



SMESEC

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

D4.5 Preliminary Integration report on Industrial Services SME pilot

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

Related WP	WP4	Document Reference	D4.5
Related Deliverable(s)	D2.1, D3.1	Dissemination Level (*)	PU
Lead Organization	WoS	Lead Author	Francisco Hernández-Ramírez
Contributors	Francisco Hernández-Ramírez (WoS)	Reviewers	José Fran. Ruíz (Atos)
	Olmo Rayón (WoS)		Kostas Lampropoulos (UoP)
	Bruno Varela (WoS)		
	José Fran. Ruíz (Atos)		

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
Jose Fran. Ruíz	Atos
Kostas Lampropoulos	UoP
Olmo Rayón	WoS
Bruno Varela	WoS
Francisco Hernández-Ramírez	WoS

Document History			
Version	Date	Change editors	Changes
0.1	11/10/2018	Jose Fran. Ruiz (Atos)	Table of contents template for all use case partners
0.2	05/11/2018	F.Hernández-Ramírez (WoS)	First draft of the document.
0.3	26/11/2018	F.Hernández-Ramírez (WoS)	Second draft after QA1
1.0	30/11/2018	F.Hernández-Ramírez (WoS)	Final version after QA2
1.1	30/11/2018	ATOS	Quality Review and Submission

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Francisco Hernández-Ramírez (WoS)	30/11/2018
Technical manager	Jose Fran. Ruíz (Atos)	30/11/2018
Quality manager	Rosana Valle Soriano (Atos)	30/11/2018
Project Manager	Jose Fran. Ruíz (Atos)	30/11/2018

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot	Page:	2 of 43
Reference:	D4.5	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
List of Acronyms.....	7
Executive Summary	8
1 Introduction.....	9
1.1 Purpose of the document	9
1.2 Relation to other project work.....	9
1.3 Structure of the document	9
1.4 Glossary adopted in this document.....	10
2 Update of requirements and needs	11
2.1 Systems information.....	11
2.2 Systems protection	11
3 Description of the use case.....	14
3.1 Architecture and design.....	15
3.2 Scenarios of application	17
3.3 Cybersecurity threats and impact	17
3.4 Cybersecurity training and awareness status	19
3.5 Business opportunity	19
4 Integration of the SMESEC Framework	20
4.1 SMESEC-enhanced business pilot	20
4.2 Process and tools integrated	21
4.2.1 MBT	22
4.2.2 Anti ROP	23
4.2.3 XL SIEM	24
4.2.4 Gravity Zone.....	25
4.2.5 NetScaler	26
4.2.6 Other tools	26
4.3 Testing.....	27
4.3.1 MBT	27

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot			Page:	3 of 43		
Reference:	D4.5	Dissemination:	PU	Version:	1.1	Status:	Final

4.3.2	Anti ROP	29
4.3.3	XL SIEM	30
4.3.4	Gravity Zone.....	30
4.3.5	NetScaler	31
4.4	Initial feedback.....	33
4.4.1	MBT	33
4.4.2	Anti ROP	33
4.4.3	XL SIEM	33
4.4.4	Gravity Zone.....	33
4.4.5	NetScaler	34
5	Next steps.....	35
5.1	Integration of business in the SMESEC Framework.....	35
5.2	Training and awareness plan	35
5.3	Initial testing and validation plan	38
6	Conclusions.....	41
6.1	Experience of the initial integration	41
6.2	Fulfilling of objectives	41
6.3	Use in SME environment	41
6.4	Improvements for the scenario	42
	References	43

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot			Page:	4 of 43		
Reference:	D4.5	Dissemination:	PU	Version:	1.1	Status:	Final

List of Tables

<i>Table 1. Summary of functional requirements of Pilot III (Industrial Services)</i>	12
<i>Table 2. High-level security requirements of Pilot III (Industrial Services)</i>	13
<i>Table 3. Criticality assessment of the elements at Pilot III (Industrial Services) architecture</i>	18
<i>Table 4. Assessment of potential security threats affecting Pilot III (Industrial Services)</i>	18
<i>Table 5. Adopted tools in the Pilot III (Industrial Services)</i>	20
<i>Table 6. Inventory of assets to be deployed at Pilot III (Industrial services)</i>	22
<i>Table 7. Training and awareness plan: targeted employees</i>	36
<i>Table 8. Training and awareness plan: general training sessions at Worldsensing</i>	36
<i>Table 9. Training and awareness plan: technical measures implemented at WS with associated training</i>	36
<i>Table 10. Training and awareness plan: degree of implementation</i>	37
<i>Table 11. SMESEC framework validation: list of planned tests</i>	38
<i>Table 12. Matching of Loadsensing vulnerabilities and protection provided by SMESEC tools</i>	40

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot			Page:	5 of 43		
Reference:	D4.5	Dissemination:	PU	Version:	1.1	Status:	Final

List of Figures

Figure 1. Loadsensing infrastructure deployed at Pilot III (Industrial Services)	11
Figure 2. General outline of the Pilot III (Industrial Services)	15
Figure 3. Overall look of the gateway server to monitor the sensors' network	16
Figure 4. Schematic of the cloud infrastructure at the Pilot III (Industrial Services)	16
Figure 5. Front-end of the functional user interface at Pilot III (Industrial Services)	17
Figure 6. Schematic of the security tools in the Pilot III (Industrial Services) and interdependencies	20
Figure 7. General views of the works at Patras' stadium	21
Figure 8. Schematic of the internal functioning of MBT (EGM tool)	22
Figure 9. MBT model design of the Loadsensing architecture	23
Figure 10. XL-SIEM: log capture interface	24
Figure 11. View of the Gravity Zone administration console	26
Figure 12. General deployment of the NetScaler tool deployed at Worldsensing's premises	27
Figure 13. View of the Loadsensing front-end at Patras' stadium	28
Figure 14. Attack to a Loadsensing gateway without Anti-ROP. Successful attack. Video: https://youtu.be/kUurVXoNB04	29
Figure 15. Attack to a Loadsensing gateway with Anti-ROP- Unsuccessful attack. Video: https://youtu.be/HOLQeUimoMU	29
Figure 16. Gravity Zone console configured to send logs to the XL-SIEM agent	30
Figure 17. Gravity Zone: web browser protection activated	30
Figure 18. Gravity Zone: end-point detection activated. Malware detection	31
Figure 19. Gravity Zone: real-time reporting to the central server working	31
Figure 20. NetScaler machine installed at Worldsensing's premises	32
Figure 21. NetScaler deployment on Worldsensing's premises. Functional view	32
Figure 22. ISO27001 certification awarded by Bureau Veritas	37

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot			Page:	6 of 43		
Reference:	D4.5	Dissemination:	PU	Version:	1.1	Status:	Final

List of Acronyms

Abbreviation / acronym	Description
CIA	Confidentiality, Integrity, Availability
DoA	Description of Action
DPO	Data Protection Officer
Dx.y	Deliverable number y belonging to WP 5
EC	European Commission
EC-GA	Grant Agreement
EDR	Endpoint Detection and Response
EU	European Union
F2F	Face-to-face
GB	Gigabytes
GCP	Google Cloud Platform
GDPR	General Data Protection Regulation
GW	Gateway
IoT	Internet of Things
ISO	International Organization for Standardization
LoRa	Low-power Range (protocol)
MBT	Model Based Testing
MFA	Multiple Factor of Authentication
Mx	Month X
NIS Directive	Directive on security of network and information systems
OWASP	Open Web Application Security Project
PoE	Power over Ethernet
PWS	Public Warning System
RAM	Random Access Memory
RoHS	Restriction of Hazardous Substances
ROP	Return-oriented programming
SaaS	Software as a Service
SEM	Security Event Management
SIEM	Security Information and Event Manager
SIM	Security Information Management
SME	Small-Medium Enterprise
SW	Software
TaaS	Technology as a Service
UX	User Experience
VM	Virtual Machine
WP	Work Package

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot	Page:	7 of 43
Reference:	D4.5	Dissemination:	PU
	Version:	1.1	Status:
			Final

Executive Summary

This deliverable provides an overview of the efforts carried out during the first 18 months of the project to deploy the SMESEC Framework in the pilot III (Industrial Services). Although the report has been generated at an early stage of the SMESEC project, in which the development of the framework is still in its infancy, the results shown herein successfully validate the objective to secure the IoT industrial solution of Worldsensing (Loadsensing) and as a result to improve the monitoring of industrial assets' operations.

On the basis of the general requirements identified in the deliverable D2.1 and the specific needs of the pilot, a detailed description of this specific use case is given, paying special attention to the integration of the SMESEC tools within the Loadsensing architecture. Apart from the evidence of the work done so far at different levels (physical installation of hardware, technical development of software, interconnection of SMESEC tools and validation tests), the document also explores the next steps to be completed by the Consortium as well as the assessment of the effective impact linked to the adoption of the Framework in terms of business improvement and cybersecurity awareness within Worldsensing.

In short, the document is just a first but critical introduction to the existing version of the Pilot III foreseen in the project. The final evaluation of the integration of the SMESEC Framework with the Worldsensing's technologies will be shown in the deliverable D4.6 at month 24 and a final and complete evaluation at the end of the project.

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot			Page:	8 of 43		
Reference:	D4.5	Dissemination:	PU	Version:	1.1	Status:	Final

1 Introduction

1.1 Purpose of the document

The aim of the deliverable is to present the development degree of the Pilot III (Industrial Services) at month 18 of the project, describing the first efforts to integrate the SMESEC Framework in a commercial IoT technology. Specifically, D4.5 provides preliminary but tangible proofs that the SMESEC tools can successfully work in an orchestrated approach to provide add-value functionalities in the field of cybersecurity, enriching the performance and as result, the business proposition of the proprietary product Loadsensing.

The document describes, therefore, one of the cornerstones activities of WP4, which aims to validate the SMESEC Framework out of the lab and demonstrate that the generic project prototype can be easily adapted to the pilots' specific needs. It also shows how SMESEC has contributed to building up a nascent cybersecurity culture within Worldsensing, which is in line with the project provision of rising the cybersecurity awareness in European SMEs.

1.2 Relation to other project work

As described in the DoA, the pilots are unique test beds to validate the SMESEC Framework potential and understand how the specific solutions can be generalized in a final and optimized solution. For this reason, the pilots' functionalities need to be evaluated as a whole from the preliminary (D4.5) to the final stage (D4.6) [2]. This knowledge will become crucial to design a meaningful evaluation campaign of the SMESEC framework envisaged in the WP5. In this context, the implementation of the Industrial Service pilot has taken as a starting point the requirements listed in D2.1 [1] and its implementation is aligned with the work done in WP3

1.3 Structure of the document

This document is structured in six major chapters, whose contents are the following:

Chapter 1 is the introduction to the document scope and structure.

Chapter 2 overviews the initial list of requirements for the pilot already presented in the deliverable D2.1.

Chapter 3 briefly presents the scope of the pilot III and how it fits in Worldsensing's roadmap. The main cybersecurity challenges that need to be faced are also listed and preliminary assessed.

Chapter 4 shows the status of the pilot deployment as this is being written, trying to describe the main achievements made to date.

Chapter 5 identifies the pending actions to be completed before the project end in order to validate the pilot and the expected functionalities and finally,

Chapter 6 recaps the main contents of the document.

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot			Page:	9 of 43		
Reference:	D4.5	Dissemination:	PU	Version:	1.1	Status:	Final

1.4 Glossary adopted in this document

This document is not based on any specific definition other than the standard ones.

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot			Page:	10 of 43		
Reference:	D4.5	Dissemination:	PU	Version:	1.1	Status:	Final

2 Update of requirements and needs

2.1 Systems information

The list with the general requirements of the technology to be deployed at the pilot venue was presented in the deliverable D2.1 [1]. As a reminder, a standard Loadsensing infrastructure (Figure 1) is divided into three well-differentiated domains: (i) sensors, (ii) gateways¹ and (iii) cloud.

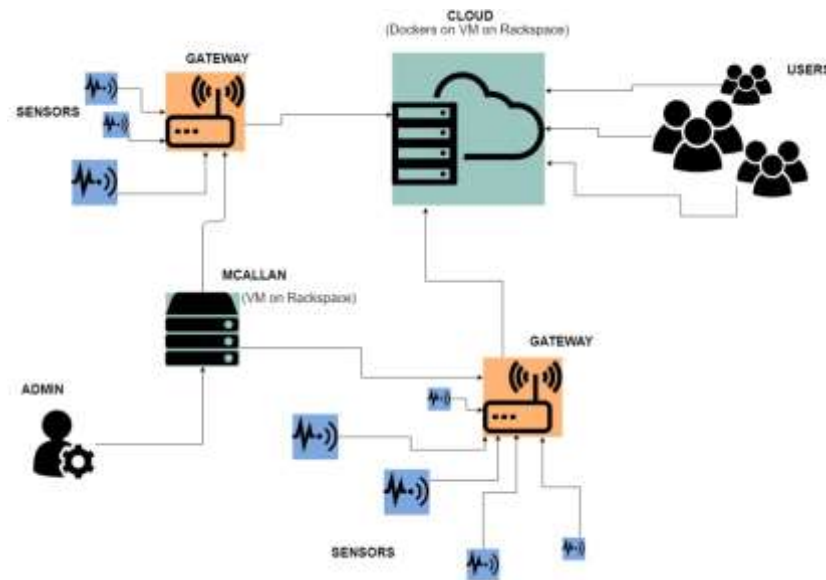


Figure 1. Loadsensing infrastructure deployed at Pilot III (Industrial Services)

As this is being written, any significant change in the items identified in the initial list [1] is neither necessary nor planned. In fact, the pilot initial conception has been fully developed since then: the tests will be conducted in an out-of-the-lab venue (football stadium) resulting in a more ambitious and complex project than that initially envisaged at the beginning of SMESEC. Nevertheless, the list of requirements remains valid and at the same time the selected location allows deepening the business perspective. For the sake of clarity, a short summary of the requirements for each domain is given in Table 1.

2.2 Systems protection

Apart from the general technical requirements shown in the previous section, a list of specific ones necessary to guarantee the integrity of the pilot against external attacks have also been envisaged from the start. Again, they have been classified depending on the applicable domain (Table 2). It must be pointed out that security aspects have often not fully been taken into account by Worldsensing's developers before the SMESEC project, and that is the reason why this field has been considered the most immature aspect of the pilot's technology.

¹ Mcallan server is a proprietary solution to manage the IoT gateways. Here, the term Gateways hub will be often used interchangeably to describe the same item.

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot	Page:	11 of 43	
Reference:	D4.5	Dissemination:	PU	
	Version:	1.1	Status:	Final

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 (220V)
		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)

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

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot	Page:	12 of 43	
Reference:	D4.5	Dissemination:	PU	
	Version:	1.1	Status:	Final

	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. High-level security requirements of Pilot III (Industrial Services)

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot			Page:	13 of 43		
Reference:	D4.5	Dissemination:	PU	Version:	1.1	Status:	Final

3 Description of the use case

The Pilot III (Industrial Services) has been conceived by Worldsensing to validate the feasibility of adding security solutions to the Industrial IoT field while keeping unchanged the most important features demanded by the market to the present commercial solutions.

Adopting an eminently practical approach, a real infrastructure has been selected to emulate a real deployment of Loadsensing proprietary technology and thus assess in a real environment the functionalities of the SMESEC framework. Kostas Davourlis stadium in Patras, Greece, is an infrastructure originally inaugurated in the 30s that despite the recent refurbishment of some of its parts still faces structural problems. For this reason, it has been judged useful to monitor the status of the structure by measuring the tilting of some points by using selected sensors.

Kostas Davourlis Stadium [3]	
Former name	Panachaiki Stadium
Location	Patras, Greece
Coordinates	38°15'42"N 21°44'45"E
Owner	Panachaiki GE
Capacity	11,321
Construction	1935
Renovated	2000



Infrastructures like the Kostas Davourlis stadium are gaining special relevance for the national economies and the well-being of citizens, since any undesired event such as a structural failure and partial collapse may lead to dreadful consequences and severe reputational damages. For this reason, there is an increasing demand for continuous information by the authorities, so that they can apply proactive corrective actions to the infrastructure management, if necessary.

In particular, the installed sensors will monitor the stability of the stadium terraces trying to establish a dependency between the load charges and the movement of the structure, fixing alarm thresholds to

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot	Page:	14 of 43
Reference:	D4.5	Dissemination:	PU
	Version:	1.1	Status:
			Final

activate contingency plans. To that end, five Loadsensing dataloggers equipped with inclination, vibration and temperature sensors are considered for the pilot deployment, together with two gateways and a duplicated cloud infrastructure. The whole system will be fully accessible through a user-friendly web interface.

The goal of the pilot, compared to regular Loadsensing installations, is the merging of the structural information coming from the sensors and the cybersecurity inputs generated by the SMESEC framework, which put together can provide for the first time a unique perspective of what is going on at an infrastructure level. In this way, anomalous scenarios originated by cyberattacks will be easily discarded in an early-stage, avoiding false alarms situations which can trigger an unnecessary overreaction by the stadium operator. Last but not least, the increased robustness of the entire Loadsensing architecture is crucial to guarantee the integrity, confidentiality and availability of the generated data. This is a must to extend the use of Loadsensing to critical infrastructures. In short, Worldsensing looks forward to replicating the technology deployed at the pilot in many other venues, aiming to provide added value to Worldsensing technology portfolio.

3.1 Architecture and design

The outlines of the pilot have been presented in the former section. In general, the deployment of Worldsensing technology must take into account the requisites and constraints coming from the stadium side: the sensors need to be installed in the backside of the terraces to guarantee the protection against adverse weather conditions and vandalism. The sensors communication is established through LoRa protocol with the gateway, which is physically located in a control room inside the stadium equipped with stable and wired internet connection. The cloud infrastructure will rely on GCP (Google Cloud Platform).



Figure 2. General outline of the Pilot III (Industrial Services)

The gateway provides a basic web server to access the sensor network information. Through this interface, basic configuration actions can be implemented, such as changing the sampling rate of the sensors. Figure 3 shows the overall appearance of this server, which can be also used to download sensors' raw data for working without connection.

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot			Page:	15 of 43
Reference:	D4.5	Dissemination:	PU	Version:	1.1
				Status:	Final

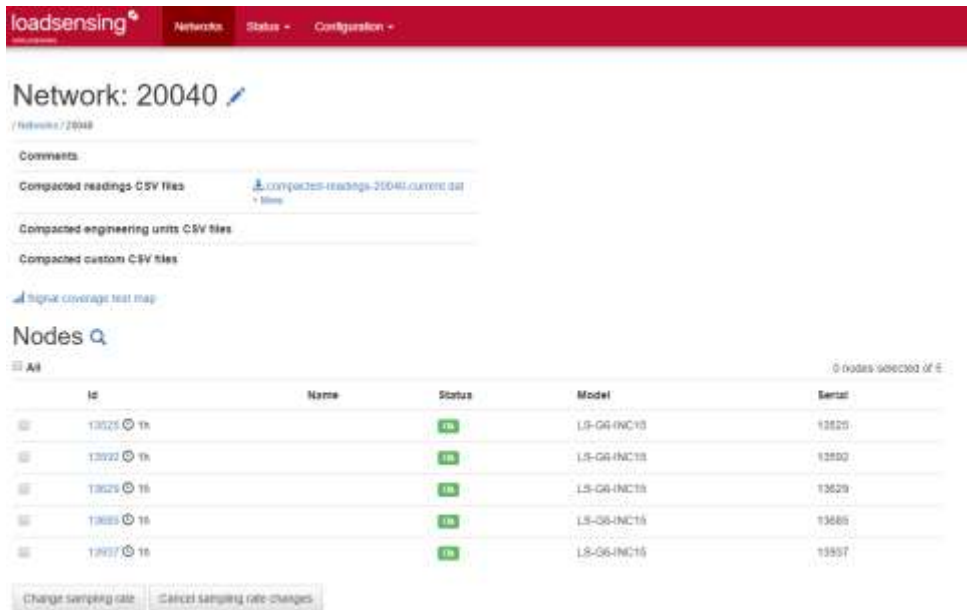


Figure 3. Overall look of the gateway server to monitor the sensors' network

While the sensors and the gateway layouts are quite straightforward, the architecture of the cloud is slightly more complex: as shown in the figure below, the gateways and the users reach the servers through the Internet. Before entering the Google Cloud domain, where both the gateways centralization and the visualization servers are deployed, they go through a dedicated-Google firewall filtering malicious traffic. The gateway centralization server acts as the backend of the system and the visualization one provides the user interface. This last server is partially based on Grafana.

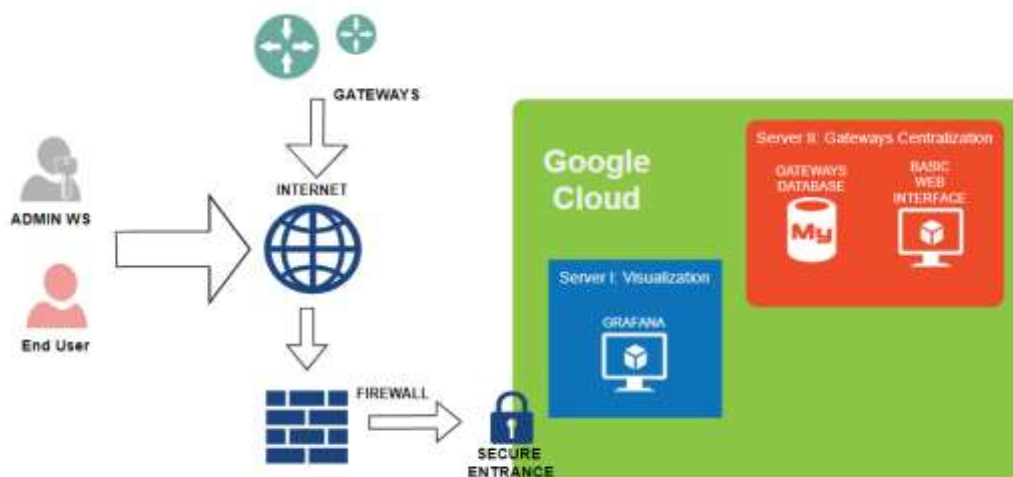


Figure 4. Schematic of the cloud infrastructure at the Pilot III (Industrial Services)

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot			Page:	16 of 43
Reference:	D4.5	Dissemination:	PU	Version:	1.1
				Status:	Final

The user interface at the Pilot III implements the latest and most advanced visualization tools offered by Worldsensing. To that end, the data coming from the sensor are displayed through Mobility, a proprietary IoT solution that helps authorities and operators to perform operational intelligence actions. Matching the security requirements, there is a secure authentication layer added to the system provided by Keycloak (www.keycloak.org).



Figure 5. Front-end of the functional user interface at Pilot III (Industrial Services)

3.2 Scenarios of application

The architecture developed for the pilot III is versatile enough to be easily adapted to many other applications. In this sense, the final scenarios where the Loadsensing + SMESEC framework suite can be translated cover all those business verticals demanding secure Operational Intelligence capabilities. Without seeking to be exhaustive, such as Loadsensing deployment is directly applicable in (i) the construction industry, (ii) mining and (iii) industrial monitoring processes. Besides, the concept of combining IoT and cybersecurity tools paves the way to address the lack of robust technologies in more critical applications, such as smart parking and traffic monitoring, in which personal data may be used. In this sense, the correct and active use of the SMESEC framework is conceived as a significant help to implement the “Security by Default” principle in vogue due to the new EU regulations such as the GDPR [4] and NIS Directive [5]. It should be pointed out that Worldsensing is present in all these sectors. Consequently, the project impact will reach different business lines in the mid- and long-term. Specifically, the pilot aims to provide real-time information of the status of the Loadsensing infrastructure in a stadium, raising dedicated alarms when cyberattacks are detected by the framework. All in all, the pilot will eventually validate that a non-skilled operator discriminates between real and fake alarms induced by internal and external attackers.

3.3 Cybersecurity threats and impact

As stated elsewhere, security is often neglected in IoT due to the accelerated pace of this market. It goes without saying that this is a major issue which may jeopardize many critical systems in the coming

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot			Page:	17 of 43		
Reference:	D4.5	Dissemination:	PU	Version:	1.1	Status:	Final

years. In this sense, Loadsensing has not been an exception up to now. SMESEC has been, however, a great excuse to introduce new working methodologies in Worldsensing based on the “Security by Default” principles.

In a first phase, each one of the assets making up the pilot has been evaluated considering the well-known model of the CIA triad used by the standard ISO27001 (Table 3). Needless to say, that this exercise is somewhat subjective, but it clearly identifies trends. As result, the gateway server deployed at the cloud has been considered the most critical item potentially subject to attacks.

CLASSIFICATION	NAME	LOCATION	CONFIDENTIALITY	INTEGRITY	AVAILABILITY	ASSET VALUE
Hardware	Kerlink Gateway (WS)	Patras Stadium	3	3	3	3,00
Hardware	Kerlink Gateway (Secure)	Patras Stadium	3	3	3	3,00
Hardware	Wireless Tiltmeter	Patras Stadium	1	4	3	2,67
Network	Gateway Internet Connexion	Patras Stadium	3	4	4	3,67
Server	Gateway / Macallan Sever	Google Cloud Platfrom	5	5	5	5,00
Server	Grafana Server	Google Cloud Platfrom	3	5	3	3,67

Table 3. Criticality assessment of the elements at Pilot III (Industrial Services) architecture

On this basis, the potential threats affecting each of the assets has been identified considering the probability of the event occurring and the resulting impact. All in all, this has allowed determining the severity of the threats against the pilot integrity as a whole.

IDENTIFIED ASSET	THREAT	PROBABILITY	CONSECUCENCE	SCORE	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)	Code injection	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
Gateway /Macallan Sever	Brute force against authentication	3	4	4,00	HIGH
Gateway /Macallan Sever	Code injection	2	5	3,33	MEDIUM
Gateway /Macallan Sever	DOS [Denial of Service]	2	4	2,67	MEDIUM
Gateway /Macallan Sever	Unpatched OS or applications	4	4	5,33	EXTREME
Grafana Server	Code injection	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

Table 4. Assessment of potential security threats affecting Pilot III (Industrial Services)

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot			Page:	18 of 43
Reference:	D4.5	Dissemination:	PU	Version:	1.1
				Status:	Final

From this exercise, it is clear that the Loadsensing architecture is vulnerable to manifold risks and threats, being the most critical ones those affecting the servers at the cloud and the connectivity with the gateway. Therefore, the accommodation of the SMESEC framework to the pilot (integration of specific tools) has been designed to cover as far as possible most of these weaknesses. The details about the exact SMESEC framework configuration to be deployed at the pilot are given in the chapters 4 and 5 of this deliverable.

3.4 Cybersecurity training and awareness status

Cybersecurity is usually a black spot in SMEs, and in particular start-ups. In this context, Worldsensing has been no exception: the importance given to security has been traditionally neglected in front of other aspects. However, as time goes by and the degree of maturity of the company increases, this aspect is reaching a more relevant role to effectively respond to the demands from the Worldsensing's investors and stakeholders.

Thus, SMESEC project has been considered an excellent catalyst to increase the cybersecurity awareness within the company, opening a period particularly active to improve the routines and habits of the employees in relation to the adoption of good practices. Parallel to the pilot deployment, the company has embarked on the objective to be externally certified (ISO27001) and adopt standard cybersecurity tools which up to now were surprisingly not in force. Full details of the work done so far and the next actions before the SMESEC completion are given in the next chapters. Nevertheless, Worldsensing would like to stress the huge challenge that the cybersecurity awareness entails, being even greater than the technical actions directly linked to the pilot technical deployment.

3.5 Business opportunity

As noted, the adoption of the SMESEC framework will result in more competitive IoT technologies which provide a clear competitive business advantage to Worldsensing's products from the competition. This is particularly true in light of the poor status of cybersecurity technologies supporting IoT worldwide.

Having said that, the business opportunity of merging the SMESEC framework with Loadsensing is twofold. In a first stage, supporting the Loadsensing normal operation with tools like those offered by SMESEC can effectively increase the robustness of the current commercial solution, which is a differential fact compared to the rest of the market offer according to the best of our knowledge. Secondly, the combination of cybersecurity logs and structural data coming from the sensors paves the way to build up in the mid-term an enriched Public Warning System (PWS) module that triggers structural alarms at the same time it discards false sensors read-outs and malicious events. This is crucial to automate many applications which require human activity at present time. As stated in section 3.2, this second objective is not limited to a specific business vertical and therefore its final impact could be huge in the long-term.

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot			Page:	19 of 43		
Reference:	D4.5	Dissemination:	PU	Version:	1.1	Status:	Final

4 Integration of the SMESEC Framework

4.1 SMESEC-enhanced business pilot

The SMESEC-enhanced business pilot has been conceived to add at least one secure tool in each one of the Loadsensing domains. This approach aims to validate that the value proposition of SMESEC can impact all points of an end-to-end IoT solution. Special efforts have been done in the upper-edge part of the pilot architecture (gateway and cloud) considering the weaknesses and criticality already identified there (see Chapter 3). Table 5 summarizes the list of the tools to be adopted in the specific instance of the SMESEC framework as well as the main expected contribution to the enriched Loadsensing functionalities.

Pilot III: adopted tools		
Tools	Provider / partner	Purpose
Security tests	EGM	Integrity checking of the infrastructure (sensors)
Anti-ROP	IBM	Passive protection of GWs
NetScaler	CITRIX	Network traffic flow monitoring
XL-SIEM	ATOS	Events log management and anomaly detection
GravityZone	Bitdefender	Antivirus and security logs generator at the cloud

Table 5. Adopted tools in the Pilot III (Industrial Services)

Schematically, the positioning of the tools within the pilot's domains and their interdependency is shown in Figure 6. The management layer offered to the end-users is expected to be fully integrated into the Loadsensing SW front-end avoiding in this way unnecessary UX duplicities.

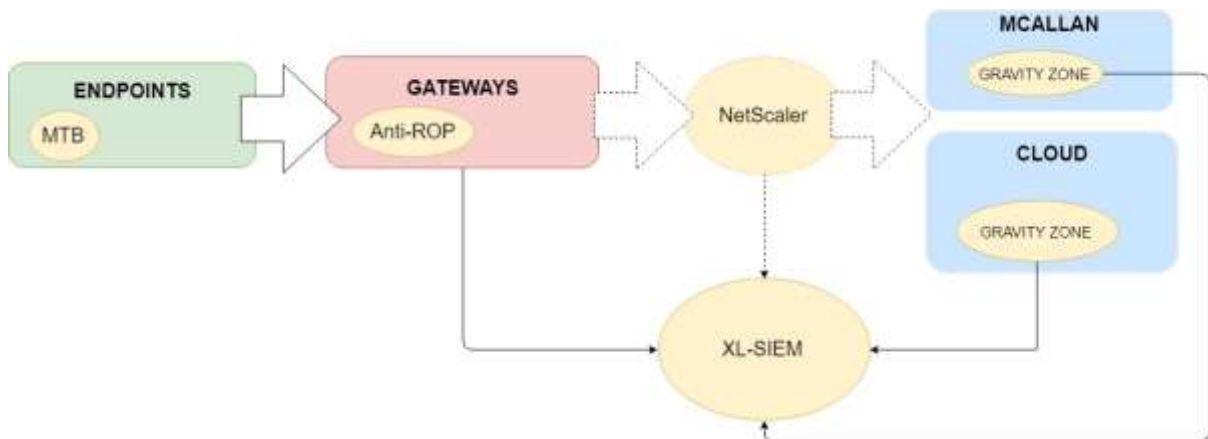


Figure 6. Schematic of the security tools in the Pilot III (Industrial Services) and interdependencies

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot	Page:	20 of 43	
Reference:	D4.5	Dissemination:	PU	
	Version:	1.1	Status:	Final

4.2 Process and tools integrated

The pilot scope is quite ambitious since it entails the active third party's involvement (stadium operator staff) and the deployment of technology in a non-controlled environment. On this basis, the first efforts have concentrated on the correct installation of the Loadsensing technology at ground level. This step is crucial to minimize the sources of potential errors that may hinder the evaluation of the SMESEC tools functionalities once the solution is running as a real demonstrator.

In July 2018, most of the elements necessary to validate the pilot were physically installed at the stadium. For that purpose, the active collaboration of the operator and the University of Patras (UoP) was highly valuable. At the time of this report, only a second gateway with Anti-ROP protection has not yet been installed and it remains at IBM premises (Israel). The purpose of this missing device is to duplicate the communication channel and demonstrate through dedicated tests the advantages of the Anti-ROP technology.

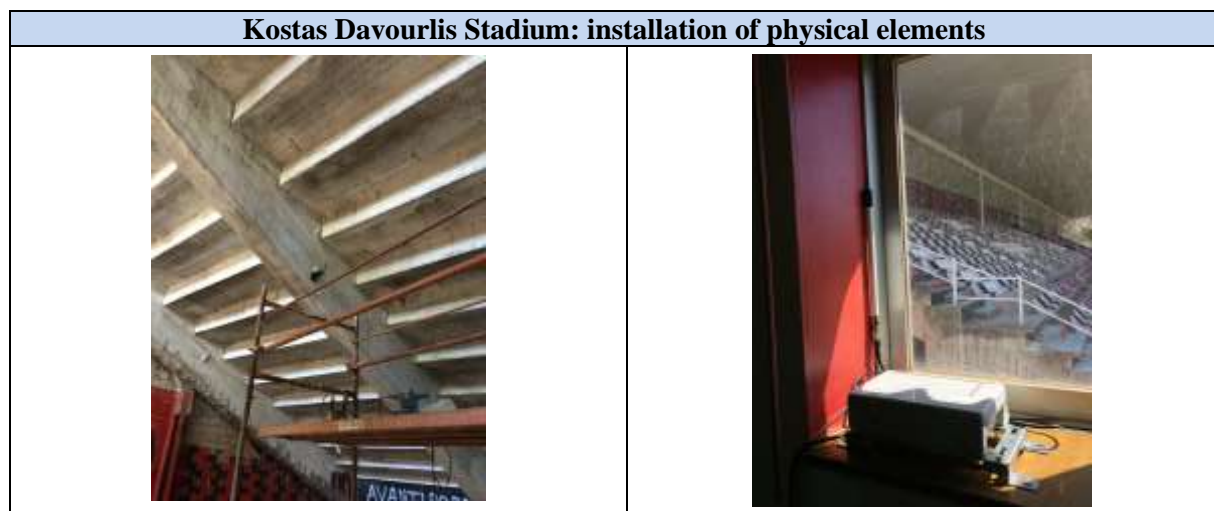


Figure 7. General views of the works at Patras' stadium

In parallel, the necessary cloud infrastructure to run the pilot has been put into operation as well. Since then, the system has been acquiring physical data and gathering enough information to correctly determine alarm thresholds for this particular infrastructure.

Device	Deployment ID	Device ID	Model	Status
Kerlink Gateway	WS Deployment	20040	LoRa IoT Station	Deployed
Kerlink Gateway	Secure Deployment	14112	LoRa IoT Station	Pending
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
Macallan Sever	WS Deployment	5.79.24.225	Linux Server	Deployed
Grafana Server	WS Deployment	162.13.144.202	Linux Server	Deployed

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot			Page:	21 of 43
Reference:	D4.5	Dissemination:	PU	Version:	1.1
				Status:	Final

Table 6. Inventory of assets to be deployed at Pilot III (Industrial services)

Focusing on the tools' integration in Loadsensing, an overview of the current situation is provided in the following subsections.

4.2.1 MBT

The EGM TaaS is a web service allowing users to execute tests concerning security issues. Test suites need a prior ad-hoc accommodation to the use cases and theoretically, they allow SMEs to access a database to evaluate a confidence level of the integrated IoT systems. In short, the test execution pinpoints failing security requirements that can be fixed afterwards.

Regarding its application to a given technology, the necessary adaptation process consists of two steps: (i) fitting in the system architecture to the model that EGM provides by default and (ii) the publication of a web front-end so that end-users can generate and run the specific tests. The final validation of the solution is also completed in this final stage (Figure 8).

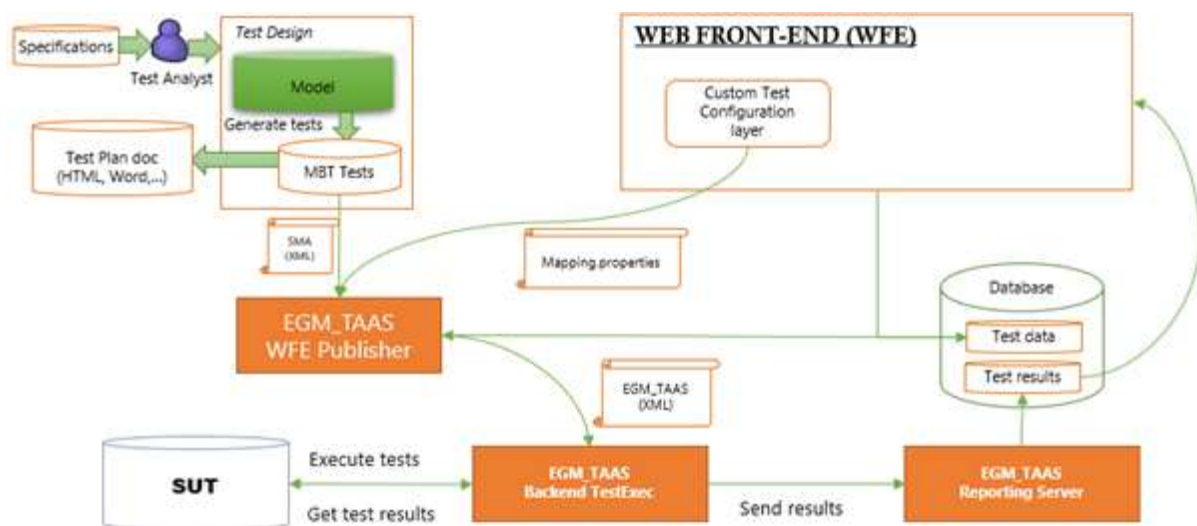


Figure 8. Schematic of the internal functioning of MBT (EGM tool)

EGM and Worldsensing have been focusing efforts on the first step, which is resulting in a more complex process due to the particularities of the Worldsensing' solution. Normally, the solutions tested with this MBT are pieces of software or even web apps, but in this pilot, the tests must deal with hardware (sensors and gateways) too. Up to now, two working sessions with EGM and Worldsensing engineers have allowed moving forward with the necessary capture of knowledge previous to the required model adaptation. Moving on to the details, MBT model creation procedure works in much simpler environments (e.g. server client model), but unfortunately this part is only one third of the Loadsensing architecture. Apart from this, it is necessary to extend the effort to the gateways, the inbound and outbound connections and the sensors. The first session focused on transferring the Worldsensing's infrastructure information to the MBT experts in EGM while the model creation was

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot	Page:	22 of 43
Reference:	D4.5	Dissemination:	PU
	Version:	1.1	Status:
			Final

not fully activated until the second one. To minimize overengineering efforts, a common framework with the rest of SMESEC pilots was used, which will be gradually polished in the coming weeks.

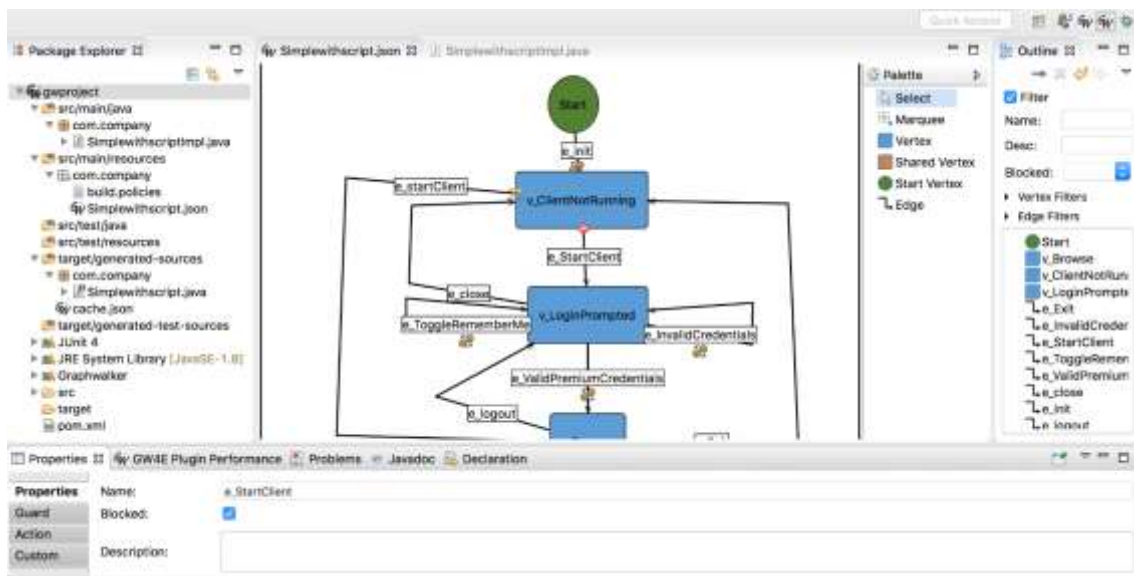



Figure 9. MBT model design of the Loadsensing architecture

4.2.2 Anti ROP

Anti-ROP is a solution that provides protection by creating unique libraries and devices. It protects the endpoint software applications against ROP and memory corruptions attacks.

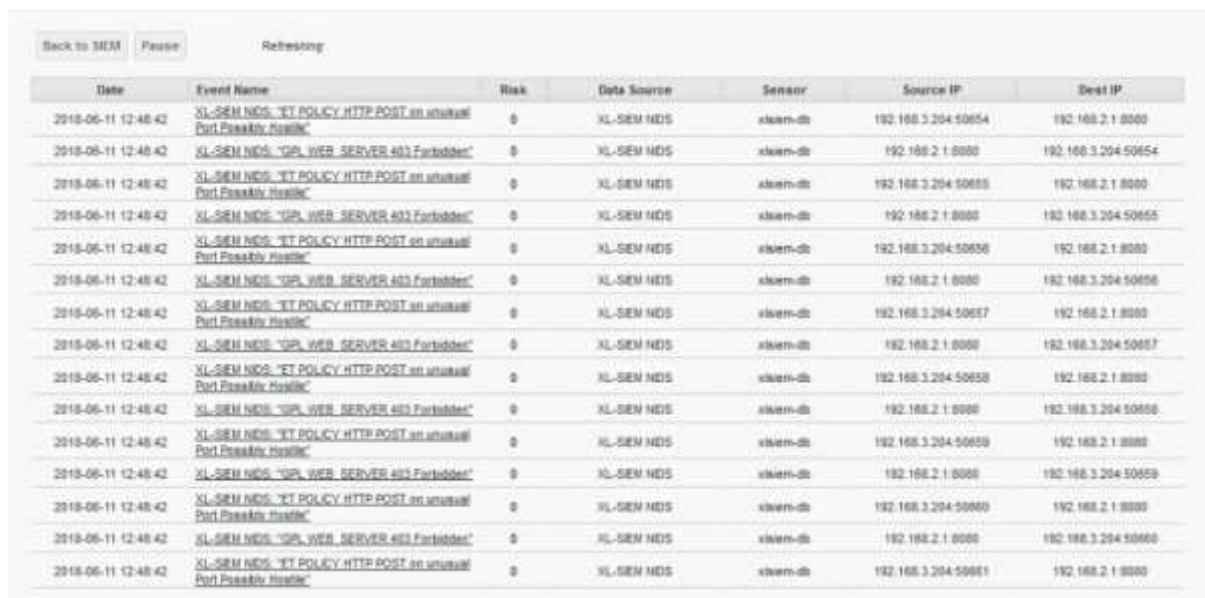
In the Pilot III framework, Anti-ROP technologies are used in the gateway domain to boost the security, avoiding with this technique that injection attacks are replicated in other devices. The ultimate objective is avoiding a malfunction avalanche in similar devices (gateways) installed worldwide.

Anti-ROP at Worldsensing's gateway	
	<p style="text-align: center;">Shakedown: compiler-based moving target protection for Return Oriented Programming attacks on an industrial IoT device</p> <p style="text-align: center;">Fady Copry¹, Francisco Hernandez², Davi Marik³, Ollas Rayko⁴</p> <p style="text-align: center;">¹IBM Research - Haifa, Israel ²Worldsensing, Spain ³rad@ellie.ibm.com</p> <p><small>Abstract. C/C++ compilers use Return Oriented Programming techniques in attack systems and IoT devices. While defenses have been developed, not all of them are applicable in constrained devices. We present Shakedown, which is a compiler-based randomizing build tool which creates several versions of the binary, each with a distinct memory layout. An attack developed against one device will not work on another device which has a different memory layout. We tested Shakedown on an industrial IoT device and shows that its normal functionality remained intact while an exploit was blocked.</small></p> <p><small>Keywords: Shakedown, exploit prevention, return-oriented-programming, IoT security.</small></p>

At the present time, Anti-ROP solution has been successfully installed in one of the Worldsensing's gateways and the main technical conclusions have resulted in a joint-technical communication prepared

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot	Page:	23 of 43
Reference:	D4.5	Dissemination:	PU
	Version:	1.1	Status: Final

by IBM and Worldensing2 [6]. The necessary knowledge to implement Anti-ROP in IoT gateways is therefore plausible, and it has already been demonstrated. The gateway to be used in the pilot has not been deployed in Patras yet since some pending tests are being conducted at IBM premises at the present time. The final objective is, once the modified gateway is installed in the stadium, to replicate the communication channel to validate the IBM solution through ad-hoc attack tests.



Date	Event Name	Risk	Data Source	Sensor	Source IP	Dest IP
2018-06-11 12:48:42	XL-SIEM NIDS: "ET POLICY HTTP POST on unusual Port Possible Header"	0	XL-SIEM NIDS	xlsem-ds	192.168.3.204:50654	192.168.2.1:8080
2018-06-11 12:48:42	XL-SIEM NIDS: "CPL WEB_SERVER 403 Forbidden"	0	XL-SIEM NIDS	xlsem-ds	192.168.2.1:8080	192.168.3.204:50654
2018-06-11 12:48:42	XL-SIEM NIDS: "ET POLICY HTTP POST on unusual Port Possible Header"	0	XL-SIEM NIDS	xlsem-ds	192.168.3.204:50655	192.168.2.1:8080
2018-06-11 12:48:42	XL-SIEM NIDS: "CPL WEB_SERVER 403 Forbidden"	0	XL-SIEM NIDS	xlsem-ds	192.168.2.1:8080	192.168.3.204:50655
2018-06-11 12:48:42	XL-SIEM NIDS: "ET POLICY HTTP POST on unusual Port Possible Header"	0	XL-SIEM NIDS	xlsem-ds	192.168.3.204:50656	192.168.2.1:8080
2018-06-11 12:48:42	XL-SIEM NIDS: "CPL WEB_SERVER 403 Forbidden"	0	XL-SIEM NIDS	xlsem-ds	192.168.2.1:8080	192.168.3.204:50656
2018-06-11 12:48:42	XL-SIEM NIDS: "ET POLICY HTTP POST on unusual Port Possible Header"	0	XL-SIEM NIDS	xlsem-ds	192.168.3.204:50657	192.168.2.1:8080
2018-06-11 12:48:42	XL-SIEM NIDS: "CPL WEB_SERVER 403 Forbidden"	0	XL-SIEM NIDS	xlsem-ds	192.168.2.1:8080	192.168.3.204:50657
2018-06-11 12:48:42	XL-SIEM NIDS: "ET POLICY HTTP POST on unusual Port Possible Header"	0	XL-SIEM NIDS	xlsem-ds	192.168.3.204:50658	192.168.2.1:8080
2018-06-11 12:48:42	XL-SIEM NIDS: "CPL WEB_SERVER 403 Forbidden"	0	XL-SIEM NIDS	xlsem-ds	192.168.2.1:8080	192.168.3.204:50658
2018-06-11 12:48:42	XL-SIEM NIDS: "ET POLICY HTTP POST on unusual Port Possible Header"	0	XL-SIEM NIDS	xlsem-ds	192.168.3.204:50659	192.168.2.1:8080
2018-06-11 12:48:42	XL-SIEM NIDS: "CPL WEB_SERVER 403 Forbidden"	0	XL-SIEM NIDS	xlsem-ds	192.168.2.1:8080	192.168.3.204:50659
2018-06-11 12:48:42	XL-SIEM NIDS: "ET POLICY HTTP POST on unusual Port Possible Header"	0	XL-SIEM NIDS	xlsem-ds	192.168.3.204:50660	192.168.2.1:8080
2018-06-11 12:48:42	XL-SIEM NIDS: "CPL WEB_SERVER 403 Forbidden"	0	XL-SIEM NIDS	xlsem-ds	192.168.2.1:8080	192.168.3.204:50660
2018-06-11 12:48:42	XL-SIEM NIDS: "ET POLICY HTTP POST on unusual Port Possible Header"	0	XL-SIEM NIDS	xlsem-ds	192.168.3.204:50661	192.168.2.1:8080

Figure 10. XL-SIEM: log capture interface

4.2.3 XL SIEM

The XL-SIEM is a system supporting a high-performance correlation engine that allows detecting intrusions and malicious activities in IT and OT systems (e.g. database, communication channels, interfaces, etc.). The tool also provides real-time and historical reports of the system status so that the administrator can undertake corrective and mitigation actions in the event a security incident occurs.

On the other hand, an effective log management strategy is crucial in any Loadsensing deployment if we want to monitor and control the status of the physical infrastructure and the sensors readouts. Nevertheless, pooling a vast amount of information coming from the cyber and physical domain results in an unsurmountable amount of data difficult to be handled. Here, it is where the XL-SIEM plays a key role: within the Pilot III, XL-SIEM gathers all the logs coming from the SMESEC tools but also the structural Loadsensing events for the later processing and analysis. A set of alarms can be also defined to facilitate the infrastructure management. The log capture interface running at present time is shown in Figure 10. Tests have been conducted to extract and send logs using syslog protocol from Gravity Zone (see next section) to the XL-SIEM, where they are parsed and displayed in a dedicated frontend.

² <https://arxiv.org/abs/1810.02090>

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot			Page:	24 of 43	
Reference:	D4.5	Dissemination:	PU	Version:	1.1	Status: Final

4.2.4 Gravity Zone

Bitdefender Gravity Zone is an integrated layered next-gen endpoint protection and easy-to-use endpoint detection and response (EDR) platform. The goal of this combination is to protect enterprises against even the most complex cyber threats. The solution offers prevention, automated detection, investigation and response tools, enabling enterprise customers with limited resources and technical skills to protect their digital assets and respond to these threats.

Regarding the Loadsensing solution, Gravity Zone is expected to provide with anti-malware intelligence from the central servers in the cloud to the gateways and other machines used to remotely administrate the pilot. At the server level, Gravity Zone checks on manifold anomalies such as suspicious traffic and unexpected user actions. On the other hand, end users will have their endpoints protected, allowing the administrators to block specific contents (black and white listing), manage general settings and activate extra features such as hard drive encryption.

GravityZone is, therefore, a unified solution as it was built with prevention, detection, investigation and response mechanisms built into a single agent, which can be managed from a unique console.

Due to the complexity of the Loadsensing solution, several development stages have been identified to complete the correct GravityZone integration within the pilot architecture. It goes without saying that these stages are interrelated and not necessarily must be completed sequentially. These steps are:

1. Deployment of the solution on premises.
2. Deployment of the solution in the cloud. The main console must be reachable from any point of the internet.
3. Selected endpoints of the Loadsensing deployment to be protected with the anti-virus endpoint package.
4. Anti-virus endpoint package to be deployed on the servers controlling the pilot (visualization server and gateways hub).
5. Securing the communication between this server and the XL-SIEM. Logs must reach the XL-SIEM agent without problems.

From a practical point of view, the first three steps have already been completed. Figure 11 shows the Bitdefender console of the deployment running on a public which is easily reachable with a standard web browser.

On the other hand, the protection of the cloud infrastructure will require more efforts. The objective is to find out a deployment protocol transparent enough for the end users that avoids stopping the running Loadsensing services. In this way, the adoption of this technology could be easily transferred in commercial Loadsensing deployments beyond the SMESEC project.

Last but not least, the communication feasibility between this solution and the XL-SIEM has already been validated (see XL-SIEM previous section), despite further work needs to be done in the coming weeks to get optimal results.

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot			Page:	25 of 43		
Reference:	D4.5	Dissemination:	PU	Version:	1.1	Status:	Final

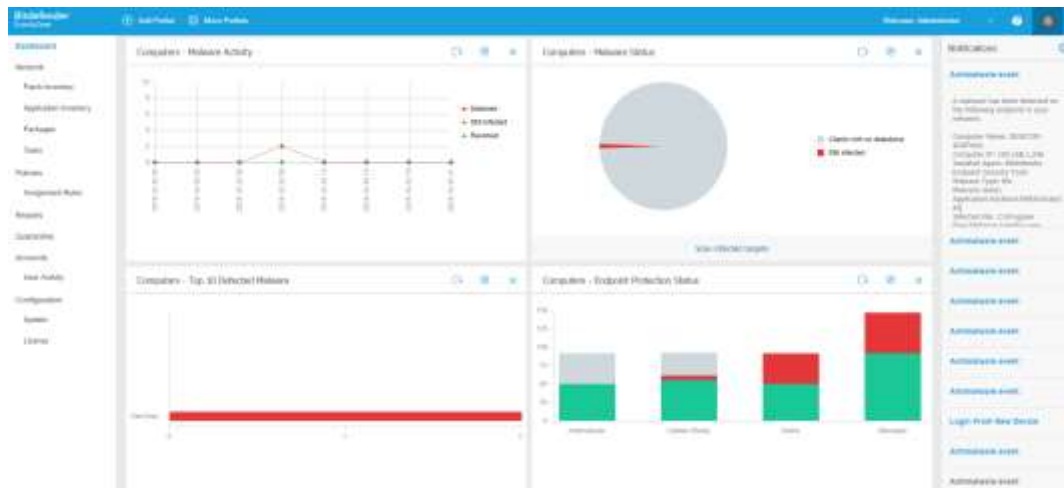


Figure 11. View of the Gravity Zone administration console

4.2.5 NetScaler

The NetScaler platform provides advanced network security solution for enterprises made up of two component parts: (i) the AppFirewall protects web applications and (ii) the Secure Web Gateway provides end-to-end security between remote devices and the company internal resources, inspecting outgoing traffic and applying security policies.

Since the Loadsensing architecture is basically a cloud-based solution, the adoption of this tool in the pilot requires two clearly differentiated phases. In the first one, NetScaler has been deployed and tested on Worldsensing premises. This has allowed understanding the inner workings of the software and gaining control on the endpoints of those employees managing the pilot. Figure 12 shows a layout of the deployed technology. Unfortunately, this approach cannot be extended to the servers and for this reason, the goal is to deploy the firewall in the cloud during the second phase. Nevertheless, there are some drawbacks to be circumvented such as the random assignment IP addresses by the cloud provider. For the time being, this is being analysed to find out a convenient solution that keeps the pilot infrastructure simple enough.

4.2.6 Other tools

Worldsensing does not exclude the adoption of other tools offered by the consortium in a later stage, such as the Honeypot technology provided by FORTH. For this reason, it is also exploring how they could fit the pilot's requirement. In particular, the primary constraint is that the whole infrastructure of a real Loadsensing deployment is based on the cloud without real physical infrastructure on the premises. This might be a major problem for the rest of the tools at present time. For the Honeypot, some tests have been even envisaged and it is conceivable to think that it will be finally integrated in the final pilot.

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot			Page:	26 of 43	
Reference:	D4.5	Dissemination:	PU	Version:	1.1	Status: Final

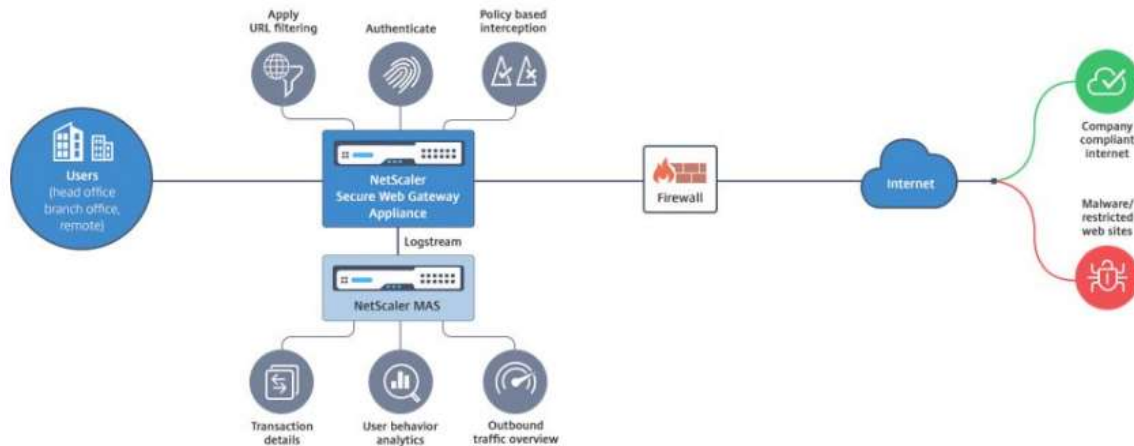


Figure 12. General deployment of the NetScaler tool deployed at Worldsensing’s premises

4.3 Testing

The preceding section provides an overview of the tools to be adopted in the pilot as well as the degree of integration at present time. Here, a detailed insight of the tests performed so far for each one is shown. Again, we would like to highlight that most of the efforts up to now have focused on the validation of the proper functioning of the Loadsensing deployment in the stadium (sensors and gateway). Actually, any functional failure not directly related to cybersecurity aspects may lead to a deception or contrivance with the results coming out from the security tests. This would jeopardize the entire SMESEC pilot scope. Until today, the deployed infrastructure is, however, working properly, allowing gathering enough data and knowledge to be used afterwards (Figure 13). As far as the tools are concerned, the work done is described in the following subsections.

4.3.1 MBT

As discussed above, the MBT integration in the pilot remains in a conceptual phase. Right now, the biggest challenge is the correct modelling of the gateway which is a theoretical defiance according to EGM inputs. In this sense, no real testing has been completed so far despite this scenario will change in the coming weeks.

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot	Page:	27 of 43	
Reference:	D4.5	Dissemination:	PU	
	Version:	1.1	Status:	Final

Loadsensing instance at Patras' stadium

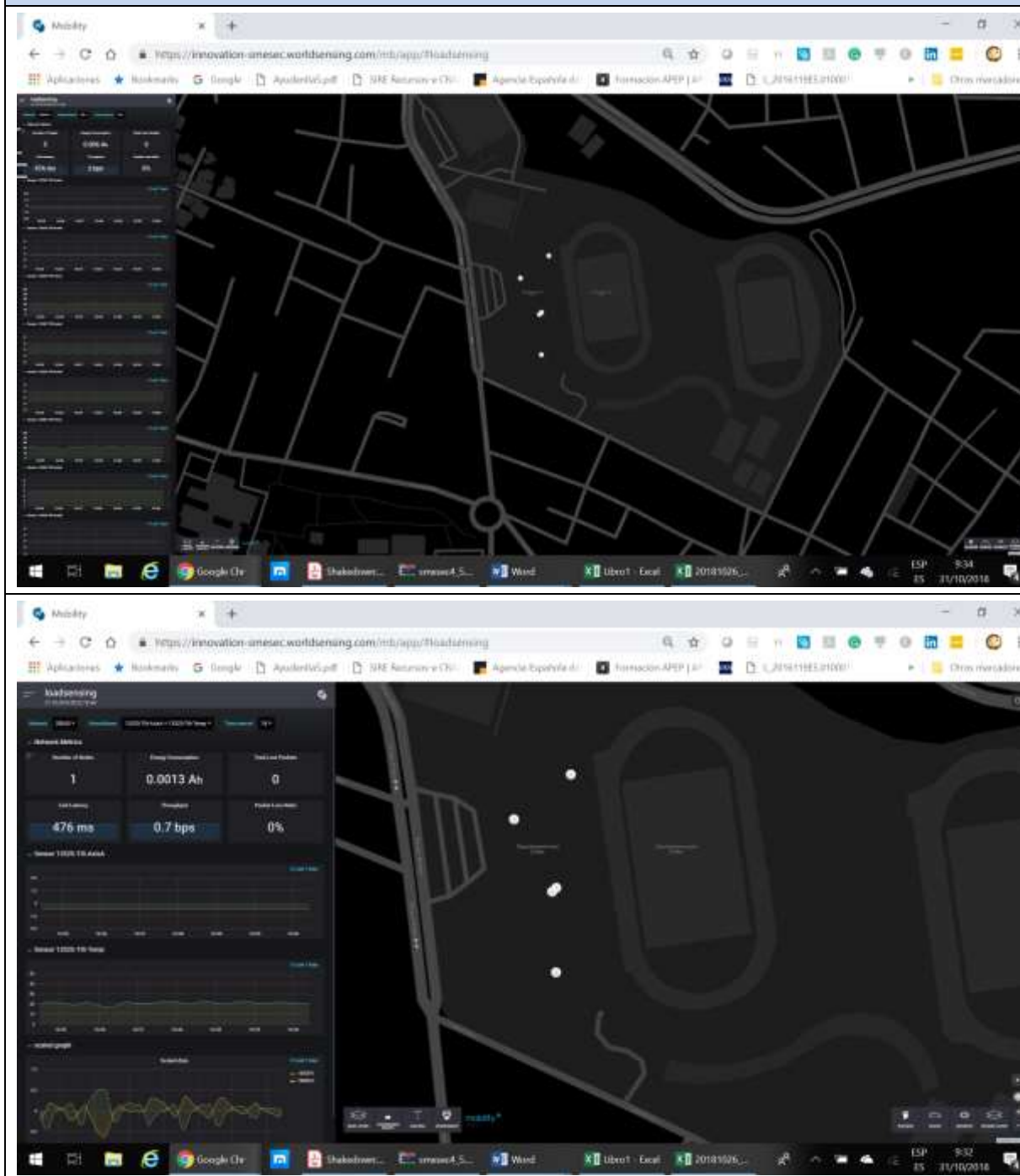


Figure 13. View of the Loadsensing front-end at Patras' stadium

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot			Page:	28 of 43		
Reference:	D4.5	Dissemination:	PU	Version:	1.1	Status:	Final

4.3.2 Anti ROP

Return-oriented programming (ROP) is a computer security exploit technique that allows an attacker to execute code in the presence of security defenses such as executable space protection. By using this technique, the attacker gains control of the call stack to hijack program control flow to then execute chosen machine instruction sequences that are already present in the machine's memory. The main interest for the pilot is the direct validation that the same attack cannot be easily replicated to all Loadensing gateways once the first one is compromised. In fact, Anti-ROP should act as a first passive security solution of these devices.

The testing done so far has consisted in launching several ROP attacks against a Loadensing gateway to thus understand how it behaves if the IBM solution is deployed or not .Figure 14 shows the successful attack to the gateway without IBM protection: the exploit is able to hack the device and get the control. On the contrary, in Figure 15, the gateway source code has been reprogramed with Anti-ROP tool. Now, the attack is launched on the right screen without tangible effects since the gateway is not vulnerable to the attack anymore.



Figure 14. Attack to a Loadensing gateway without Anti-ROP. Successful attack. Video:
<https://youtu.be/kUurVXoNB04>




Figure 15. Attack to a Loadensing gateway with Anti-ROP- Unsuccessful attack. Video:
<https://youtu.be/HOLQeUimoMU>

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot	Page:	29 of 43
Reference:	D4.5	Dissemination:	PU
	Version:	1.1	Status: Final

4.3.3 XL SIEM

A security information and event management (SIEM) is a software product that provides with services that combine security information management (SIM) and security event management (SEM). This information is provided in real-time while the solution is simultaneously performing an analysis of security alerts generated by the applications and the network hardware. As discussed earlier, this is critical for a reliable Load sensing operation.

In pilot III, the status of the integration does not allow a full testing of the deployed elements. For this reason, efforts have concentrated on checking the connection with the Gravity Zone which is expected to be the main logs generator within the pilot.

Enable Syslog

Server Name / IP	Protocol	Port
35.210.3.176	TCP	5007

Figure 16. Gravity Zone console configured to send logs to the XL-SIEM agent

Figure 16 shows that Gravity Zone is already configured to send logs to the server in which the ATOS' agent is deployed (public IP), being the tool in this way ready to receive data from the stadium-dedicated infrastructure. In parallel, Worldsensing has provided feedback to ATOS about those structural events that should be also collected by the XL-SIEM so that a clear picture of what is going on in the physical installation can be achieved and monitored.

4.3.4 Gravity Zone

The testing of Gravity Zone is in a more advanced stage in respect of the XL-SIEM. At present, the malware detection capability has already been validated. The next three figures illustrate some of the tests completed so far: (i) end-user protection by filtering the malware, (ii) deleting the infected files and (iii) the notifications to the system administrator through the central console of the system.



Figure 17. Gravity Zone: web browser protection activated

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot			Page:	30 of 43		
Reference:	D4.5	Dissemination:	PU	Version:	1.1	Status:	Final



Figure 18. Gravity Zone: end-point detection activated. Malware detection

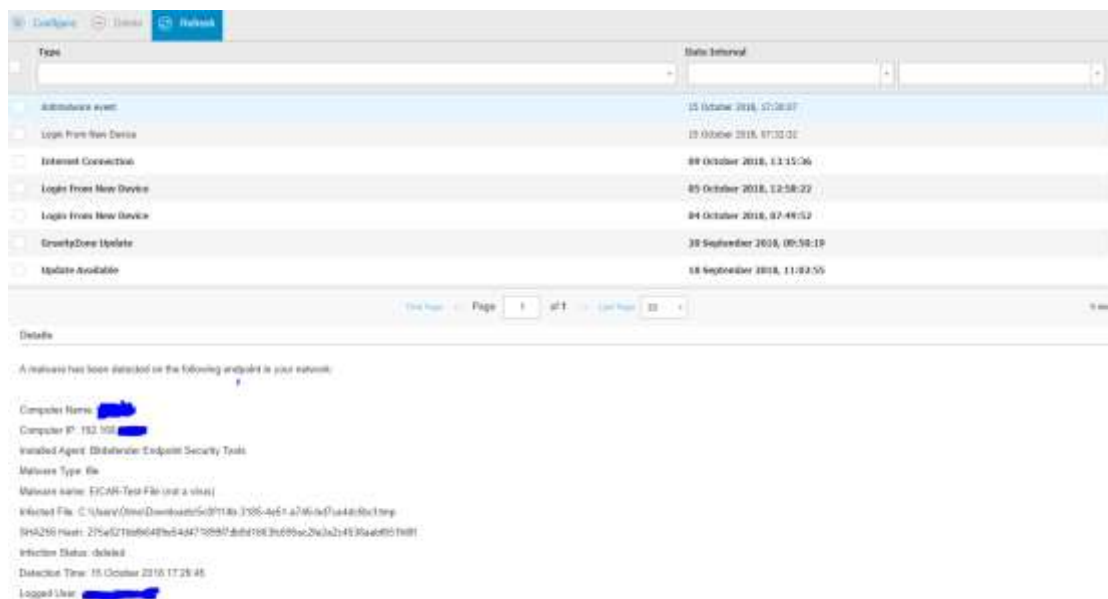


Figure 19. Gravity Zone: real-time reporting to the central server working

4.3.5 NetScaler

As explained in a previous section, a testing machine with the tool has been deployed in Worldsensing’s own premises before moving to the cloud. The instance is labelled as ‘SPFW01’, whose characteristics are shown in Figure 20.

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot			Page:	31 of 43		
Reference:	D4.5	Dissemination:	PU	Version:	1.1	Status:	Final

Hardware Configuration	
CPU	2 vCPUs
Memory	2 GB
Hard disk 1	20 GB
Network adapter 1	VM Network (Connected)
Network adapter 2	VM Network (Connected)
Video card	4 MB
Others	Additional Hardware

Resource Consumption	
Consumed host CPU	4 GHz
Consumed host memory	1.31 GB
Active guest memory	122 MB

Storage	
Provisioned	20 GB
Uncommitted	19.2 GB
Not-shared	2.91 GB
Used	2.91 GB

Figure 20. NetScaler machine installed at Worldsensing’s premises

The first tests, launched in our hypervisor, have successfully validated that the system is up and running (Figure 21). The VM was launched in Worldsensing’s internal network with public IP.

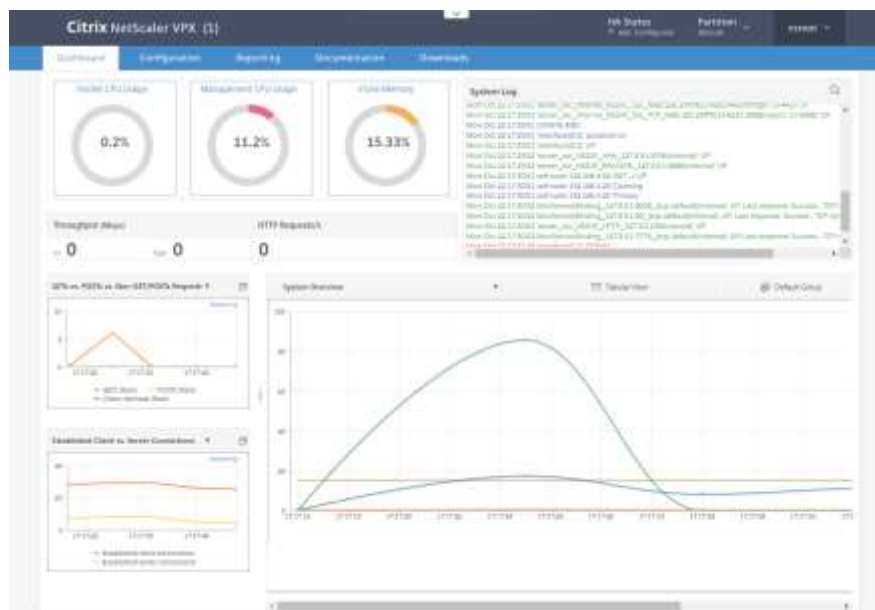


Figure 21. NetScaler deployment on Worldsensing’s premises. Functional view

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot	Page:	32 of 43	
Reference:	D4.5	Dissemination:	PU	
	Version:	1.1	Status:	Final

4.4 Initial feedback

The pilot validation is still in its infancy. For this reason, the feedback provided in this section about the added value resulting from the merge of the SMESEC framework and the Loadsensing commercial solution can only be qualitative. In the following lines, first remarks per tool are given stressing technological and security aspects. While the first one aims to identify the integration challenges we are facing right now, the second critically assesses how the robustness of the Worldsensing technology is improved by adopting the tool. The overall assessment of the pilot is given in Chapter 6.

4.4.1 MBT

The effort necessary to integrate this tool in the pilot III is high since it must be deeply customized before meaningful outputs are obtained. Since no real tests have been completed so far, the real impact of the tool and the associated benefits remain unclear from the Worldsensing's perspective.

4.4.2 Anti ROP

IBM's continued support has paved the way towards the effective integration of Anti-ROP in Loadsensing's gateways. Nevertheless, it remains unclear how a handmade work can be scaled up to hundreds of gateways produced and deployed per month. In fact, the final adoption of this technology would entail changing the internal production protocols at company level, which is assessed as a huge challenge involving certain risks. Besides, the upgrading of the existing gateways remains as an unresolved issue. Nevertheless, these drawbacks cannot hide the ability of Anti-ROP to block the replication of an attack based on Return Oriented Programming techniques, and it provides an intrinsic added-value to Loadsensing compared to the competitors' portfolio.

4.4.3 XL SIEM

The integration of the XL-SIEM with Loadsensing is still on an early phase. From a technological point of view, there are some aspects to be solved such as (i) the amount of data generated by the ATOS agent installed at Worldsensing's infrastructure, which results in a non-optimized use of the resources, and (ii) the adaptation of all the logs to the *syslog* codification, which is the XL-SIEM standard. Having said that, no major problems are expected once these issues are solved. It goes without saying that the XL-SIEM use is a value in itself, and it provides a unique overview of the events (structural and cybersecurity ones) occurring at the pilot.

4.4.4 Gravity Zone

The initial deployment of Gravity Zone was slightly more difficult than initially envisaged. However, Bitdefender has facilitated a server on the cloud that circumvents most of the problems with an optimal operation of the tool. Gravity Zone allows a deep control of the selected infrastructures, providing good visibility and transparency over the endpoints' security alerts and events. The first positive impression is supported not only with the reactive security capabilities (raw events), but thanks to the predictive actions offered such as policies enforcement and cryptologic controls through the central server. In short, Gravity Zone effectively protects the pilot's servers meeting the initial expectations.

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot			Page:	33 of 43		
Reference:	D4.5	Dissemination:	PU	Version:	1.1	Status:	Final

4.4.5 NetScaler

NetScaler has been the latest tool to be adopted within the pilot and consequently, it remains the less tested. From the on-site deployment point of view, the experience and results are quite satisfactory despite the short period of time that the instance has been running. The potential of this tool is obvious, but it needs further testing before reaching a meaningful opinion about the final impact in Loadsensing.

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot			Page:	34 of 43		
Reference:	D4.5	Dissemination:	PU	Version:	1.1	Status:	Final

5 Next steps

From M18 to M24, the pilot III (Industrial Services) faces the critical phase in which the security features provided by the SMESEC framework will be evaluated in depth. Actually, the tools are expected to cover most of the weaknesses identified in Chapter 3.

Here, the next integration steps of the tools are presented paying a special attention to the business proposition of the whole solution within the Loadsensing product. This chapter also overviews the training and awareness plan launched within Worldsensing taking advantage of the SMESEC activity.

5.1 Integration of business in the SMESEC Framework

As stated in the Chapter 3, the real business proposition of the SMESEC framework for the pilot III (Industrial Services) goes beyond offering the increase of the resilience of the Loadsensing infrastructure against external cyberattacks, which in itself is useful, and it will certainly help Worldsensing to increase its present IoT market share. Actually, the framework has been intended as supporting point to penetrate the sector of the critical infrastructures, in which the data confidence is crucial. The automate monitoring of these assets requires, however, that fake alarms are eliminated so that Operational Intelligence functionalities can be offered to customers, providing revenues in the long term. Thus, the final objective is to attain an infrastructure alert system that can automatically trigger alarms through dedicated channels (i.e. SMS, Apps) thanks to a dedicate software module that analyse the data coming from the assets by conducting real-time anomaly detection. To this end, ruling out fake data resulting from cyberattacks or the malfunction of the infrastructure in place is a must. How this technology will reach the market (i.e. SaaS) has not yet been defined, but it goes without saying that it will benefit the rest of the SMESEC consortium offering security tools.

5.2 Training and awareness plan

Security measures enhance the endurance of the information systems against external attacks in all the organizations, but these intrusion attempts represent only 30% of the conflictive events. The remaining 70% are directly or indirectly employee-made situations that put their companies at risk. The human factor is, by far, the weakest link of the cybersecurity chain, and this is the main reason to conduct training and awareness plans among the staff in a regular approach. In fact, well-designed security awareness programs guarantee an adequate level of cybersecurity knowledge of employees and instill accountability principles within organizations.

Alongside the implementation of SMESEC, Worldsensing is maturing quickly from a start-up to a well-established company. In this accelerated process, a Security Awareness Plan has been envisaged to improve the status of cybersecurity knowledge, which is made up with small and focused projects. The main actions to be conducted have been classified in the following security blocks:

- Grouping of employees and specific training;
- Improving cybersecurity in specific areas, covering critical topics and phases of the security cycle (attacks), and;
- Feedback analysis and continuous improvement of the completed actions.

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot			Page:	35 of 43		
Reference:	D4.5	Dissemination:	PU	Version:	1.1	Status:	Final

Regarding the grouping of employees, Worldsensing has first targeted those roles with special training requirements due to their potential criticality (Table 7), while the rest are subject to a generic training program described down below (Table 8).

Training and awareness plan: targeted employees	
Group	Objective / Rationale
C-Level	Sensitization of cybersecurity importance. Critical targets
Department managers	Cascade effect to their teams
Privileged users	Specific needs due to the sensitive data they handle (i.e. IT, HR)
Engineering Dpt	Security by default principles
Legal Dpt (i.e. DPO)	Alignment of policies with the legal framework
Third Parties	Information of the security policies and standards in WS

Table 7. 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 8. Training and awareness plan: general training sessions at Worldsensing

As far as the specific actions to improve critical security areas go, tailored training sessions focusing on the different phases of an attack (prevention, detection and response) have been devised, aiming to spread clear instructions among the staff on how to handle these scenarios. On the other hand, technical measures are being progressively introduced at a company level to improve the resilience of the internal systems to attacks (Table 9).

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

Table 9. Training and awareness plan: technical measures implemented at WS with associated training

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot	Page:	36 of 43	
Reference:	D4.5	Dissemination:	PU	
	Version:	1.1	Status:	Final

Last but not least, the main outputs of the plan will be properly analyzed getting the employees feedback through questionnaires, F2F meetings and equivalent tools. Despite the implementation of all these actions are still in its infancy, they have allowed getting ISO27001 certified in July 2018, which can be considered a major success given our starting point.

Table 10 summarizes the status of the different actions of the plan at the time of this writing. All of them will be running by M24 of the SMESEC project.



Figure 22. ISO27001 certification awarded by Bureau Veritas

ACHIEVE AWARENESS BY		PLANIFICATION	IMPLEMENTED	
GROUPS	TARGETED EMPLOYEES	C-Level	YES	YES
		Data Protection Officer	YES	YES
		Managers	YES	YES
		Privileged Users	YES	NO
		Engineering DPT	YES	NO
	Third Parties	YES	YES	
	GENERAL SESSIONS	Onboarding	YES	YES
Periodic	YES	YES		
Post incident	NO	NO		
AREAS	PHASES	Prevention	NO	NO
		Detection	NO	NO
		Response	NO	NO
	TOPICS	Policies	YES	YES
		MFA	YES	YES
		Phishing	NO	NO
		Social Engineering	YES	NO
		Ransomware	YES	NO
		Mobile Devices	YES	YES
		Backups	YES	YES
		Working Remote	YES	YES
		Antivirus	YES	YES
		Passwords Management	YES	YES
		Legal Framework (GDPR)	YES	YES
FEEDBACK	SESSION ENHANCEMENT	Content Feedback	NO	NO
	IMPACT MEASUREMENT	Phishing campaigns	YES	NO
		Awareness Survey	YES	NO

Table 10. Training and awareness plan: degree of implementation

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot			Page:	37 of 43	
Reference:	D4.5	Dissemination:	PU	Version:	1.1	Status: Final

5.3 Initial testing and validation plan

Worldsensing aims to guarantee the functionality of the SMESEC framework through a set of specific tests. The objective is to check the protection against targeted attacks provided by the orchestrated operation of the different tools, as well as the usability and resilience of the system.

In the following table³ (Table 11), individual and joint tests are identified and briefly described. It goes without saying that the test campaign is a live process that will be enriched with the help of the technological partners.

Validation campaign: planned tests			
Code	I/ J	Tool	Description
IT_01_IBM	Individual	Anti-ROP	Resilience to a code injection attack
IT_02_ATOS	Individual	XL-SIEM	Create relevant alerts from suspicious behaviours
IT_03_BD	Individual	Gravity Zone	Detect malware in an endpoint system and respond
IT_04_BD	Individual	Gravity Zone	Malware exploiting un patched server OS is handled by the antivirus
IT_05_CTX	Individual	NetScaler	Stop a DDoS attack
IT_06_FO	Individual	FORTH	Detect and get information of a DDoS attack
IT_07_EGM	Individual	Security tests	Identify Loadsensing vulnerabilities through modelling
JT_01_ATOS_B D	Joint	XL-SIEM & Gravity Zone	Malware detection and alerts rising
JT_02_CTX_FO	Joint	NetScaler & HoneyPot	Traffic forwarding to the honeypot, detection and gathering of information

Table 11. SMESEC framework validation: list of planned tests

Below the individual and joint tests are briefly described, and the success criteria identified.

IT_01_IBM: Code injection prevention (code execution)	
Objective:	Resist to a code injection attack
Test definition:	Attack designed and executed by an external to IBM and Worldsensing entity. Code injection in the gateways by using ROP techniques.
Fail criteria:	The attack code is executed, and the gateways obey the injected order (reboot, change of parameters...)
Success criteria:	The gateways resist, and no action occurs

IT_02_ATOS: Suspicious behaviour alerts	
Objective:	Create relevant alerts from suspicious behaviour within the systems.
Test definition:	The XL-SIEM collects specific pieces of logs regarding configurations within the systems and the alerts are arisen when unplanned set of changes happen.

³ Here, the integration of the honeypot offered by FORTH has already been considered, despite this tool is not integrated in the first version of the pilot prototype.

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot	Page:	38 of 43				
Reference:	D4.5	Dissemination:	PU	Version:	1.1	Status:	Final

IT_02_ATOS: Suspicious behaviour alerts	
Fail criteria:	The system detects less than 70% of the changes or the alerts are not sent to the administrator.
Success criteria:	The system is able to detect these changes in more than 70% of the cases. Alerts are sent to the administrator when changes are made.

IT_03_BD: Endpoint protection	
Objective:	Detect the presence of malware within an endpoint equipment and react accordingly.
Test definition:	A piece of malware exploiting unpatched endpoint OS or an application is placed in the server to evaluate the response of the anti-virus.
Fail criteria:	No detection of the malware neither proper reaction: deletion of the file, quarantine or similar.
Success criteria:	Detection of the malware and proper reaction.

IT_04_BD: Server protection	
Objective:	Detect the presence of malware within the server and react accordingly.
Test definition:	A piece of malware exploiting unpatched Server OS or an application is placed in to evaluate the response of the anti-virus.
Fail criteria:	No detection of the malware neither proper reaction: deletion of the file, quarantine or similar.
Success criteria:	Detection of the malware and proper reaction.

IT_05_CTX: Denial of service avoidance	
Objective:	Stop a denial of service attack by blocking the traffic coming from unauthorized IPs.
Test definition:	DDoS attack designed and executed by external to Citrix and Worldsensing entity that will attempt to freeze one of the protected servers.
Fail criteria:	The traffic is able to reach the server.
Success criteria:	The traffic is blocked by NetScaler.

IT_06_FORTH: DDoS detection	
Objective:	Detect and get information from a DDoS attack.
Test definition:	DDoS attack designed and executed by external to Forth and Worldsensing entity.
Fail criteria:	The attack is not detected or there is no information about it.
Success criteria:	The attack is detected and there is information regarding the attackers available.

IT_07_EGM: Loadsensing infrastructure simulation	
Objective:	Simulation of the Loadsensing infrastructure to deploy tests and find vulnerabilities.
Test definition:	Perform a simulation of the operative Loadsensing deployment.
Fail criteria:	The simulation is not complete or accurate to the Loadsensing deployment
Success criteria:	The simulation is complete or accurate to the Loadsensing deployment

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot	Page:	39 of 43				
Reference:	D4.5	Dissemination:	PU	Version:	1.1	Status:	Final

JT_01_ATOS_BD: Malware detection and alerts rising	
Objective:	(i) BD: detection of a malware attack. (ii) ATOS: alert rising and sent to the administrator
Test definition:	Malware placement within one of the protected endpoints or servers.
Fail criteria:	No detection of the attack or no reporting to the administrator
Success criteria:	Simultaneous detection and alarm triggering

JT_02_CTX_FO: Traffic forwarding to honeypot, detection and information gathering	
Objective:	(i) CITRIX: detects traffic form an unauthorised range and forward it to the honeypot. (ii) FORTH: detection of the type of attack. Alarm sent to admin.
Test definition:	DDoS attack designed and executed by external to Forth, Citrix and Worldensing entity that will attempt to freeze the protected servers.
Fail criteria:	Traffic not diverted or no reporting to the administrator
Success criteria:	Simultaneous detection and alarm triggering

It must not be forgotten that the primary objective of the SMESEC framework is to respond to the Loadsensing vulnerabilities identified in the section 3.3.2. The Table 12 shows how the most critical ones will be at least partially covered by SMESEC, validating the initial approach of the pilot.

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	X	
Kerlink Gateway (WS)	MIMT [Man in the Middle]	VERY LOW						X
Kerlink Gateway (WS)	Code injection	HIGH		X				
Kerlink Gateway (WS)	Brute force against authentication	MEDIUM	X			X	X	
Kerlink Gateway (Secure)	DOS [Denial of Service]	MEDIUM	X			X	X	
Kerlink Gateway (Secure)	MIMT [Man in the Middle]	VERY LOW						X
Kerlink Gateway (Secure)	Code injection	LOW		X				
Kerlink Gateway (Secure)	Brute force against authentication	MEDIUM	X			X	X	
Wireless Tiltmeter	Equipments robbery	MEDIUM						
Wireless Tiltmeter	DOS [Denial of Service]	LOW						X
Wireless Tiltmeter	MIMT [Man in the Middle]	LOW						X
Wireless Tiltmeter	Administration errors	MEDIUM						
Gateway Internet Connection	Service Down	MEDIUM						
Gateway Internet Connection	Traffic sniffing	LOW				X		
Gateway Internet Connection	Administration errors	MEDIUM						
Macallan Sever	Brute force against authentication	HIGH	X		X	X	X	
Macallan Sever	Code injection	MEDIUM						
Macallan Sever	DOS [Denial of Service]	MEDIUM			X	X	X	
Macallan 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

Table 12. Matching of Loadsensing vulnerabilities and protection provided by SMESEC tools

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot			Page:	40 of 43		
Reference:	D4.5	Dissemination:	PU	Version:	1.1	Status:	Final

6 Conclusions

The pilot III (Industrial services) has been successfully designed and preliminary put into operation at the selected venue, Kostas Davourlis stadium, Patras. Aiming to validate the principles of the SMESEC framework, some of the available tools have been integrated into the commercial Loadsensing product, covering all the domains of the solution (sensors, gateways and the cloud). The adoption of security tools by an IoT company like Worldsensing is not only envisaged as a strategy to increase the robustness of the present commercial offer, but to explore new markets with strict and up to now unattainable requirements related to security, such as the critical infrastructure monitoring. SMESEC project and the associated pilot activity have proved to be an excellent catalyst to instilling cybersecurity principles within the company, reversing a discouraging historical trend.

6.1 Experience of the initial integration

From the perspective of Worldsensing, the first 18 months of the SMESEC project have been mainly used to identify and understand the full potential of the individual tools offered by the Consortium, and to assess the added-value they can provide to our IoT solutions. In this sense, the work done so far can be divided in the following stages: (i) security analysis of the bare Loadsensing solution, (ii) selection of the suitable tools to be deployed at the pilot, (iii) their integration and deployment within the Loadsensing architecture and (iv) the first functional tests at individual and joint-level.

Up to know, the work has however not resulted in tangible results except for the validation that the tools are compatible with the Worldsensing's technology. From now on, the pilot faces the challenging stage in which is necessary to demonstrate how the Loadsensing technology can be enriched by the SMESEC framework.

6.2 Fulfilling of objectives

Looking ahead, the pilot III (Industrial Services) pursues three effective objectives: (i) adoption of cybersecurity tools in a commercial IoT technology, (ii) providing a competitive advantage regarding competitors by opening new markets (critical infrastructures) and implementing new functionalities, and (iii) rising the cybersecurity awareness. As discussed in the former sections, for the time being only the objectives 1 and 3 have been partially achieved in line with the initial schedule. As far as the objective 2 is concerned, it will be fully developed once the integrated framework is under operation. In fact, the full potential of the SMESEC concept will gain a perceptible impact as soon as the framework becomes something else than a mere sum of sum of cybersecurity tools, most of them already commercial. Having said that, Worldsensing is very optimistic about the results achieved so far, and it is fully convinced that the initially fixed objectives will become a reality in the coming months.

6.3 Use in SME environment

The final usability of the SMESEC framework by the SME environment is extremely difficult to be judged at present, since the final solution is far from become a reality. Up to now, most of the work

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot			Page:	41 of 43		
Reference:	D4.5	Dissemination:	PU	Version:	1.1	Status:	Final

conducted by Worldsensing has focused to substantiate the integration of security tools in a closed technological product, making necessary a dedicated activity that unfortunately falls out of the knowledge scope of most of the SMEs. This is expected to change once the joint framework is ready and the applicability scenarios are clear. Considering the user interfaces of some of the deployed solutions (Gravity Zone and Netscaler), it is conceivable thinking that the SMESEC framework will be, at least in part, an adequate solution for SMEs with basic knowledges in cybersecurity.

6.4 Improvements for the scenario

As discussed in the document, the first prototype is still under development. Nevertheless, the potential adoption of other security tools such as honeypots (FORTH) in a second release are still under evaluation. For the sake of convenience, and aiming to avoid overambitious objectives, the final decision will be reached only when the current prototype is fully operative.

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot			Page:	42 of 43		
Reference:	D4.5	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. *D4.6 – Final integration report on Industrial Services SME pilot*. Francisco Hernández-Ramirez. 2019 (pending)
- [3] WIKIPEDIA. *Kostas Davourlis Stadium*. https://en.wikipedia.org/wiki/Kostas_Davourlis_Stadium, retrieved 2018-11-05.
- [4] EU GDPR.ORG. <https://eugdpr.org/>, retrieved 2018-11-05.
- [5] European Commission. *The Directive on security of network and information systems (NIS Directive)*. <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive>, retrieved 2018-11-05
- [6] arXiv.org. *Shakedown: compiler-based moving target protection for Return Oriented Programming attacks on an industrial IoT device*. <https://arxiv.org/abs/1810.02090>, retrieved 2018-11-05

Document name:	D4.5 Preliminary Integration report on Industrial Services SME pilot			Page:	43 of 43		
Reference:	D4.5	Dissemination:	PU	Version:	1.1	Status:	Final