoT device of WorldSensing used in their use case

1. Hardware Key Features

1.1 System

CPU:

- Based on ARM 926EJS core processor
- Up to 230 MIPS
- Real-time clock saved by battery
- Hardware watchdog
- Optimised power consumption management

Volatile memory:

- Low power DDRAM 128 MB
- 10 MB used for system firmware

Non-volatile memory:

- 128 MB NAND flash (40MB used for system firmware and autorecovery mechanism)

1.2 User interfaces

Internal LEDs:

- Operational status : power, GSM signal strength level, WAN connectivity indicator

USB host interface allowing :

- Local software upgrade with simple USB key
- USB/NET local configuration/maintenance access

Internal push buttons:

- Manual station reset
- Manual test or installation procedure launch

1.3 Communication

LongRange:

- Incorporate LoRa (TM) bidirectional communications technology (RX : 863-873MHz , TX : 863-873MHz) *
- Sensitivity : up to -141 dBm
- Tx conducted power from 0dBm to +28dBm
- 49 LoRa Demodulators over 9 channels
- More than 15km range in sub-urban situation

WWAN:

- HSDPA/UMTS (900/2100MHz) : DL 3.6 Mbps / UL 384 Kbps (HSDPA), UL/DL 384Kbps (UMTS)
- GPRS/EDGE (850/900/1800/1900MHz) : UL/DL 85.6Kbps (GPRS), UL/DL 236.8Kbps (EDGE)
- IMEI inside
- Internal antenna

Ethernet :

- PowerOverEthernet IEEE 802.3af alternative B 10/100 Base T compliant

1.4 Positioning/Timing

GPS:

- Integrated GNSS high sensitivity GPS module
- NMEA 2.0 compliant
- Internal antenna

1.5 Sensors

- Embedded temperature sensor
- Door opening detection system

1.6 Power

- PowerOverEthernet supply : 48V class 0 (Max : 15Watts, Nominal : 3Watts (Lora Rx mode with GSM network attachment)
- DC power supply (ex : solar panel use) : 11 to 30Volts
- Power control : ignition detection, software OFF switching
- Back-up battery (up to about 1 minute allowing safe powerdown)

Document name:	D3.4 SMESEC products integration on the Unified Architecture			Page:	66 of 66
Reference:	D3.4	Dissemination:	PU	Version:	1.1
		Status:			Final