



SMESEC

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

D4.6 Final integration report on Industrial Services SME pilot

Document Identification			
Status	Final	Due Date	31/05/2019
Version	1.1	Submission Date	31/05/2019

Related WP	WP4	Document Reference	D4.6
Related Deliverable(s)	D2.1, D3.1, D4.5	Dissemination Level (*)	PU
Lead Organization	WoS	Lead Author	Francisco Hernández-Ramírez
Contributors	Francisco Hernández-Ramírez (WoS) Olmo Rayón (WoS) Hamza Baqa (EGM) Alireza Shojaifar (FHNW)	Reviewers	Filip Gluszak (Grid)

Keywords:
IoT, security, pilot, SME

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
Carles San Agustín	WoS
Michael Rohrer	WoS
Hamza Baqa	EGM
Alireza Shojaifar	FHNW
Olmo Rayón	WoS
Bruno Varela	WoS
Francisco Hernández-Ramírez	WoS

Document History			
Version	Date	Change editors	Changes
0.1	08/05/2019	Olmo Rayón (WoS)	Table of contents template for all use case partners
0.2	14/05/2019	F.Hernández-Ramírez (WoS)	First draft of the document.
0.3	-		Second draft after QA1
0.4	27/05/2019	Alireza Shojaifar	CYSEC contribution
1.0	27/05/2019	F.Hernández-Ramírez (WoS)	Final version after QA2
1.1	31/05/2019	ATOS	Quality review + submission to EC.

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Francisco Hernández-Ramírez (WoS)	31/05/2019
Technical manager	Christos Tselios (Citrix)	31/05/2019
Quality manager	Rosana Valle Soriano (Atos)	31/05/2019
Project Manager	Jose Fran. Ruíz (Atos)	31/05/2019

Document name:	D4.6 Final integration report on Industrial Services SME pilot				Page:	2 of 40	
Reference:	D4.6	Dissemination:	PU	Version:	1.1	Status:	Final

Table of Contents

Document Information	2
Table of Contents	3
List of Figures	5
List of Tables.....	6
List of Acronyms.....	7
Executive Summary	9
1 Introduction.....	10
1.1 Purpose of the document	10
1.2 Relation to other project work.....	10
1.3 Structure of the document	10
2 Requirements and needs: from planning to action	12
3 Scenarios and usability.....	14
3.1 Updates and enhancement	14
3.2 Architecture.....	15
3.2.1 Physical Architecture.....	15
3.2.2 Functional Architecture	15
3.3 Scenarios of SMESEC.....	16
3.3.1 Case 1: Infrastructure operator	16
3.3.2 Case 2: Infrastructure and security manager	16
3.4 Impact of SMESEC in the use case.....	17
3.4.1 Asset Inventory.....	17
3.4.2 Threat Modelling and Analysis	18
3.4.3 Monitoring (end-systems)	19
3.5 Business impact.....	20
4 Technical integration of SMESEC.....	21
4.1 Integration of SMESEC in the use case	21
4.2 Analysis and evaluation of SMESEC.....	23
4.2.1 Test as a Service [TaaS]	23
4.2.2 Return-Oriented Programming Blocker [Anti-ROP]	25
4.2.1 System Information and Events Manager [XL-SIEM].....	25

Document name:	D4.6 Final integration report on Industrial Services SME pilot				Page:	3 of 40	
Reference:	D4.6	Dissemination:	PU	Version:	1.1	Status:	Final

4.2.2	Malware Prevention System [Gravity Zone].....	25
4.2.3	NetScaler	26
4.2.4	Honeypot	26
4.2.5	SMESEC Extensions [Recommendation Engine].....	27
4.2.6	SMESEC Awareness Tool [CYSEC].....	28
4.3	Testing and feedback provided.....	29
4.3.1	Test as a Service [TaaS]	29
4.3.2	Return-Oriented Programming Blocker [Anti-ROP]	29
4.3.3	System Information and Events Manager [XL-SIEM].....	29
4.3.4	Malware Prevention System [Gravity Zone].....	30
4.3.5	NetScaler	31
4.3.6	Honeypot	31
4.3.7	SMESEC Extensions [Recommendation Engine].....	33
4.3.8	SMESEC Awareness Tool [CYSEC].....	33
5	Cybersecurity awareness and training.....	34
5.1	Training and awareness	34
6	Conclusions.....	36
6.1	Final analysis and next steps	36
6.2	Fulfillment of objectives.....	36
6.3	Future outcomes and business development	36
	References	38
	Annexes.....	39

Document name:	D4.6 Final integration report on Industrial Services SME pilot				Page:	4 of 40	
Reference:	D4.6	Dissemination:	PU	Version:	1.1	Status:	Final

List of Figures

Figure 1. General view of the stadium: IoT deployment enlargement	14
Figure 2. Physical architecture of the pilot	15
Figure 3. Functional architecture of the pilot	15
Figure 4. Data frontend view with structural information from the stadium	16
Figure 5. Pilot III (Industrial Services): IT and OT layers main items	17
Figure 6. Pilot Asset Inventory: graphical representation	18
Figure 7. Pilot Asset Inventory: detailed information	18
Figure 8. Risk Assessment of Assets in Pilot III: severity overview	19
Figure 9. Risk Assessment of Assets in Pilot III: mitigation actions against critical risks	19
Figure 10. Monitoring tool: front-end server at Pilot III status	20
Figure 11. Pilot's threats coverage by the adopted SMESEC solutions	21
Figure 12. Overlap of Net Scaler functionalities with Gravity Zone and Honeypot	22
Figure 13. Information flow at the pilot's domains	22
Figure 14. Matching between SMESEC tools and Pilot III domains	23
Figure 15. LoRaWAN test set-up	24
Figure 16 LoRa testing configuration page (ABP)	24
Figure 17. Loadsensing, Gravity Zone and XL-SIEM integration scheme	25
Figure 18. Honeypot emulation of IoT services (screenshot)	26
Figure 19. Honeypot architecture and integration within SMESEC architecture	27
Figure 20. Honeypot architecture and integration within SMESEC architecture	27
Figure 21. SMESEC Recommendation Engine. General architecture	28
Figure 22. CYSEC tool: screenshot of one of the filled forms	28
Figure 23. TaaS report on LoRa	29
Figure 24. XL-SIEM frontend. General indicators of Pilot III	30
Figure 25. Gravity Zone. Overall figures of the monitored infrastructure	30
Figure 26. Gravity Zone. Malware detection and deletion	30
Figure 27. Gravity Zone and XL-SIEM integration. (Up) General logs repository. (Down) Detailed information of one of the security events.	31
Figure 28. Database with log interaction towards the honeypot	32
Figure 29. Successful attack example from IOT-Honeypot	32
Figure 30. CYSEC: screenshot of the questionnaires	33

Document name:	D4.6 Final integration report on Industrial Services SME pilot				Page:	5 of 40	
Reference:	D4.6	Dissemination:	PU	Version:	1.1	Status:	Final

List of Tables

Table 1. Summary of functional requirements of Pilot III (Industrial Services)..... 12

Table 2. Summary of security requirements of Pilot III (Industrial Services)..... 13

Table 3. Summary of “testing and feedback” requirements of Pilot III (Industrial Services) 13

Table 4. Adopted tools in the Pilot III (Industrial Services) 21

Table 5. Training and awareness plan: targeted employees..... 34

Table 6. Training and awareness plan: general training sessions at Worldsensing 34

Table 7. Training and awareness plan: technical measures implemented at WS with associated training 35

Document name:	D4.6 Final integration report on Industrial Services SME pilot				Page:	6 of 40
Reference:	D4.6	Dissemination:	PU	Version:	1.1	Status: Final

List of Acronyms

Abbreviation / acronym	Description
AWS	Amazon Web Services
DB	Database
DPO	Data Protection Officer
Dx.y	Deliverable number y belonging to WP x
EC	European Commission
EWIS	Electrical Wiring Interconnection System
FE	Frontend
GDPR	General Data Protection Regulation
GW	Gateway
GSLB	Global Server Load Balance
HA pair	High Availability Pair
HTTP	Hyper Text Transfer Protocol
HTTPS	HTTP Secure
IP	Internet Protocol
IT	Information Technology
JSON	JavaScript Object Notation
MIP	Mobile Internet Protocol
NetBIOS	Network Basic Input/Output System
NTP	Network Time Protocol
OWASP	Open Web Application Security Project
PKCS	Public Key Cryptography Standards
RCP	Remote Copy Protocol
REST	Representational state transfer
ROTI	Report of Test and Inspection
SIEM	Security Information and Event Management
SMB	Server Message Block
SME	Small Medium Enterprise
SMTP	Simple Mail Transfer Protocol

Document name:	D4.6 Final integration report on Industrial Services SME pilot				Page:	7 of 40	
Reference:	D4.6	Dissemination:	PU	Version:	1.1	Status:	Final

Abbreviation / acronym	Description
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TelNet	Telecommunication Network
TFTP	Trivial Files Transfer Protocol
VM	virtual machine
VP	Vice-President
VPC	Virtual Private Cloud
VPN	Virtual Private Network
WAF	Web Application Firewall
XML	Extensible Mark-up Language

Document name:	D4.6 Final integration report on Industrial Services SME pilot				Page:	8 of 40	
Reference:	D4.6	Dissemination:	PU	Version:	1.1	Status:	Final

Executive Summary

This deliverable describes the work associated with the integration of the SMESEC Framework in the Pilot III “Industrial Services” at M24. The report is based in the deliverable D4.5 provided at M18. Here, we build on top of this initial document the following iterations done in the project, both from a technical and an awareness point of views. Together with the updates implemented in the system, we report the work done in the awareness and training area to cover the needs of the employees identified at the beginning of SMESEC.

Additionally, we also report the pilot status and next steps to be done in the project with the SMESEC Framework and how the initial objectives of the use case are fulfilled. We also describe the business development and the impact SMESEC has in the IoT area, as business improvement is a topic for the project as critical as the technical development.

Finally, this document describes in detail the specifics of the Pilot III use case: scenarios, the update of requirements, testing, the impact of SMESEC in the use case, and other minor aspects.

In summary, this document overviews the current status of the “Industrial Services” pilot. The work described here will be continued in WP5 for further testing, analysis, and improvement using the enhancements done incrementally in SMESEC during the third year and taking advantage of the large testing and feedback provided by the open call activity.

Document name:	D4.6 Final integration report on Industrial Services SME pilot				Page:	9 of 40	
Reference:	D4.6	Dissemination:	PU	Version:	1.1	Status:	Final

1 Introduction

1.1 Purpose of the document

This is the second deliverable of WP4 related to the “Industrial Services” pilot. The role of this WP in the project is to adapt the SMESEC security framework prototype to the different pilots proposed in the grant agreement.

Specifically, D4.6 provides an in-depth description of the integration of SMESEC in the use case at M24, the impact at the organization level (Worldsensing), the cybersecurity training and awareness performed in the scope of the project, fulfilment of objectives as described in the first year and the next steps, which will be followed in WP5.

Specifically, D4.6 provides tangible proofs that the SMESEC tools are effectively working on top of the Worldsensing’s infrastructure, enriching the business proposition of the core product of the company. Besides, it is shown how the nascent cybersecurity awareness rising within Worldsensing is being consolidated slowly but surely.

1.2 Relation to other project work

As described before, this document covers the advanced efforts carried out to integrate the SMESEC security framework into the “Industrial Services” pilot. The work described here will be used for other deliverables and Work Packages such as:

- D5.1 testing of the scenarios for validation
- D5.2: specification of the integrated products, services and specific test in the use case
- D5.3: execution of trials in the use case
- WP6: the results of this deliverable will be used for enriching the exploitation and dissemination activities

For a better understanding of this document, it is also absolutely recommendable reading D2.1, which provides the rationale behind the main list of the pilot’s requirements and D4.5 that provides a first introduction to the pilot’s motivations and rationale.

1.3 Structure of the document

This document is structured in 6 major chapters:

Chapter 1 presents an introduction to the deliverable’s motivation.

Chapter 2 updates and reviews the requirements and needs identified in the second year.

Chapter 3 presents characteristics of the use case: update of the architecture, description of the scenarios, and the impact of SMESEC in the use case from a technical and business point of view.

Chapter 4 presents the technical integration of SMESEC tools in the use case, updated from the last version presented in M18.

Document name:	D4.6 Final integration report on Industrial Services SME pilot				Page:	10 of 40	
Reference:	D4.6	Dissemination:	PU	Version:	1.1	Status:	Final

Chapter 5 describes the cybersecurity awareness and training plan used in the use case.

Chapter 6 summarizes the conclusions at M24 of the integration status of the SMESEC platform in the use case.

Document name:	D4.6 Final integration report on Industrial Services SME pilot				Page:	11 of 40	
Reference:	D4.6	Dissemination:	PU	Version:	1.1	Status:	Final

2 Requirements and needs: from planning to action

The list with the general requirements of the deployed technology at the pilot venue was initially presented in the deliverables D2.1 and D4.5. Since then, both the functional and security requirements have hardly changed, except for minor adjustments in the Cloud domain directly linked to the normal progress of Loadsensing product. However, a new set of requirements labelled as “testing and feedback” has been identified as crucial. Actually, the real added value of the pilot for Worldsensing consists of providing a full picture of how the system behaves once the security layer is running. These requirements are listed in Table 3, and they should materialize in internal documentation to be used in future deployment experiences and similar projects.

Domain	Description	Requirements
IoT devices	Sensors and dataloggers	Low-power devices
		Robust design
		RoHS compliant
		Inclination measurements (2-axis)
Gateways	Bridge to transfer sensors' data to the Cloud	Stable internet connection
		Adequate physical location
		PoE system (57V)
		Waterproof protection
Cloud	Data processing and user interface	Centralization server
		Linux Server (Ubuntu 16)
		8GB of RAM
		500 GB hard drive
		SSH to the gateways
		Data storage capability
		Visualization server
		Linux Server (Ubuntu 16)
		8GB of RAM
		500 GB hard drive
		User friendly interface

Table 1. Summary of functional requirements of Pilot III (Industrial Services)

Document name:	D4.6 Final integration report on Industrial Services SME pilot				Page:	12 of 40	
Reference:	D4.6	Dissemination:	PU	Version:	1.1	Status:	Final

Domain	Requirement	Rationale
IoT devices	Enhanced physical security	Integrity of data to be guaranteed.
		Easy manipulation of the devices is highly likely.
		No administration rights on the system (SW).
Gateways	Attack scalability (mitigation)	The successful attack to one device should not be replicable to others.
	Enhanced physical security	The device should not be easily accessible to avoid unauthorized handling.
	Segmented and protected network	Packages reaching the gateway to be filtered.
	Remote access	Reaching the gateway through shell should be only possible through VPN or an equivalent technology.
Cloud	Servers hardening	Apply highly restrictive protocols since the communications are well bounded advisable.
	Vulnerability assessment	Penetrations tests should reveal the real status of the server in relation with security once the pilot is running.
	Enhanced web app security	Errors such as Cross Site Scripting, Injections and Broken Authentication to be early detected. OWASP recommended
	Segmented and protected network	Packages reaching the server to be filtered.
	Sandbox systems	Traffic labelled as malicious should be redirected to a sandbox system for later monitoring and analysis.
	User awareness plan	The human behaviour in organizations is a rich source of security threats. Users involved in the pilot should have some basic security knowledge to minimize risks.

Table 2. Summary of security requirements of Pilot III (Industrial Services)

Domain	Requirement	Rationale
Client	Data gathering	Easiness assessment of the generated data collection. Export feasibility.
	Usability	Feedback of the overall impression created by the end-user.
	Infrastructure management	Specific feedback from the infrastructure manager.
	Security management	Specific feedback from the security manager.
SMESEC partners	Integration	Feedback of the security tool integration experience.
	Documentation	Assessment of the pilot documentation.
	Security assessment	Assessment of the Loadsensing maturity level.
Testing Environment	Uptime / downtime	Evaluation of the system availability.
	Remote access	Evaluation of the external access to the network infrastructure.
	Lessons learnt	Identification of general problems identified by third parties involved in the pilot.

Table 3. Summary of “testing and feedback” requirements of Pilot III (Industrial Services)

Document name:	D4.6 Final integration report on Industrial Services SME pilot				Page:	13 of 40	
Reference:	D4.6	Dissemination:	PU	Version:	1.1	Status:	Final

3 Scenarios and usability

3.1 Updates and enhancement

The preliminary deployment of the pilots' elements was already completed at M18, as explained in D4.5. Since then, the pilot has evolved to both meet the requirements of the stadium operator and adopt the new functionalities of the SMESEC solution.

As regards the first point, the need for a more ambitious Loadsensing deployment has been identified as a priority to monitor the entire infrastructure. Quoting the first feedback from the end-user: *“Visibility over the whole infrastructure¹ would be highly valuable since sensors deployed in one side of the stadium do not leave any chance to induce what is the status of the other one”*. This has resulted in a scaling-up of the installed physical IoT nodes in the stadium (Fig.1). Besides, the user interface layer of the system has been revised to respond the following specific concern: *“It would be nice to have a more user-friendly front-end to visualize the data instead of just having the raw information from the sensors”* (Annex I).

The SMESEC implementation has also risen the awareness of the numerous cybersecurity risks in Worldsensing. This has resulted in the adoption of new monitoring tools and development strategies beyond the mere security framework, purposely all of them intended for hardening the entire pilot infrastructure.



Figure 1. General view of the stadium: IoT deployment enlargement

On the other hand, the main updates directly linked to the SMESEC framework have focused on the effective interconnection between the security tools (i.e. antivirus logs sent to XL-SIEM) and the development of business rules necessary to deal with the alerts coming from the solutions when attacks and malfunctions in the IT domain occur.

¹ Visibility is here defined as the monitoring capability of the entire infrastructure.

Document name:	D4.6 Final integration report on Industrial Services SME pilot				Page:	14 of 40	
Reference:	D4.6	Dissemination:	PU	Version:	1.1	Status:	Final

The details of the changes implemented from M18 to M24 and the current status of the pilot are provided in the following sections of this deliverable.

3.2 Architecture

The upgrade of the pilot elements outlined in the former section is reflected in some minor changes of the end-to-end solution architecture. Despite the fundamentals remains the same compared to the presented one in the deliverable D4.5, there are slight differences which are commented on below.

3.2.1 Physical Architecture

To attain the requested upgrade of services, the physical architecture (IoT nodes) has been doubled, moving from 5 dataloggers and a single gateway, to 10 dataloggers and two gateways (Fig.2). This new deployment is intended to increase the quality of service (improved granular data acquisition capability), but also to ease the validation of some of the SMESEC specific functionalities. In particular, each one of the gateways implements two different firmware instances to thus assess the effective Anti-ROP protection capabilities.



Figure 2. Physical architecture of the pilot

3.2.2 Functional Architecture

The pilot instance running at M18 was basically an exchange point for the end-user to get data coming from the sensors (Layers 0 and 1 in Fig, 3), while security tools were running in background processes.

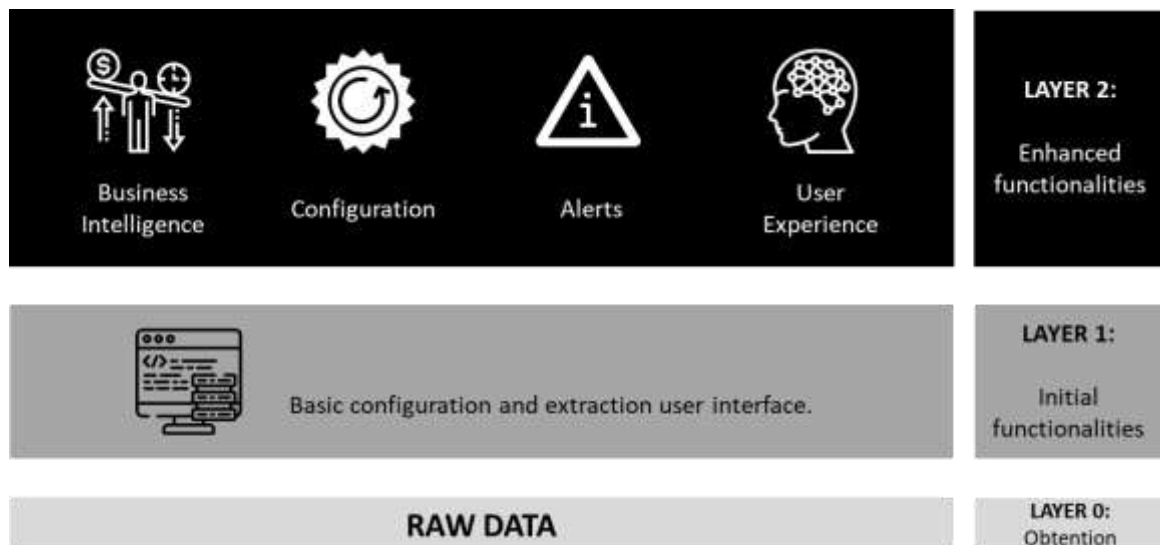


Figure 3. Functional architecture of the pilot

Document name:	D4.6 Final integration report on Industrial Services SME pilot				Page:	15 of 40	
Reference:	D4.6	Dissemination:	PU	Version:	1.1	Status:	Final

Since then, the pilot infrastructure has been enriched by adding a third layer (Layer 2), which provides the enhanced functionalities envisaged in the pilot conception stage. Basically, the user becomes an active asset in the protection of the infrastructure by managing security alarms and receiving update information of the three domains (IoT, gateway and cloud). Actually, this new layer enables the scenarios of the SMESEC framework tests within the Worldsensing’s infrastructure, as discussed in the next section.

3.3 Scenarios of SMESEC

The architecture developed for Pilot III is versatile enough to be easily adapted to many different applications and business verticals. In this sense, the final scenarios where the Loadsensing elements join the SMESEC framework suite can be translated to cover all those verticals demanding secure Operational Intelligence capabilities. Without seeking to be exhaustive, such a Loadsensing deployment is directly applicable in (i) the construction industry, (ii) mining and (iii) industrial monitoring processes, as clearly stated in the deliverable D4.5. According to these general remarks and independently of the specific business vertical, two different cases of application are identified at the moment.

3.3.1 Case 1: Infrastructure operator

From a practical viewpoint, Industrial IoT systems are commonly used by individuals with diverse profiles but generally a poor experience in cybersecurity area. They are usually infrastructure operators focusing on the OT dimension but without a genuine interest in IT. Hence, in this case, the system (pilot) is data oriented and only critical cybersecurity alarms are displayed, suggesting simple mitigation actions when incidences and attacks occur.



Figure 4. Data frontend view with structural information from the stadium

3.3.2 Case 2: Infrastructure and security manager

The preventive maintenance of any infrastructure makes necessary the active management of the OT domain without disregarding the IT-related information. This is particularly important if distributed

Document name:	D4.6 Final integration report on Industrial Services SME pilot				Page:	16 of 40	
Reference:	D4.6	Dissemination:	PU	Version:	1.1	Status:	Final

pieces of hardware and software coexist, and the communication is conducted through multiple methods and protocols.

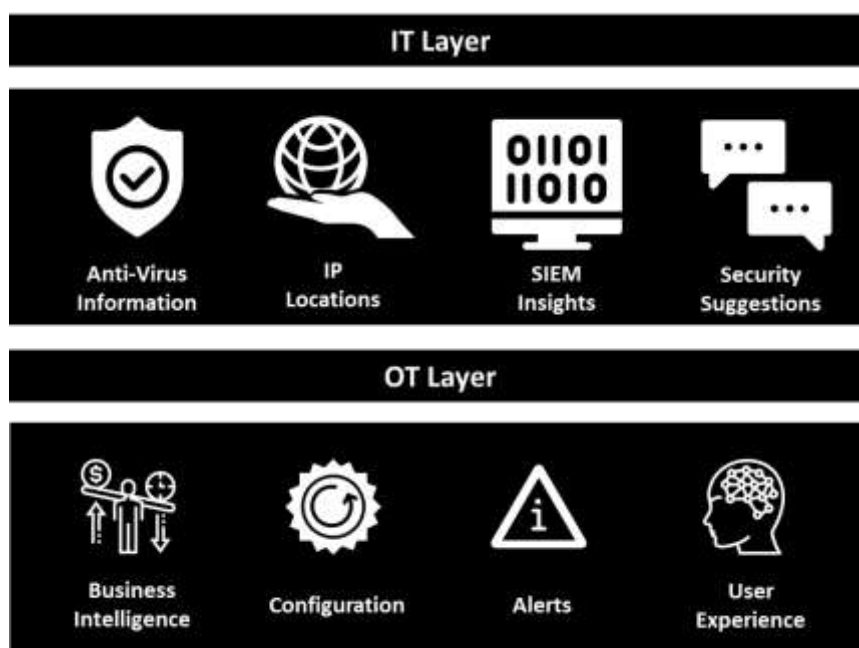


Figure 5. Pilot III (Industrial Services): IT and OT layers main items

In this case, the specialist user has full access to both the OT and IT domain through a unified tool to thus conduct comprehensive check-ups of the infrastructure status at any time. Besides, the system aggregates heterogeneous logs which are automatically processed by applying predefined business rules that automatically raise alarms and delivers contingency recommendations if an incident in one of the two domains is detected. This latest functionality is a strong point of the SMESEC framework since the inputs of different security solutions are correlated providing meaningful information to the end-user and a higher level of control of the whole infrastructure.

3.4 Impact of SMESEC in the use case

SMESEC has brought a significant improvement in the cybersecurity field, not only due to the adoption of some tools but thanks to the experience gained in the first two years of the project participation at company level. The main outputs achieved so far are described below.

3.4.1 Asset Inventory

An asset inventory is essential to keep control of any deployed infrastructure. Worldsensing has adopted the practice of collecting the information from the physical infrastructure deployed worldwide, which can be easily used in the event of a cybersecurity incident to thus restrict the potential and undesired derivative impact. Both a database and diagrams of the pilot's assets are available at the moment for Pilot III.

Document name:	D4.6 Final integration report on Industrial Services SME pilot				Page:	17 of 40	
Reference:	D4.6	Dissemination:	PU	Version:	1.1	Status:	Final

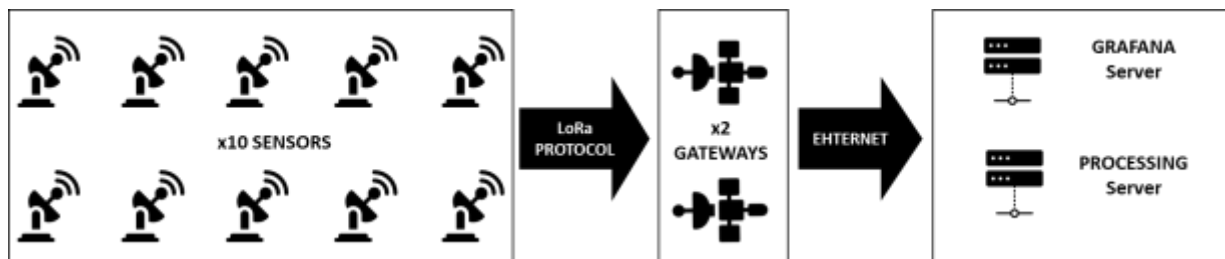


Figure 6. Pilot Asset Inventory: graphical representation

Device	Deployment ID	Device ID	Model	Status
Kerlink Gateway	WS Deployment	20040	LoRa IoT Station	Deployed
Kerlink Gateway	Secure Deployment	14112	LoRa IoT Station	Sent
Wireless Tiltmeter	WS Deployment	13525	LS-G6-INC15	Deployed
Wireless Tiltmeter	WS Deployment	13592	LS-G6-INC15	Deployed
Wireless Tiltmeter	WS Deployment	13629	LS-G6-INC15	Deployed
Wireless Tiltmeter	WS Deployment	13685	LS-G6-INC15	Deployed
Wireless Tiltmeter	WS Deployment	13937	LS-G6-INC15	Deployed
Wireless Tiltmeter	Secure Deployment	19097	LS-G6-INC15	Sent
Wireless Tiltmeter	Secure Deployment	19047	LS-G6-INC15	Sent
Wireless Tiltmeter	Secure Deployment	19081	LS-G6-INC15	Sent
Wireless Tiltmeter	Secure Deployment	19154	LS-G6-INC15	Sent
Wireless Tiltmeter	Secure Deployment	19167	LS-G6-INC15	Sent
Macallan Sever	WS Deployment	5.79.24.225	Linux Server	Deployed
Grafana Server	WS Deployment	162.13.144.202	Linux Server	Deployed

Figure 7. Pilot Asset Inventory: detailed information

3.4.2 Threat Modelling and Analysis

Once the assets infrastructure is fully understood and controlled by Worldsensing, the next step towards a secured system is to conduct a risk analysis. This is crucial to adopt safeguards seeking to minimize the most critical ones. In this sense, Worldsensing has implemented a detailed analysis considering the SMESEC tools security coverage as well as the new practices adopted by the company since the beginning of SMESEC.

Fortunately, the impact of the security countermeasures running at pilot level keeps the overall risk at low (Fig.8), and those concrete scenarios labelled as high or extreme have obtained the proper treatment (Fig.9).

Document name:	D4.6 Final integration report on Industrial Services SME pilot				Page:	18 of 40	
Reference:	D4.6	Dissemination:	PU	Version:	1.1	Status:	Final

IDENTIFIED ASSET	THREAT	PROBABILITY	CONSEQUENCE	SOCRE	SEVERITY
Kerlink Gateway (WS)	DOS [Denial of Service]	2	4	2.67	MEDIUM
Kerlink Gateway (WS)	MiMt [Man in the Middle]	1	4	1.33	VERY LOW
Kerlink Gateway (WS)	Remote Code Execution	3	4	4.00	HIGH
Kerlink Gateway (WS)	Brute force against authentication	3	3	3.00	MEDIUM
Kerlink Gateway (Secure)	DOS [Denial of Service]	2	4	2.67	MEDIUM
Kerlink Gateway (Secure)	MiMt [Man in the Middle]	1	4	1.33	VERY LOW
Kerlink Gateway (Secure)	Code injection	3	2	2.00	LOW
Kerlink Gateway (Secure)	Brute force against authentication	3	3	3.00	MEDIUM
Wireless Tiltmeter	Equipments robbery	2	4	2.67	MEDIUM
Wireless Tiltmeter	DOS [Denial of Service]	2	3	2.00	LOW
Wireless Tiltmeter	MiMt [Man in the Middle]	2	3	2.00	LOW
Wireless Tiltmeter	Administration errors	4	2	2.67	MEDIUM
Gateway Internet Connection	Service Down	2	4	2.67	MEDIUM
Gateway Internet Connection	Traffic sniffing	2	3	2.00	LOW
Gateway Internet Connection	Administration errors	3	3	3.00	MEDIUM
Macallan Sever	Use server as DDoS attacker	3	4	4.00	HIGH
Macallan Sever	Code injection	2	5	3.33	MEDIUM
Macallan Sever	DOS [Denial of Service]	2	4	2.67	MEDIUM
Macallan Sever	Unpatched OS or applications	4	4	5.33	EXTREME
Grafana Server	Use server as DDoS attacker	3	4	4.00	HIGH
Grafana Server	Cross site scripting	2	5	3.33	MEDIUM
Grafana Server	DOS [Denial of Service]	2	4	2.67	MEDIUM
Grafana Server	Unpatched OS or applications	4	4	5.33	EXTREME

Figure 8. Risk Assessment of Assets in Pilot III: severity overview

IDENTIFIED ASSET	THREAT	SOCRE	SEVERITY	RISK MANAGEMENT	ACTIONS
Kerlink Gateway (WS)	Remote Code Execution	4.00	HIGH	Transfer	Kerlink certifies their hardware and the robustness of their OS.
Macallan Sever	Use server as DDoS attacker	4.00	HIGH	Mitigate	Deploy monitoring solutions
Macallan Sever	Unpatched OS or applications	5.33	EXTREME	Mitigate	Deployed version is updated and patched.
Grafana Server	Use server as DDoS attacker	4.00	HIGH	Mitigate	Deploy monitoring solutions
Grafana Server	Unpatched OS or applications	5.33	EXTREME	Mitigate	Deployed version is updated and patched.

Figure 9. Risk Assessment of Assets in Pilot III: mitigation actions against critical risks

3.4.3 Monitoring (end-systems)

As a result of the risk analysis presented in the former section, it was concluded that high-risk assets can be correctly managed only through close monitoring of the pilot infrastructure as a whole. In this context, Worldsensing has deployed daemons in the servers that are constantly sending information to a centralized system with the aim to understand the global pilot status at any moment.

Document name:	D4.6 Final integration report on Industrial Services SME pilot				Page:	19 of 40	
Reference:	D4.6	Dissemination:	PU	Version:	1.1	Status:	Final

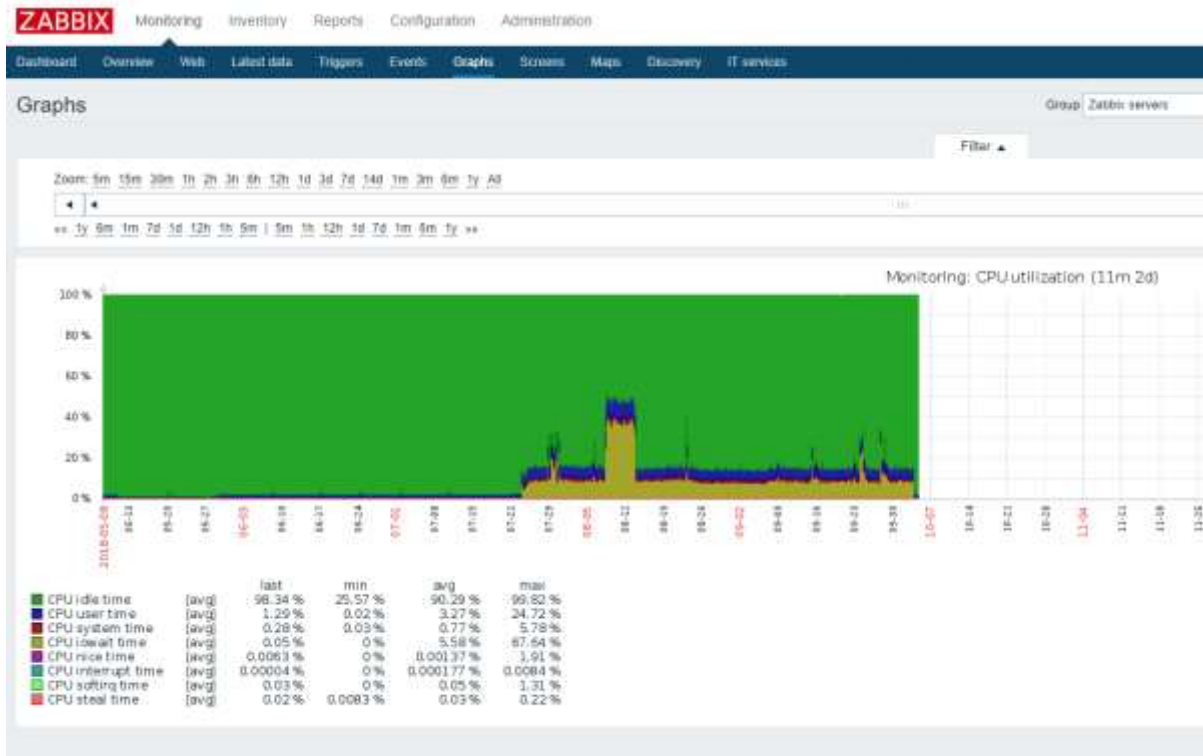


Figure 10. Monitoring tool: front-end server at Pilot III status

3.5 Business impact

No significant changes in the expected business impact already presented in the deliverable D4.5

Document name:	D4.6 Final integration report on Industrial Services SME pilot				Page:	20 of 40	
Reference:	D4.6	Dissemination:	PU	Version:	1.1	Status:	Final

4 Technical integration of SMESEC

4.1 Integration of SMESEC in the use case

The use case tested at Pilot III was initially conceived to incorporate at least one SMESEC tool in each of the Loadsensing domains. This approach aimed to validate the value proposition of the project in an end-to-end commercial IoT solution. Nevertheless, effective efforts have concentrated on the upper-edge part of the pilot architecture (gateway and cloud) after taking into account the risk analysis results (Chapter 3) and the nature of the different SMESEC solutions. Table 4 shows the list of the tools adopted in the pilot and the main contributions to the enriched Loadsensing functionalities, as well as the current integration status.

Pilot III: adopted tools			
Tools	Provider / partner	Purpose	Status
TaaS	EGM	Integrity checking of the infrastructure (LoRa)	Running
Anti-ROP	IBM	Passive protection of GWs	Running
NetScaler	CITRIX	Network traffic flow monitoring	Planned
XL-SIEM	ATOS	Events log management and anomaly detection	Running
GravityZone	Bitdefender	Antivirus and security logs generator at the cloud	Running
Honeypot	FORTH	Emulate pilot elements for attacks detection	Running (lab)
CYSEC	FHNW	Awareness and Training	Planned

Table 4. Adopted tools in the Pilot III (Industrial Services)

The breakdown of the pilot's threats against the expected protection coverage offered by the adopted solutions is shown below. Most of the identified challenges are significantly mitigated with the present pilot configuration.

IDENTIFIED ASSET	THREAT	PROBABILITY	Threats Protection					
			XL-SIEM (ATOS)	Anti-ROP (IBM)	Gravity Zone (Bitdefender)	Net Scaler (Citrix)	Honeypot (FORTH)	TaaS (EGM)
Kerlink Gateway (WS)	DOS (Denial of Service)	MEDIUM	X				X	
Kerlink Gateway (WS)	MMI (Man in the Middle)	VERY LOW						X
Kerlink Gateway (WS)	Code injection	HIGH		X				
Kerlink Gateway (WS)	Brute force against authentication	MEDIUM	X				X	
Kerlink Gateway (Secure)	DOS (Denial of Service)	MEDIUM	X				X	
Kerlink Gateway (Secure)	MMI (Man in the Middle)	VERY LOW						X
Kerlink Gateway (Secure)	Code injection	LOW		X				
Kerlink Gateway (Secure)	Brute force against authentication	MEDIUM	X				X	
Wireless Tiltmeter	Equipments robbery	MEDIUM						
Wireless Tiltmeter	DOS (Denial of Service)	LOW						X
Wireless Tiltmeter	MMI (Man in the Middle)	LOW						X
Wireless Tiltmeter	Administration errors	MEDIUM						
Gateway Internet Connection	Service Down	MEDIUM						
Gateway Internet Connection	Traffic sniffing	LOW						
Gateway Internet Connection	Administration errors	MEDIUM						
Macalan Sever	Brute force against authentication	HIGH	X		X	X	X	
Macalan Sever	Code injection	MEDIUM						
Macalan Sever	DOS (Denial of Service)	MEDIUM			X	X	X	
Macalan Sever	Unpatched OS or applications	CRITICAL	X		X			X
Grafana Server	Code injection	HIGH	X		X	X	X	
Grafana Server	Cross site scripting	MEDIUM						
Grafana Server	DOS (Denial of Service)	MEDIUM			X	X	X	
Grafana Server	Unpatched OS or applications	CRITICAL	X		X			X

Figure 11. Pilot's threats coverage by the adopted SMESEC solutions

Document name:	D4.6 Final integration report on Industrial Services SME pilot				Page:	21 of 40	
Reference:	D4.6	Dissemination:	PU	Version:	1.1	Status:	Final

If one goes into detail of Figure 10, it can be seen that the protection level offered by Net Scaler overlaps with that of Gravity Zone and the Honeypot (Fig.12). Thus, and with the aim to be effective, at this stage only the exploratory actions to integrate CITRIX's solution have been completed, while the effective installation within the pilot architecture will be done after M24. In fact, this tool can be considered in our case as a redundancy protection technology of the other two (antivirus and honeypot).

THREAT	PROBABILITY	Threats Protection		
		Gravity Zone (Bitdefender)	Net Scaler (Citrix)	Honeypot (FORTH)
DOS [Denial of Service]	MEDIUM			X
MiMt [Man in the Middle]	VERY LOW			
Code injection	HIGH			
Brute force against authentication	MEDIUM			X
DOS [Denial of Service]	MEDIUM			X
MiMt [Man in the Middle]	VERY LOW			
Code injection	LOW			
Brute force against authentication	MEDIUM			X
Equipments robbery	MEDIUM			
DOS [Denial of Service]	LOW			
MiMt [Man in the Middle]	LOW			
Administration errors	MEDIUM			
Service Down	MEDIUM			
Traffic sniffing	LOW			
Administration errors	MEDIUM			
Brute force against authentication	HIGH	X	X	X
Code injection	MEDIUM			
DOS [Denial of Service]	MEDIUM	X	X	X
Unpatched OS or applications	EXTREME	X		
Code injection	HIGH	X	X	X
Cross site scripting	MEDIUM			
DOS [Denial of Service]	MEDIUM	X	X	X
Unpatched OS or applications	EXTREME	X		

Figure 12. Overlap of Net Scaler functionalities with Gravity Zone and Honeypot

At this stage of the pilot development, the SMESEC tools have merged the Loadsensing architecture in a harmonious combination without interfering the Industrial services functionalities (Fig.13).

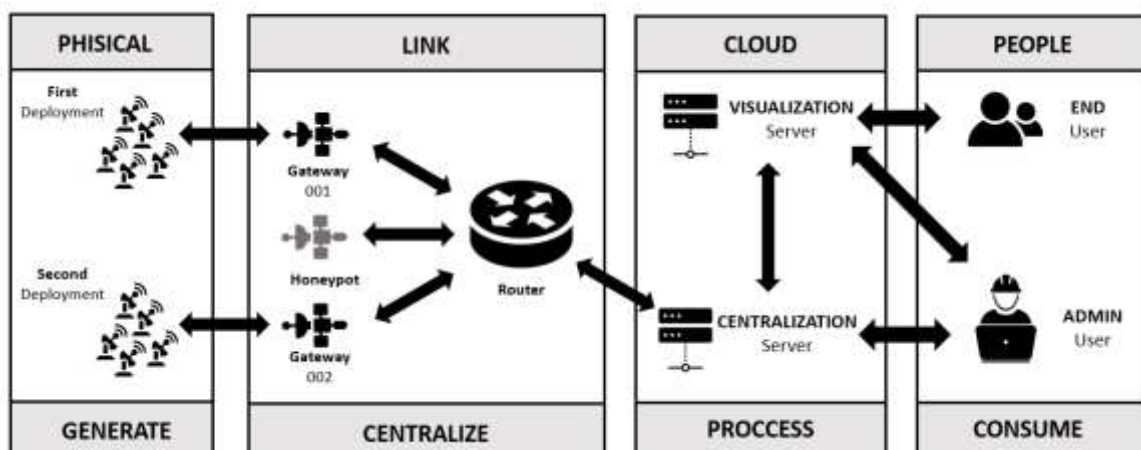


Figure 13. Information flow at the pilot's domains

Document name:	D4.6 Final integration report on Industrial Services SME pilot			Page:	22 of 40
Reference:	D4.6	Dissemination:	PU	Version:	1.1
				Status:	Final

For each of the pilot’s domains, at least one solution provided by the project partners has been adopted. It should be pointed out that the sensor layer has been modelled by the testing service offered by EGM, shedding light on potential vulnerabilities of the data loggers. This is a key point to define a path of continuous improvement of the existing technology in Worldensing’s internal technology roadmap. On the other hand, the CYSEC tool offered by FHNW is, in fact, a three-domain contributor, since it raises the cybersecurity awareness from a global perspective. The CYSEC tool is used in the context of the use case, being available at the cloud and accessible through the SMESEC framework frontend. The network administrator has access to CYSEC, does cybersecurity self-assessment, sees the recommendations (in the specific area based on the priorities), and communicates with the relevant staff in the company. Since the solution provides holistic SME-specific training and awareness content (cloud-based or on-premise) for do-it-yourself cybersecurity assessment and capability improvement, it can integrate into the work process to improve the SME solution.

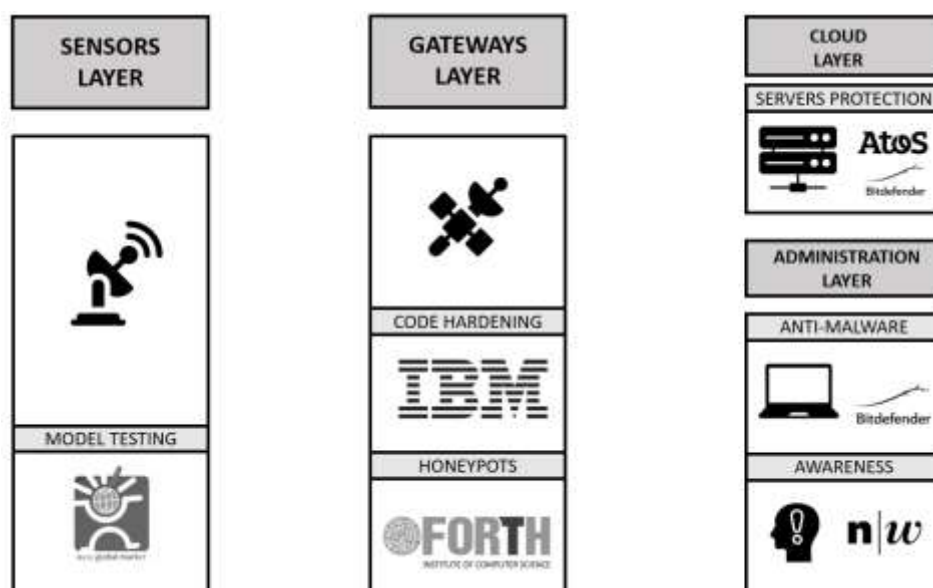


Figure 14. Matching between SMESEC tools and Pilot III domains

4.2 Analysis and evaluation of SMESEC

In the following lines, a more detailed analysis of the integration of SMESEC in Loadsensing is given. The work done with the different tools and the framework as a whole is reviewed to provide a comprehensive and full picture of the attained results at the moment.

4.2.1 Test as a Service [TaaS]

EGM TaaS is an online testing solution where users can setup their System Under Test (SUT) configuration and launch test execution without any manual installation on the machine itself. End users can define the configuration through a web application and select which test cases should run.

Document name:	D4.6 Final integration report on Industrial Services SME pilot				Page:	23 of 40	
Reference:	D4.6	Dissemination:	PU	Version:	1.1	Status:	Final

TaaS will then produce readable reports in the web interface containing statistics, reports about test failures, and other useful information. It is based on Travern Tool² for the generation of test cases and the platform allows to perform multiple types of test, for instance: API testing and Lora testing.

In the case of the LoRa testing, relevant service for Pilot III, the TaaS is designed to play the role of the Network Server and Application Server while interacting with an end device. As shown in Figure 15, the end device is running the LoRaWAN Implementation Under Test (IUT) and the user must provide a compliant LoRA gateway running a packet forwarder.

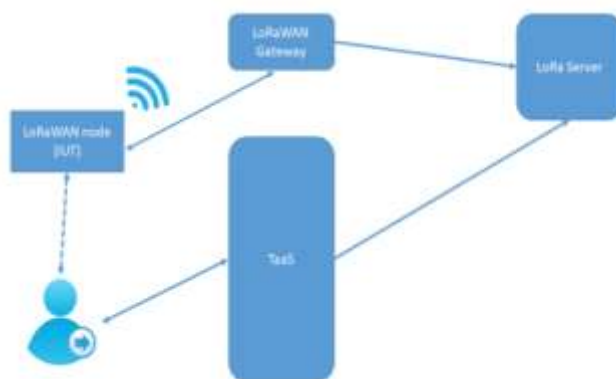


Figure 15. LoRaWAN test set-up

From a practical point of view, as the TaaS is a web service, Worldsensing does not need any implementation or integration of the tool in the pilot infrastructure, but only connect a gateway to EGM LoRa Server. The user needs then to navigate to the “LoRa Testing” section in the TaaS GUI. An instruction page shows up providing a brief explanation for the different LoRa connection types. The user needs to choose the appropriate one based on the selected LoRa implementation, ABP in the case of Worldsensing.



Figure 16 LoRa testing configuration page (ABP)

² <https://tavernesting.github.io/>

Document name:	D4.6 Final integration report on Industrial Services SME pilot			Page:	24 of 40
Reference:	D4.6	Dissemination:	PU	Version:	1.1
				Status:	Final

Figure 16 shows the Lora configuration webpage: the user needs to provide the appropriate information related to the device based on the effective connection type (i.e, Device Appkey and DevEUI for ABP connection).

4.2.2 Return-Oriented Programming Blocker [Anti-ROP]

Anti-ROP integration in the gateway was already completed at M18. Lab tests demonstrated that this endpoint device could be effectively protected against ROP and memory corruption attacks. Further details were given in the deliverable D4.5.

Since then, a second gateway has been prepared with the IBM technology and sent to Patras (Greece) to duplicate the pilot infrastructure. This should enable the validation of Anti-ROP capabilities in a real environment during the test campaign (WP5) by running the same proofs successfully completed in Haifa (Israel) a few months ago.

4.2.1 System Information and Events Manager [XL-SIEM]

The XL-SIEM in the Pilot III was envisaged as a log gatherer, processor and analyzer of the main cybersecurity events occurring at the Loadsensing infrastructure. With the help of a set of automatic alarms, incidences are early detected to facilitate infrastructure management and later processing and analysis. Apart from the first deployment already presented in the deliverable D4.5, at M24 the connection between the tool and the Gravity Zone has been stabilized as well as the reporting capabilities of the tool. Further details are given in the next sections.

4.2.2 Malware Prevention System [Gravity Zone]

Gravity Zone integration in the pilot was already completed at M18, as explained in the deliverable D4.5. Since then, some functional tests have been conducted to validate continuous and stable operation. Generated logs are now automatically sent to the XL-SIEM through a dedicated agent installed in Worldensing’s cloud infrastructure, as shown in Figure 17.

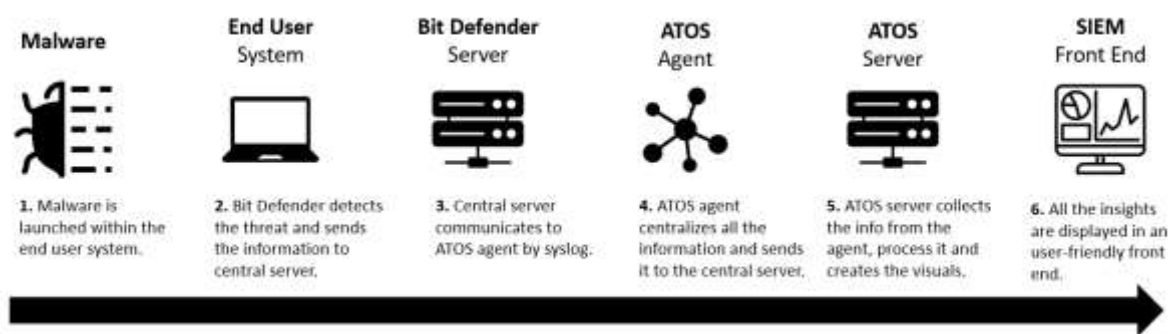


Figure 17. Loadsensing, Gravity Zone and XL-SIEM integration scheme

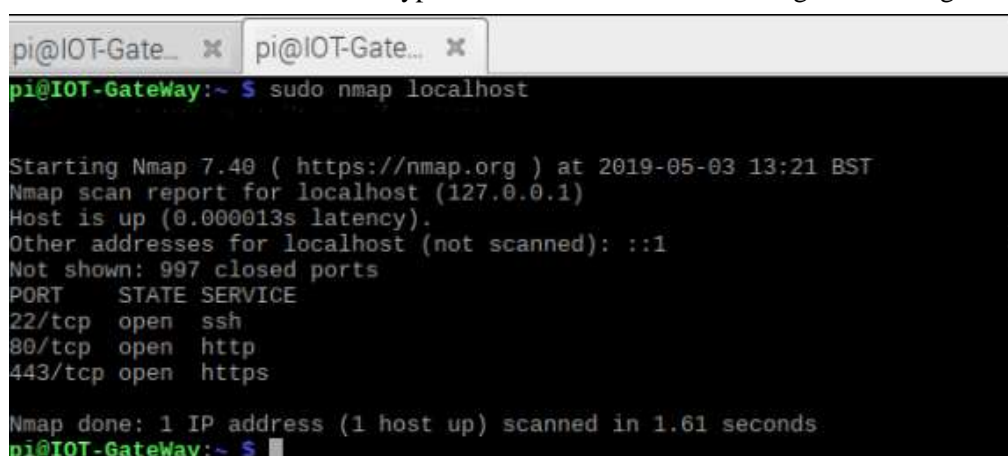
Document name:	D4.6 Final integration report on Industrial Services SME pilot			Page:	25 of 40
Reference:	D4.6	Dissemination:	PU	Version:	1.1
				Status:	Final

4.2.3 NetScaler

As explained in the deliverable D4.5, NetScaler solution has been tested in a separated machine installed on Worldsensing’s premises. On the other hand, CITRIX has adapted the installation supporting documentation so that the solution can be easily installed in Google Cloud infrastructure when needed. Initially, the installation guide was intended for AWS only. Full deployment of the solution will be completed beyond M24.

4.2.4 Honeypot

A honeypot is a device that pretends being vulnerable to different types of attacks. It is used as a lure for both internal and external malicious actors to thus early identify potential attacks. This functionality is interesting enough for Pilot III, and consequently, it has been adopted in the second release of the use case. In particular, the honeypot emulates the gateway of the Loadsensing architecture. To accomplish this, a modified version of a cowrie³ honeypot emulates the services running in the real gateway.



```

pi@IoT-GateWay:~$ sudo nmap localhost

Starting Nmap 7.40 ( https://nmap.org ) at 2019-05-03 13:21 BST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000013s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 1.61 seconds
pi@IoT-GateWay:~$

```

Figure 18. Honeypot emulation of IoT services (screenshot)

If any attacker attempts to connect/compromise the “emulated honeypot gateway”, the infrastructure manager is immediately notified of the event, and the system logs all the interactions between the honeypot and the malicious actor and send them to the XL-SIEM.

The honeypot logs include all the connection details, the complete shell interaction of the attacker and any downloaded binaries from the emulated environment. To that end, the well-known network scanner, Nmap⁴, useful to map the replicated services, runs in the honeypot, which after all may result as a key element to divert attacks from the real gateway.

³ <https://github.com/cowrie/cowrie/>

⁴ <https://nmap.org/>

Document name:	D4.6 Final integration report on Industrial Services SME pilot				Page:	26 of 40	
Reference:	D4.6	Dissemination:	PU	Version:	1.1	Status:	Final

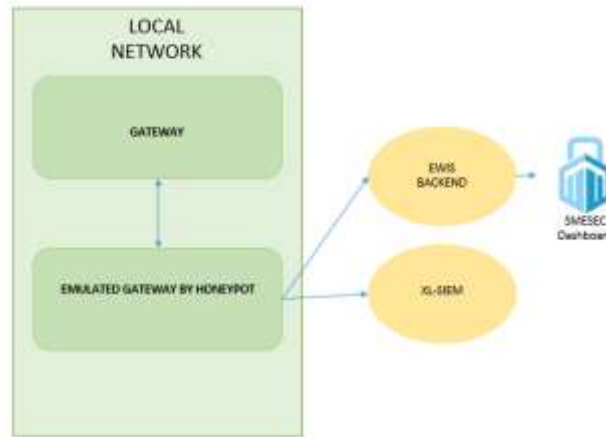


Figure 19. Honeypot architecture and integration within SMESEC architecture

4.2.5 SMESEC Extensions [Recommendation Engine]

The SMESEC framework is expected to be more than just the sum of different security solutions. On the contrary, the final architecture of the whole system (Fig.20) has several modules to correlate heterogeneous data inputs and to ease the management of the SMEs assets. Providing fine details about them are out of the scope of this document and they will be explained elsewhere [WP3].

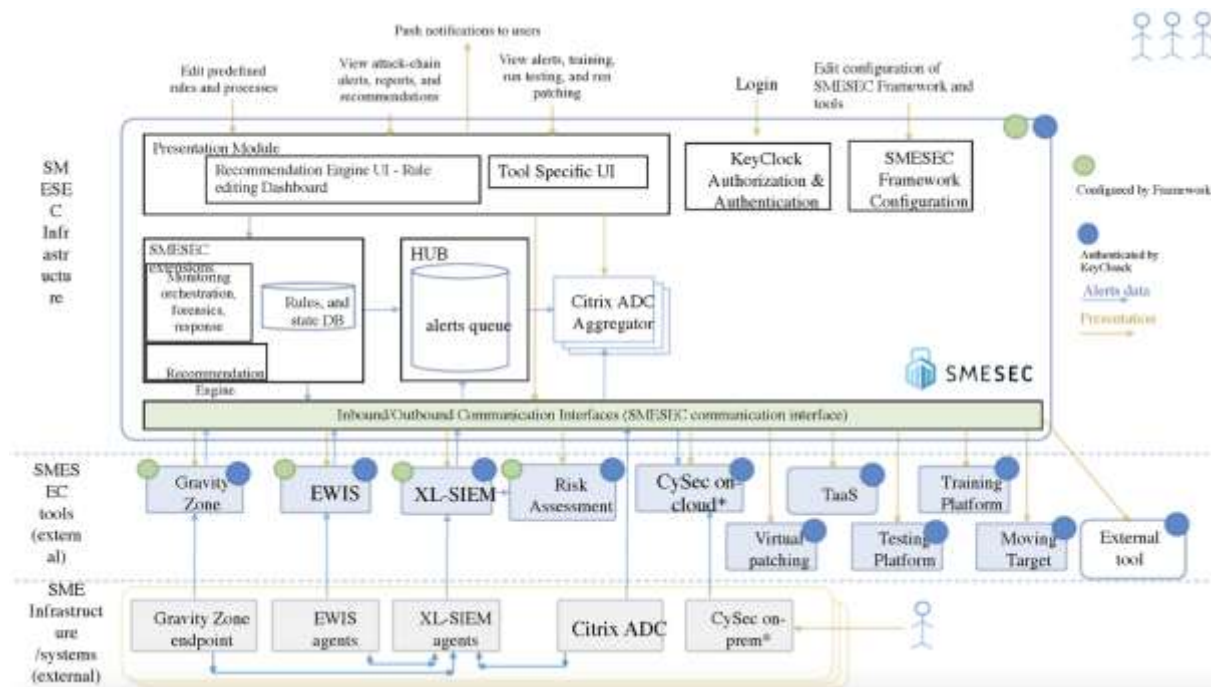


Figure 20. Honeypot architecture and integration within SMESEC architecture

In particular and regarding Pilot III, a key element is the so-called alert and recommendation engine. This module ingests data coming from different SMESEC security solutions and correlates them by applying pre-defined business rules that rise alerts and recommendations to the end user. At this moment, the system is ready for the practical use and preliminary proofs are running at lab level.

Document name:	D4.6 Final integration report on Industrial Services SME pilot			Page:	27 of 40
Reference:	D4.6	Dissemination:	PU	Version:	1.1
				Status:	Final

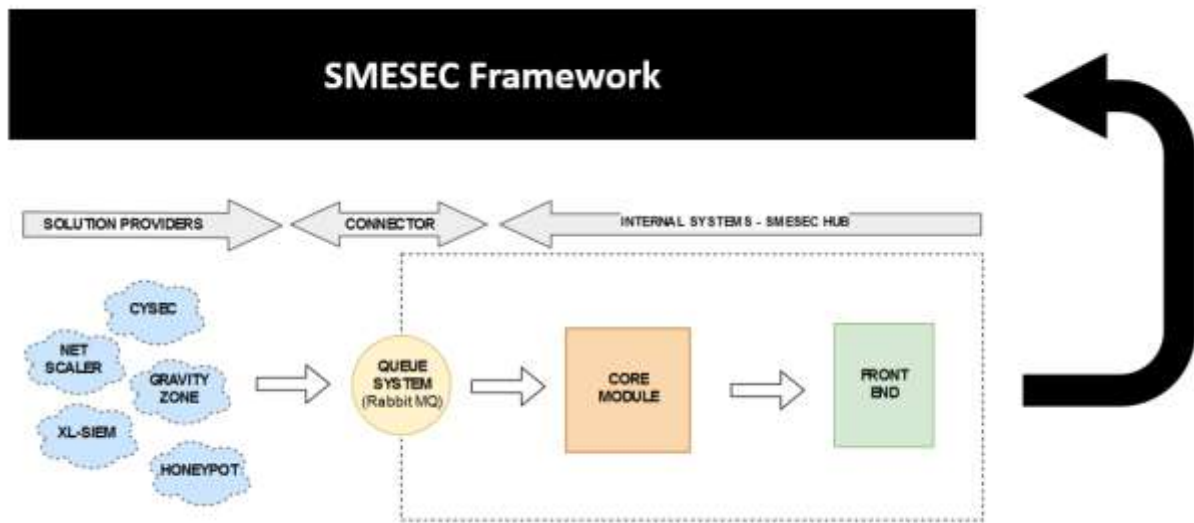


Figure 21. SMESEC Recommendation Engine. General architecture

4.2.6 SMESEC Awareness Tool [CYSEC]

Some Worldsensing selected employees have been subject to the CYSEC test, specifically designed to identify the strengths and weaknesses in cybersecurity at company level. The outputs will be used to determine the level of match between Worldsensing internal policies and the standard practices in the sector.

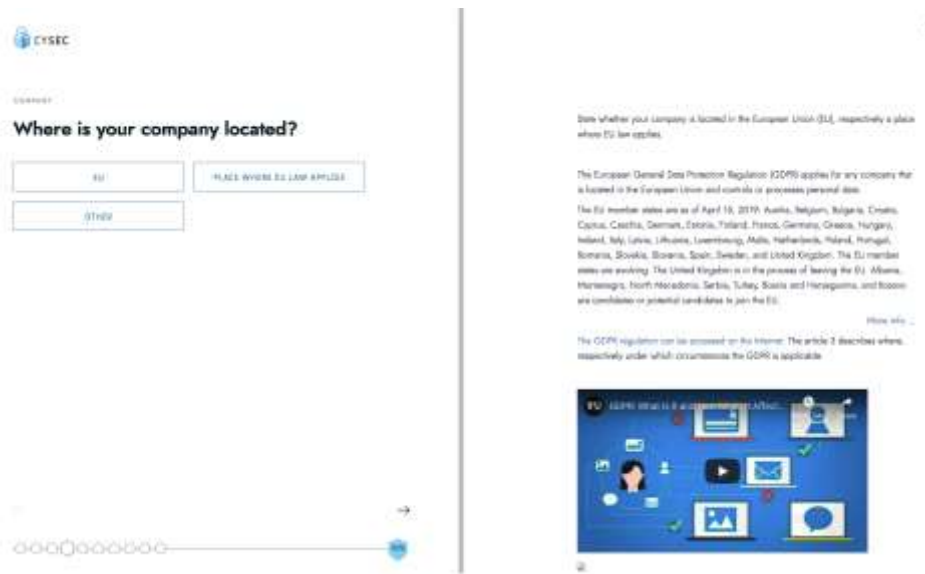


Figure 22. CYSEC tool: screenshot of one of the filled forms

Document name:	D4.6 Final integration report on Industrial Services SME pilot				Page:	28 of 40	
Reference:	D4.6	Dissemination:	PU	Version:	1.1	Status:	Final

4.3 Testing and feedback provided

From M18 to M24, the main tests performed have concentrated on demonstrating the functionality of each one of the modules outlined in the former section. It should be pointed out that SMESEC framework tests will be conducted in the frame of WP5, and here only the operational validation of the different tools has been searched. In the following lines, a detailed description of the work done so far per security solution is presented.

The general impression that comes out of this activity is that the pilot is ready for the systematic pilot campaign running from M24 on.

4.3.1 Test as a Service [TaaS]

As mentioned in a previous section, the user needs to introduce the configuration of the device on the TaaS GUI. The TaaS generates a report about failures based on the described test cases: Join Request, Confirmed packets, unconfirmed uplink, Ping Pong.

Figure 23 shows an example of the first generated reports in the case of “LoRa testing”. Results to date are encouraging.

Test Case	Verdict	Observations
Join Request	PASS	ABP
Confirmed packets	PASS	ABP
Unconfirmed uplink	PASS	ABP
Ping Pong	PASS	ABP

Figure 23. TaaS report on LoRa

4.3.2 Return-Oriented Programming Blocker [Anti-ROP]

No additional tests to those reported in the deliverable D4.5.

4.3.3 System Information and Events Manager [XL-SIEM]

Worldsensing infrastructure was already reporting events to the XL-SIEM at M18. Logs generated by Gravity Zone have been acquired for last six months with the aim to validate both the system and the connection stability. Results to date are encouraging.

Document name:	D4.6 Final integration report on Industrial Services SME pilot				Page:	29 of 40	
Reference:	D4.6	Dissemination:	PU	Version:	1.1	Status:	Final



Figure 24. XL-SIEM frontend. General indicators of Pilot III

4.3.4 Malware Prevention System [Gravity Zone]

Worldsensing infrastructure (cloud and some selected computers) have been monitored by Gravity Zone for roughly one year now. Apart from the expected functionalities that allows protecting the pilot servers in an efficient way, the tool also provides aggregated figures of the attacks and incidences attempts that have occurred in the period. This later information can be useful to rethink internal security policies in Worldsensing.



Figure 25. Gravity Zone. Overall figures of the monitored infrastructure



Figure 26. Gravity Zone. Malware detection and deletion

Nevertheless, the main efforts have concentrated on the effective interconnection between Gravity Zone and XL-SIEM. At the time of this writing, logs generated by the antivirus automatically arrive in the tool, generating a rich database useful for raise alarms in real time and if necessary, perform forensic analysis in case that an attack occurs.

Document name:	D4.6 Final integration report on Industrial Services SME pilot			Page:	30 of 40
Reference:	D4.6	Dissemination:	PU	Version:	1.1
				Status:	Final

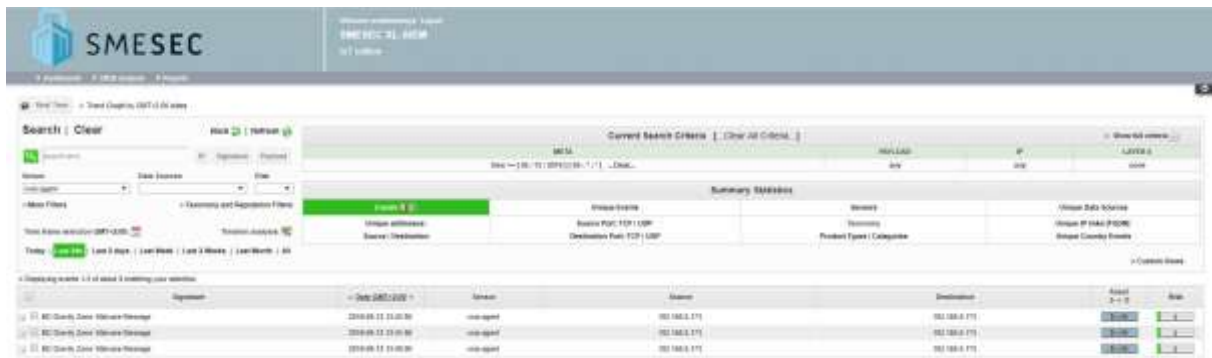


Figure 27. Gravity Zone and XL-SIEM integration. (Up) General logs repository. (Down) Detailed information of one of the security events.

4.3.5 NetScaler

Not applicable

4.3.6 Honeypot

At present, FORTH has set up a test environment similar to that of the Pilot III and performed various attacks originating from (i) the same and (ii) an external network. It was verified that these attacks were logged in the EWIS backend databases, as it is depicted in Figure 28. FORTH also made sure that the honeypot implementation is plug-and-play for easier integration with the rest of the pilot elements and it reinitializes correctly upon reboot.

Document name:	D4.6 Final integration report on Industrial Services SME pilot				Page:	31 of 40	
Reference:	D4.6	Dissemination:	PU	Version:	1.1	Status:	Final


```
mysql> select * from input;
+-----+-----+-----+-----+-----+-----+
| id | session | timestamp | realm | success | input |
+-----+-----+-----+-----+-----+-----+
| 1 | dc5c4bd0d31e | 2019-05-09 12:42:37 | NULL | 1 | ls -la |
| 2 | dc5c4bd0d31e | 2019-05-09 12:42:38 | NULL | 1 | exit |
| 3 | ebfc95703bfe | 2019-05-10 12:34:40 | NULL | 1 | iname -a |
| 4 | ebfc95703bfe | 2019-05-10 12:34:40 | NULL | 0 | iname -a |
| 5 | ebfc95703bfe | 2019-05-10 12:34:58 | NULL | 1 | uname -a |
| 6 | ebfc95703bfe | 2019-05-10 12:35:07 | NULL | 1 | uname -r |
| 7 | ebfc95703bfe | 2019-05-10 12:35:24 | NULL | 1 | cat /etc/passwd |
+-----+-----+-----+-----+-----+-----+
7 rows in set (0.00 sec)

mysql> select * from auth;
+-----+-----+-----+-----+-----+-----+
| id | session | success | username | password | timestamp |
+-----+-----+-----+-----+-----+-----+
| 1 | dc5c4bd0d31e | 0 | root | 12345678 | 2019-05-09 12:42:28 |
| 2 | dc5c4bd0d31e | 1 | root | 123456 | 2019-05-09 12:42:33 |
| 3 | 30b645f24751 | 0 | pi | 123456 | 2019-05-10 12:32:35 |
| 4 | 30b645f24751 | 0 | pi | 12345678 | 2019-05-10 12:32:42 |
| 5 | ebfc95703bfe | 0 | root | 12345678 | 2019-05-10 12:33:37 |
| 6 | ebfc95703bfe | 1 | root | 123456 | 2019-05-10 12:33:45 |
+-----+-----+-----+-----+-----+-----+
6 rows in set (0.00 sec)
```

Figure 28. Database with log interaction towards the honeypot

```
pi@IoT-GateWay:~$ ssh root@localhost
root@localhost's password:
Permission denied, please try again.
root@localhost's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@IoT-GW:~# iname -a
-bash: iname: command not found
root@IoT-GW:~# uname -a
Linux IoT-GW 3.2.0-4-amd64 #1 SMP Debian 3.2.68-1+deb7u1 x86_64 GNU/Linux
root@IoT-GW:~# uname -r
3.2.0-4-amd64
root@IoT-GW:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
```

Figure 29. Successful attack example from IOT-Honeypot

In Figure 28, we can see a sample of the logs stored in the EWIS database: the auth table displays all the connection attempts towards the honeypot successful or not, and in the input table we can see all the commands executed inside the honeypot by successful attackers.

Figure 29 shows an example of a successful attack and get a glimpse of what the attacker sees when she successfully connects to the honeypot. The honeypot console appears like a real IoT-GW console tricking the attacker into believing they have compromised the production gateway.

Document name:	D4.6 Final integration report on Industrial Services SME pilot				Page:	32 of 40	
Reference:	D4.6	Dissemination:	PU	Version:	1.1	Status:	Final

4.3.7 SMESEC Extensions [Recommendation Engine]

Preliminary tests at lab level operated only through console commands have been completed to validate the functionality of the first set of business rules. At the moment, the system functionality is quite limited and just proof-of-concept alarms have been successfully implemented, such as the detection of an anomalous IP address attempting to access the Pilot cloud or a disproportionate use of CPU resources. Further details about SMESEC Extensions are given in WP3 deliverables.

4.3.8 SMESEC Awareness Tool [CYSEC]

Finally, and as stated in former sections, CYSEC questionnaires have been filled by some WorldSensing employees. FHNW is expected to provide the full analysis of the results in the coming days at the time of this writing. Preliminary results show however the following findings:

- The self-assessment questionnaires (CYSEC coaches) and produced recommendations need to be presented in an easy-to-understand way;
- The assessment questionnaires and recommendations need to be adapted to the use case partner's needs;
- User privacy perception should be satisfied to improve the tool adoption intention.



Figure 30. CYSEC: screenshot of the questionnaires

Document name:	D4.6 Final integration report on Industrial Services SME pilot				Page:	33 of 40	
Reference:	D4.6	Dissemination:	PU	Version:	1.1	Status:	Final

5 Cybersecurity awareness and training

5.1 Training and awareness

As stated in D4.5, up to 70% of the external attacks in organizations are directly or indirectly employee-made situations. This means that the human factor is the weakest link of the cybersecurity chain, and therefore, the continuous training and awareness campaigns to the employees is a necessary good practice in any company. In this sense, well-designed security awareness programs contribute to an adequate level of cybersecurity knowledge of the staff and instill accountability principles within organizations.

Alongside the implementation of SMESEC, Worldsensing is moving from a start-up with a high appetite for risk to a consolidated company with defined internal processes. In this path, a dedicated Security Awareness Plan beyond the pilot was envisaged at the beginning of SMESEC, made up of small and delimited projects grouped in three different areas:

- Classification of employees to conduct specific training actions;
- Improving cybersecurity by covering critical aspects of the different phases of the security cycle (attacks). Alignment of the internal processes to the demanding legal general framework (i.e. GDPR and NIST directive), and;
- Feedback analysis and continuous improvement of the ongoing actions.

As far as the grouping of employees goes, Worldsensing has first targeted those profiles and roles with special training requirements due to their potential criticality (Table 4), while the rest are continuously subject to a generic training program described down below (Table 5).

Training and awareness plan: targeted employees	
Group	Objective / Rationale
C-Level	Sensitization of cybersecurity importance. Internal project prioritization
Department managers	Cascade effect. General awareness. Risk assessment (compliance)
Privileged users	Specific needs due to the sensitive data they handle (i.e. IT, HR)
Engineering Dpt	Security by default principles: good practices during development
Legal Dpt (i.e. DPO)	Alignment of policies and processes with the legal framework
Third Parties	Information of the security policies and standards within WS

Table 5. Training and awareness plan: targeted employees

Training and awareness plan: general sessions	
Session	Objective / Rationale
On-boarding	Kick-off during the first days in the company. General cybersecurity principles presented
Periodic	Topic-oriented sessions. Continuous training approach
Post-incident	Special events to discuss about lessons-learned and next actions to be implemented

Table 6. Training and awareness plan: general training sessions at Worldsensing

Document name:	D4.6 Final integration report on Industrial Services SME pilot			Page:	34 of 40
Reference:	D4.6	Dissemination:	PU	Version:	1.1
				Status:	Final

From M18 to M24, the training actions addressed to all employees has become more systematic, actively involving different departments. In fact, at this point, several activities are running in parallel, such as a fast and well-established on-boarding sessions addressed to the new personnel, topic-oriented seminars opened to all employees (i.e. GDPR workshop led by external advisors), and targeted recommendations campaigns after specific incidences (i.e. notebook theft outside Worldsensing’s offices). On the other hand, the endeavor of the Cybersecurity Manager of the company, Mr. Olmo Rayón, to make key managers aware of developing tools to effectively respond to potential attacks during their different phases (prevention, detection and response) has borne fruit in the form of new policies and processes that are duly followed at company level.

Regarding the technical measures specifically designed for increasing the security level of the whole company, it is noteworthy to say that all of them, which had already been outlined at M18 (D4.5), continue to evolve. In fact, with the aim to build up a robust ISMS capable of minimizing risk and ensure business continuity in the event of a security breach, these measures are envisaged for a slow but progressive implementation still far from complete (Table 6). Nevertheless, and despite some of them are slightly delayed with respect to the initial time schedule, such as the phishing campaign, the overall result is fairly positive. Actually, in less than two years, Worldsensing has implemented a system sufficient to be certified to ISO27001. In this sense, the certification renewal is scheduled in September 2019, when most of the weaknesses detected by auditors are expected to be corrected. All in all, we can without a shadow of doubt say that SMESEC has acted as catalyst agent for change in Worldsensing, raising interest and awareness of cybersecurity among the employees.

Training and awareness plan: technical measures		
Measure	Objective / Rationale	Status at M24
Policies	Procedures to respond to specific scenarios. Alignment with ISO27001 requirements	Completed.
MFA	Double authentication through mobile phone in some systems	Completed
Phishing	Simulation of a phishing campaign and analysis of the results	Pending
Social engineering	Simulation of attacks usually done through apparently harmless questions. Analysis of the results	Pending
Mobile devices	Proper monitoring of mobile devices with company data	Completed
Backups	Regular backups of the company's assets	Completed
Remote working	Measures to keep remote working compatible with security principles	Pending
Antivirus	Adoption of an endpoint antivirus software. Training to understand those notifications the software provides	Completed
Passwords	Adoption of a password manager (LastPass). Training.	Completed
GDPR	Introduction of privacy by design principles at company level	Partially achieved
	Audit of commercial products	Completed

Table 7. Training and awareness plan: technical measures implemented at WS with associated training

Document name:	D4.6 Final integration report on Industrial Services SME pilot				Page:	35 of 40	
Reference:	D4.6	Dissemination:	PU	Version:	1.1	Status:	Final

6 Conclusions

6.1 Final analysis and next steps

The “Industrial Services” pilot was initially conceived by Worldsensing as a proof-of-concept use case to validate the feasibility of adding cybersecurity capabilities to a standard IoT deployment without jeopardizing the key features demanded by the market, such as easy use and affordability of the IoT systems. Based on Worldsensing’s previous experience, a real infrastructure was selected to complete and assess a real deployment of Loadsensing proprietary technology actively protected by the SMESEC framework.

In this way and adopting an eminently practical approach, the project outputs can be tested in different real scenarios, facing the same daily problems of any other Worldsensing infrastructure and simulating new ones (WP5). This will be extremely useful to gain meaningful and multifaceted insight into the potential overhead derived from adopting the SMESEC tools.

Having said that, it can be asserted that the pilot has allowed fulfilling the expected results, responding to the initial requirements except those initially targeted to the IoT domain since they are not specifically covered by SMESEC solutions. At the time of this writing, the selected SMESEC tools have been adopted within the Loadsensing architecture and they are ready to be tested in the frame of WP5. In fact, the challenge ahead us is to validate that the framework can work in an orchestrated way providing a clear added value to the current commercial solution.

6.2 Fulfillment of objectives

The main objective of the Pilot III was the practical implementation of the SMESEC framework in industrial IoT systems, addressing the defiance of adapting a generic security solution to the specificities of this market niche. Two of the three domains (gateway and cloud) of the Loadsensing architecture have been secured through the adoption of specific tools, providing meaningful inputs to the infrastructure operators, who are typically poorly trained in the cybersecurity field.

Besides, the SMESEC framework actively correlates different events inputs to raise IT alarms that complement the OT warnings that are already gathered by the Loadsensing system. Despite this last function is still at the development stage and further work is necessary to achieve the desired level required in the production stage, the first tests have shown promising results, which will need to be confirmed in the frame of WP5 activity.

6.3 Future outcomes and business development

SMESEC is the first project within Worldsensing that delivers a clear added value in the cybersecurity field. IoT technologies have usually overlooked this aspect, and this unique opportunity to enrich our products with a flexible security framework was early identified as a business opportunity already in the proposal phase.

Document name:	D4.6 Final integration report on Industrial Services SME pilot				Page:	36 of 40	
Reference:	D4.6	Dissemination:	PU	Version:	1.1	Status:	Final

For Worldsensing, the business development proposition linked to SMESEC is twofold. On the one hand, the whole Loadsensing infrastructure will become incident covered thanks to the adoption of standard cybersecurity tools. This undoubtedly increases the resilience of the system to attacks, even if the operators are not experts, increasing the goal price of Loadsensing hardware and hopefully the market penetration.

On the other hand, the SMESEC framework also paves the way towards the deployment of a robust Public Warning System (PWS) capable of discerning between OT and IT alarms and events. This is a crucial differentiating factor in the IoT business if Worldsensing aims to offer a reliable business intelligence service for infrastructure monitoring. Helping the system administrator to validate between true and false positives linked to the health of critical infrastructures is crucial to provide an optimal service, which presumably will reach the market in the form of a SaaS.

Document name:	D4.6 Final integration report on Industrial Services SME pilot				Page:	37 of 40	
Reference:	D4.6	Dissemination:	PU	Version:	1.1	Status:	Final

References

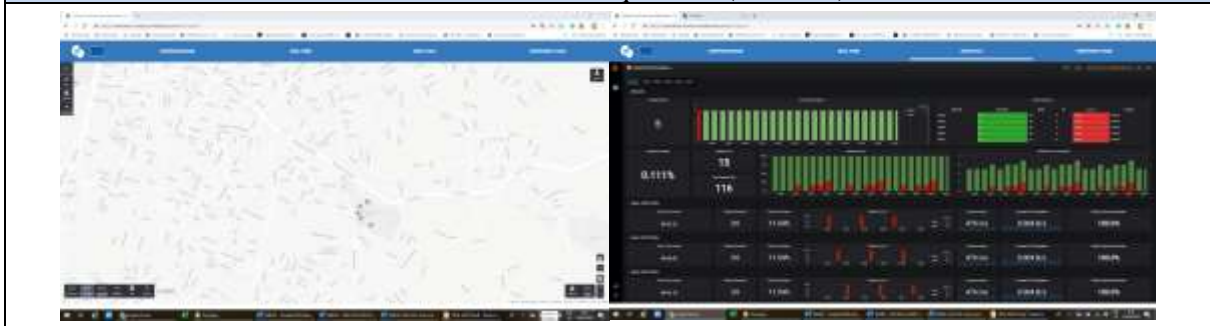
- [1] SMESEC. D2.1 - SME security characteristics description, security and market analysis report. George Oikonomou. 2017
- [2] SMESEC. D4.5 – Final integration report on Industrial Services SME pilot. Francisco Hernández-Ramirez. 2018
- [3] SMESEC. D3.3 – Final Version of the SMESEC security framework Unified Architecture. Fady Copt. 2019

Document name:	D4.6 Final integration report on Industrial Services SME pilot				Page:	38 of 40	
Reference:	D4.6	Dissemination:	PU	Version:	1.1	Status:	Final

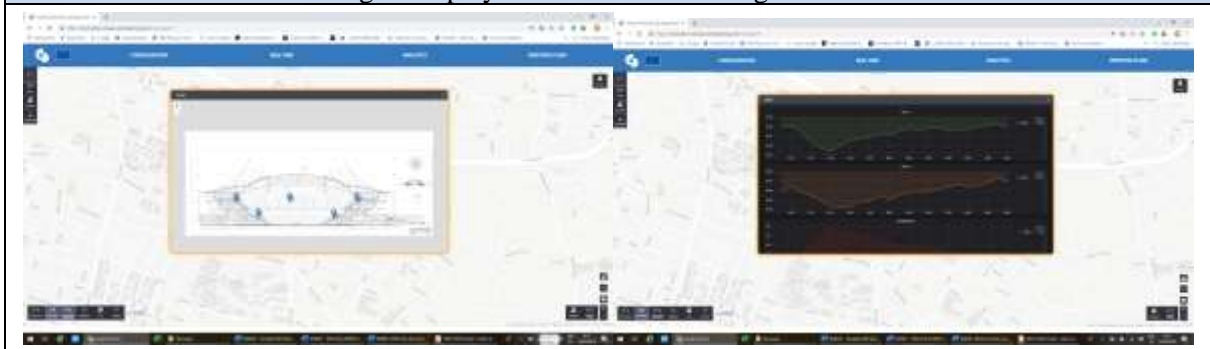
Annexes

The Loadsensing instance for the pilot has been hardened and stabilized from M18 to M24. The Worldsensing data platform (OneMind) is now ready to incorporate some of the SMESEC functionalities once the project is over.

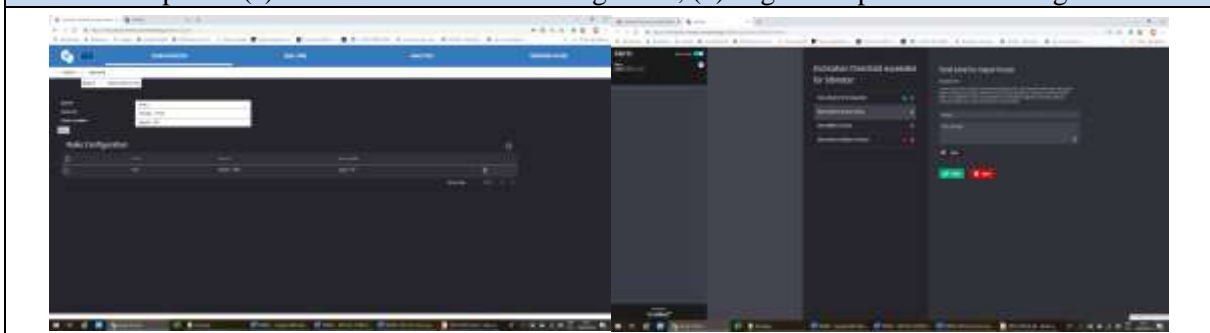
(Left) General view of Patras with the sensors displayed at the stadium. (Right) Analytics dashboard with KPIs on data acquisition (real time)



Structural data acquisition at the Pilot III: (a) Left: sensors layout in the stadium infrastructure. (b) Right: displayed data of Loadsensing tiltmeters



Alarm panel: (a) Left: Business Rules configurator, (b) Right: Response Plan configurator



Document name:	D4.6 Final integration report on Industrial Services SME pilot				Page:	39 of 40	
Reference:	D4.6	Dissemination:	PU	Version:	1.1	Status:	Final

[END OF THE DOCUMENT]

Document name:	D4.6 Final integration report on Industrial Services SME pilot				Page:	40 of 40	
Reference:	D4.6	Dissemination:	PU	Version:	1.1	Status:	Final