



# SMESEC

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

## D4.4 Final integration report on Smart City pilot

<b>Related WP</b>	WP4	<b>Document Reference</b>	D4.1, D4.3, D4.5, D4.7
<b>Related Deliverable(s)</b>	D2.1, D3.1, D3.2 D3.4, D3.5	<b>Dissemination Level (*)</b>	PU
<b>Lead Organization</b>	University of Patras (UOP)	<b>Lead Author</b>	Kostas Lampropoulos
<b>Contributors</b>	Kostas Lampropoulos (UOP)	<b>Reviewers</b>	Ovidiu Costel Mihaila (Bitdefender) Noemi Folch (Scytl)

<b>Document Identification</b>			
<b>Status</b>	Final	<b>Due Date</b>	31/05/2019
<b>Version</b>	1.0	<b>Submission Date</b>	31/05/2019

<b>Keywords:</b>
security, system, design, architecture, integration, WP4, requirements, goals, innovation, use case, smart city, protection, defence, management.

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
Kostas Lampropoulos	University of Patras
Manos Athanatos	Forth
Alireza Shojaifar	FHNW

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	23/05/2019	Kostas Lampropoulos (UOP)	First version of the document
0.3	23/05/2019	Alireza Shojaifar (FHNW)	Input on architecture design figure and section 5
0.4	24/05/2019	Ovidiu Costel Mihaila (Bitdefender)	First review
0.5	23/05/2019	Kostas Lampropoulos (UOP)	First review comments addressed.
0.6	29/05/2019	Noemi Folch (SCY)	Second review
0.7	30/05/2019	Kostas Lampropoulos	Second review comments addressed.
1.0	30/05/2019	ATOS	Quality Review + Submission to EC

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Kostas Lampropoulos (UOP)	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

<b>Document name:</b>	D4.4 Final integration report on Smart City pilot				<b>Page:</b>	2 of 18	
<b>Reference:</b>	D4.1, D4.3, D4.5, D4.7	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0	<b>Status:</b>	Final

# Table of Contents

Document Information .....	2
Table of Contents .....	3
List of Figures .....	5
List of Acronyms.....	6
Executive Summary .....	7
1 Introduction.....	8
1.1 Purpose of the document .....	8
1.2 Relation to other project work.....	8
1.3 Structure of the document .....	8
2 Requirements and needs: from planning to action.....	9
3 Scenarios and usability.....	10
3.1 Updates and enhancement .....	10
3.2 Architecture.....	10
3.3 Scenarios of SMESEC.....	11
3.4 Impact of SMESEC in the use case.....	11
3.5 Business impact.....	11
4 Technical integration of SMESEC.....	12
4.1 Integration of SMESEC in the use case .....	12
4.1.1 Integration GravityZone with XL-SIEM.....	12
4.1.2 FORTH cloud IDS solution.....	12
4.1.3 IBM code analysis.....	12
4.1.4 FHNW CYSEC tool .....	13
4.2 Analysis and evaluation of SMESEC.....	13
4.3 Testing and feedback provided.....	14
4.3.1 Testing the integration of GravityZone with XL-SIEM .....	14
4.3.2 Testing FORTH's cloud IDS.....	14
4.3.3 Testing of FHNW CYSEC tool.....	14
5 Cybersecurity awareness and training.....	15
5.1 Training and awareness .....	15
5.1.1 Training and awareness plan .....	15

<b>Document name:</b>	D4.4 Final integration report on Smart City pilot				<b>Page:</b>	3 of 18	
<b>Reference:</b>	D4.1, D4.3, D4.5, D4.7	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0	<b>Status:</b>	Final

5.1.2	Securityaware.me training platform .....	15
6	Conclusions .....	16
6.1	Final analysis and next steps .....	16
6.2	Fulfillment of objectives.....	16
6.3	Future outcomes and business development .....	16
	References .....	18

<b>Document name:</b>	D4.4 Final integration report on Smart City pilot				<b>Page:</b>	4 of 18	
<b>Reference:</b>	D4.1, D4.3, D4.5, D4.7	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0	<b>Status:</b>	Final

---

## List of Figures

---

<i>Figure 1: Smart City SMESEC infrastructure</i>	11
<i>Figure 2: Code analysis for sense.city service (by IBM)</i>	13
<i>Figure 3: Forth cloud IDS</i>	14

<b>Document name:</b>	D4.4 Final integration report on Smart City pilot				<b>Page:</b>	5 of 18	
<b>Reference:</b>	D4.1, D4.3, D4.5, D4.7	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0	<b>Status:</b>	Final

## List of Acronyms

Abbreviation / acronym	Description
D4.3	Deliverable number 3 belonging to WP 4
EC	European Commission
EU	European Union
GDPR	General Data Protection Regulation
QA	Quality Assurance
SIEM	Security Information and Event Manager
SME	Small-Medium Enterprise
TaaS	Technology as a Service
VM	Virtual Machine
WP	Work Package

<b>Document name:</b>	D4.4 Final integration report on Smart City pilot				<b>Page:</b>	6 of 18	
<b>Reference:</b>	D4.1, D4.3, D4.5, D4.7	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0	<b>Status:</b>	Final

## Executive Summary

This deliverable describes the final work done, and reported on M24, of the integration of the SMESEC Framework in the Smart City pilot. The report is based in the initial version provided at M18 and we build on top of it the following iterations done in the project, both from a technical and awareness point of view. Together with the advancements and updates done in the system we also report the work done in the awareness and training area in order to cover the needs of the employees identified at the beginning of the project.

Additionally, we report the final analysis and next steps to be done in the project for the work with the SMESEC Framework and how far it fulfilled the objectives of the use case. We also describe the business development and the impact SMESEC has in this area, as business improvement is a topic for SMESEC as critical as the technical development.

Finally, this document describes in detail the specifics of the Smart City use case: scenarios, update of requirements (if any), testing, impact of SMESEC in the use case, etc.

In summary, this document describes the current version of the Smart City pilot. The work described here will be continued in WP5 for further testing, analysis, and improvement using the enhancements done incrementally in SMESEC in the third year and taking advantage of the large testing and feedback provided by the open call.

<b>Document name:</b>	D4.4 Final integration report on Smart City pilot				<b>Page:</b>	7 of 18	
<b>Reference:</b>	D4.1, D4.3, D4.5, D4.7	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0	<b>Status:</b>	Final

# 1 Introduction

## 1.1 Purpose of the document

This is the second deliverable of WP4 (after D4.3 [1]) related to Smart City pilot. The role of this WP in the SMESEC project is to adapt the SMESEC security framework prototype to the different pilots proposed in the project.

Specifically, deliverables D4.3 and D4.4 provide an in-depth description of the integration of SMESEC in the Smart City use case, the impact in the use case and organization (also from an organization point of view), the cybersecurity training and awareness performed in the scope of the project, fulfilment of objectives as described in the first year and next steps, which will be followed in WP5.

## 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 Smart City 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 and services in the four use cases
- D5.3: execution of trials in the pilots
- WP6: the results of this deliverable will be used for exploitation and dissemination activities

## 1.3 Structure of the document

This document is structured in 6 major chapters

**Chapter 1** presents an introduction to the use case, objectives and its integration with SMESEC.

**Chapter 2** describes updates and review of the requirements and needs identified in the first year and any new one that was included since the previous deliverable.

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

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

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

**Chapter 6** presents the conclusions at M24 of the integration of the SMESEC platform in the use case.

<b>Document name:</b>	D4.4 Final integration report on Smart City pilot				<b>Page:</b>	8 of 18	
<b>Reference:</b>	D4.1, D4.3, D4.5, D4.7	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0	<b>Status:</b>	Final



## 2 Requirements and needs: from planning to action

During the last two years of the deployment of SMESEC framework the sense.city service has evolved, creating new features and services. Even though the basic requirements for security remain the same (secure cloud infrastructure, nodes etc.) UOP is always working towards transforming sense.city into a business product. Security is a major factor for achieving this, thus within the SMESEC project we are working closely with our partners to identify how the innovations of their products can support our needs. In this context, we have decided to extend the use of some of the SMESEC tools into more nodes (except from the testing nodes created for the SMESEC project). In particular currently we are deploying the GravityZone solution to various operational nodes as well as other nodes inside the UOP cloud which are not associated with the sense.city service. Other services that are also examined to be used outside the testing facility are the EWIS system of FORTH and XL-SIEM. In terms of security incidents, UOP is happy to report that it didn't suffered any major issues the previous year.

One of the solutions specifically requested by UOP from SMESEC project was cloud security. This solution was deployed by FORTH. However, after some discussions between UOP and FORTH, it was decided to not directly deploy it in the UOP cloud since the whole process required the installation of components on operational nodes and UOP considered this to be risky. To address this issue, UOP setup a new physical machine with the same hypervisor as its private cloud (clone). In this physical machine FORTH deployed and successfully tested its cloud IDS tool. UOP considers this solution to be very useful and will examine the testing results to evaluate whether it can also be deployed in UOP cloud's operational nodes.

<b>Document name:</b>	D4.4 Final integration report on Smart City pilot				<b>Page:</b>	9 of 18	
<b>Reference:</b>	D4.1, D4.3, D4.5, D4.7	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0	<b>Status:</b>	Final

## 3 Scenarios and usability

### 3.1 Updates and enhancement

The updates for the Smart City pilot for the duration between M18 and M24 are the following.

1. Antimalware solution from Bitdefender (GravityZone) is now integrated with the XL-SIEM from ATOS. Incidents identified by GravityZone are now successfully sent to the XL-SIEM UOP agent and presented in UOP's XL-SIEM account.
2. IBM has provided a first version of code analysis for the sense.city service. This analysis was examined by the sense.city team of developers and various vulnerabilities of the service were covered. UOP is currently building a docker container with the sense.city service so that IBM can make further code analysis of the platform.
3. FORTH successfully deployed its cloud IDS tool on a testing node inside UOP premises. Initial tests successfully caught the performed attacks (network scan, DDoS attack) and produced the expected syslog logs.
4. For the CYSEC tool, UOP hosted a one-day workshop in Patras where FHNW presented the current version of the tool. Even though the tool is not yet operational for UOP to evaluate its current security maturity level, the conclusions of this workshop is that, compared to the beginning of the project, CYSEC tool is much more user-friendly.
5. New courses for cyber security training have been uploaded to the securityaware.me platform and UOP will go through these courses and propose its developers and municipality employees (civil servants) to take advantage of them.

No updates were made on the EGM Test-as-a-Service solution.

### 3.2 Architecture

As mentioned above, UOP deployed the cloud security solution from FORTH. However, since this deployment required the installation of components on various operational nodes, UOP refused to deploy the solution directly on its cloud infrastructure (VMs and hypervisor), considering it to be risky for the sense.city operation. To address this situation, UOP setup a new physical machine (node) with the same hypervisor as its private cloud (clone). In this physical machine FORTH deployed and successfully tested its solution. The new architecture of UOP testing facility for the SMESEC project is depicted in Figure 1

<b>Document name:</b>	D4.4 Final integration report on Smart City pilot				<b>Page:</b>	10 of 18	
<b>Reference:</b>	D4.1, D4.3, D4.5, D4.7	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0	<b>Status:</b>	Final

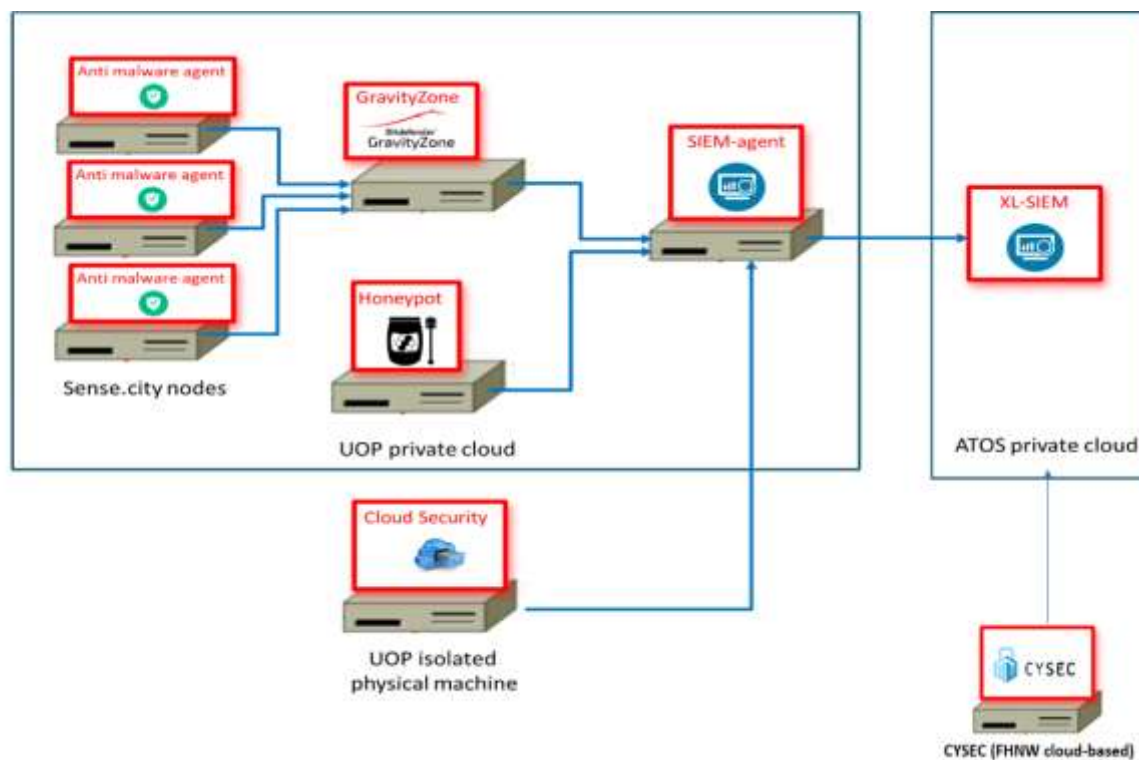


Figure 1: Smart City SMESEC infrastructure

### 3.3 Scenarios of SMESEC

There is no update on the application scenarios of SMESEC framework inside the sense.city service. The reader can find the identified scenarios in section 3.2 of deliverable D4.3.

### 3.4 Impact of SMESEC in the use case

Again, for this section there is no considerable additional impact in the SMESEC identified use cases. The reader can find relevant information on this subject in section 3.3 of deliverable D4.3

### 3.5 Business impact

Sense.city is expanding its functionality adding services for people with special needs. This functionality not only has a significant impact to the municipality services but has also draw the attention of public protection services like the fire department and police. These departments requested to able to locate people with special needs in case of an emergency (e.g. locate people with mobility problems in case of an earthquake). These new features and use cases increase the value of sense.city platform but at the same time impose even higher security requirements. SMESEC framework and the experts of the consortium partners are among of the key solutions that UOP relies on for the security planning, implementation and updating of the sense.city platform.

<b>Document name:</b>	D4.4 Final integration report on Smart City pilot			<b>Page:</b>	11 of 18
<b>Reference:</b>	D4.1, D4.3, D4.5, D4.7	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0
				<b>Status:</b>	Final

## 4 Technical integration of SMESEC

### 4.1 Integration of SMESEC in the use case

Sense.city now has its own account in the SMESEC framework. With this account the UOP team can see all the tools that have been installed for the Smart City use case, as well as information about cybersecurity awareness, training and other available security solutions. The list of SMESEC tools which were integrated in sense.city platform until M18 can be found in section 4.2 of deliverable D4.3. Compared to this list the following updates were made up to M24.

#### 4.1.1 Integration GravityZone with XL-SIEM

Until M18 the XL-SIEM monitoring tool and the GravityZone antivirus were both installed in UOP infrastructure, however they were not able to communicate (exchange syslog reports, alarms etc). UOP, ATOS and Bitdefender explored the issue and eventually solved it by updating the XL-SIEM agent installed in UOP.

#### 4.1.2 FORTH cloud IDS solution

The cloud IDS solution developed by FORTH is capable of detecting possible attacks that take place within a host running many VMs. Virtual hosts operating under the same Hypervisor are able to produce orders of magnitude more network throughput than conventional communication over the internet. This happens as VMs are using the internal CPU BUS to communicate, which can lead to throughput over 30 GB/s. To this end, an infected VM could produce massive DoS or other attacks against other co-hosted VMs.

FORTH's solution is able to identify intra-VM attacks and inter-VM attacks, as well as, attacks originating from the internet, that cannot be identified by the IDS monitoring the uplink of a cloud infrastructure. The cloud IDS solution can be deployed either to the Cloud or locally and requires the installation of a special hypervisor and an intrusion detection system on top of it. The feasibility of this solution has been tested on the KVM hypervisor, which is the same one as the hypervisor of UOP's private cloud. As also mentioned above, UOP setup a new physical machine (node) with the same hypervisor as its private cloud (clone) and in this physical machine FORTH deployed and successfully tested its cloud IDS tool.

#### 4.1.3 IBM code analysis.

For the IBM code analysis solution, UOP was a special case since its requirements were based on the analysis of javascript code. IBM did not support this capability at the beginning of the project but was able to provide it at a later stage. Since this process started late in the project its deployment is still ongoing with some early results already sent to UOP. Figure 2 below presents parts of the static code analysis from IBM. All recommendations have been examined from UOP and all required updates to the code have already been made. Currently UOP is preparing a docker container with a copy of the

<b>Document name:</b>	D4.4 Final integration report on Smart City pilot			<b>Page:</b>	12 of 18
<b>Reference:</b>	D4.1, D4.3, D4.5, D4.7	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0
				<b>Status:</b>	Final

sense.city service to send it to IBM for further analysis. Since this is a complicated task (because the sense.city service has a large number of components connected to it), UOP and IBM are in discussions to identify the required functionality that the container must have so that the IBM’s analysis can produce valuable results.

```

Queries that are potentially vulnerable to sql injection:
1. /r JOIN 'R
   profi ' AND
2. /r req t
3. /r d + "
   WHE
4. /r req t

Places potentially vulnerable to directory traversal exploits:
5. /r
6. /r
7. /r
8. /r meta[1],
   'be

A few places potentially vulnerable to nosql injection exploits:
9. /r
10. /r
  
```

**Figure 2: Code analysis for sense.city service (by IBM)**

#### 4.1.4 FHNW CYSEC tool

CYSEC tool has been used in the context of the use case. CYSEC is integrated by the network hub but not with ICT network in the SME. Through SMESEC hub, the network administrator can have access to CYSEC, do cybersecurity self-assessment, see the recommendations (in the specific area based on the priorities), and communicate with the relevant staff in the company. Since CYSEC 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 project.

## 4.2 Analysis and evaluation of SMESEC

The integration of SMESEC framework has been an easy process for UOP. We must note though, that the team of people from UOP that were involved in the project has very good expertise in programming and system administration and was able to easily collaborate with the technical personnel of the tool providers. Valuable information about the installation process and the operation of SMESEC security tools can be found in the training courses that were created by the tool providers. In this context, we are confident that the deployment of SMESEC framework can also be completed by SMEs and personnel that do not have very good technical and security background.

About the importance of SMESEC to the Smart City pilot we can say that after our initial security evaluations and their alarming low scores, the UOP team started taking security more seriously, dedicating more effort on protecting our assets. With the guidance of the consortium partners our security status has now been improved and we are able to identify a) what are the open issues that we still need to address and b) how critical they are, not only for the security of the sense.city platform but also for the rest of the services running in UOP’s private cloud.

<b>Document name:</b>	D4.4 Final integration report on Smart City pilot			<b>Page:</b>	13 of 18
<b>Reference:</b>	D4.1, D4.3, D4.5, D4.7	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0
				<b>Status:</b>	Final

The installed monitoring tools (XL-SIEM) along with the agents of IDS and antimalware solutions provide a clear view of the kind of attacks that our systems are facing every day. This information is valuable and gives us the ability to better plan on how to defend ourselves, what kind of security solutions we need to deploy and what kind of measurements and mitigation actions we must prepare.

Finally, apart from the tools and activities for increasing cyber security awareness, the newly created training material of SMESEC project also helps our developers to better understand how to build more secure products and our users (e.g. municipality employees) to act with security in mind (protect their devices, use strong authentication methods etc.)

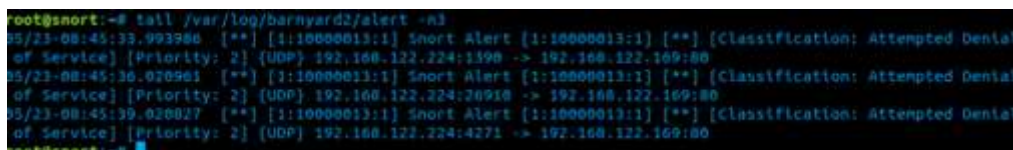
## 4.3 Testing and feedback provided

### 4.3.1 Testing the integration of GravityZone with XL-SIEM

For this test we repeated the same testing procedure we did in M18 to evaluate the proper installation of the GravityZone tool. The difference now was to check if the GravityZone event was successfully sent to the XL-SIEM and presented in the UOP XL-SIEM account. For this test we downloaded a test-malware file from the internet and check if it is recognized and blocked by our antimalware. More details about this test can be found in section 4.3.2 of deliverable 4.3. The test was successful and the XL-SIEM received and presented to UOP XL-SIEM account the malware event.

### 4.3.2 Testing FORTH's cloud IDS

To test this solution, UOP setup a new physical machine (node) with the same hypervisor as its private cloud (clone). In this physical machine FORTH deployed and successfully tested its solution. Figure 3 depicts the results of a successful test on the cloud IDS solution.



```

root@snort:~# tail /var/log/barnyard2/alert -n3
05/23-08:45:33.993986  ** [1:10000013:1] Snort Alert [1:10000013:1] ** [Classification: Attempted Denial
of Service] [Priority: 2] {UDP} 192.168.122.224:1398 -> 192.168.122.169:80
05/23-08:45:36.078961  ** [1:10000013:1] Snort Alert [1:10000013:1] ** [Classification: Attempted Denial
of Service] [Priority: 2] {UDP} 192.168.122.224:26918 -> 192.168.122.169:80
05/23-08:45:39.020027  ** [1:10000013:1] Snort Alert [1:10000013:1] ** [Classification: Attempted Denial
of Service] [Priority: 2] {UDP} 192.168.122.224:4271 -> 192.168.122.169:80
root@snort:~#

```

**Figure 3: Forth cloud IDS**

The cloud IDS solution can be integrated with the XL-SIEM. To achieve this the system communicates through syslog, reporting the events and alerts to the XL-SIEM cyber agent over UDP at port 514. This integration has not yet been completed for the Smart City pilot but all involving partners are working on it.

### 4.3.3 Testing of FHNW CYSEC tool

CYSEC: For this tool, the network administrator logged in the website (cloud-based CYSEC) through SMESEC hub and saw the dashboard and went through the three coaches (access control and audit, patch management, end-user training). The evaluation of CYSEC was based on a 1-day workshop case study.

<b>Document name:</b>	D4.4 Final integration report on Smart City pilot			<b>Page:</b>	14 of 18
<b>Reference:</b>	D4.1, D4.3, D4.5, D4.7	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0
				<b>Status:</b>	Final

## 5 Cybersecurity awareness and training

### 5.1 Training and awareness

#### 5.1.1 Training and awareness plan

In section 5.2 of deliverable 4.3 we presented the training and awareness plan for the Smart City pilot as well as its peculiarities due the fact that the service is operated by a University and not a company. Our training and awareness plan is generally focused on three groups of people.

- a) **Developers:** The developers of sense.city platform have a good knowledge on security but in the beginning of the project, security was not among their highest priority tasks. However, after the initial alarming results we received from SMESEC evaluation process, our developers decided to implement more testing and QA (quality assurance) phases in their work. Also IBM code analysis results have enabled them to better identify various code vulnerabilities. Finally even though GDPR is not currently supported by SMESEC, our team used various online tools and sources to make sure that sense.city service is compliant with all the strict requirements of the new regulation.
- b) **Infrastructure/service management:** The impact that the SMESEC project had on the team responsible for the sense.city infrastructure management is that this team now performs more often security and vulnerability checks. Furthermore all tools tested inside the SMESEC framework are also evaluated to be installed in the operational VMs of the cloud. Finally the team now implements stricter rules and policies for access control and is trying enforce various security practices like plans for updating and patching, response and mitigation actions etc.
- c) **Public servants:** For the people working in public administration we still haven't done many actions to promote security awareness. The plan is to recommend them a set of selected courses created by SMESEC for basic cybersecurity aspects, good practices, phishing attacks' protection, antivirus protection etc.

#### 5.1.2 Securityaware.me training platform

UOP has updated its securityaware.me training platform with the help of FHNW UX designers. In particular, during a meeting held in Patras between UOP and FHNW, it was decided to make various changes on the presentation of the courses, the menus of the website, and the overall design of multiple pages. Various recommendations were given to UOP which are still under development.

Currently a new webpage to host the SMESEC training courses has been added in the platform. This webpage has similar design with the design of the overall framework.

Considering the training courses, UOP has already received courses from the consortium partners and has uploaded them in the platform. However, since these courses are very technical for the average user, we have decided to wait until more courses are created and then organize an event to promote the platform and its courses to sense.city developers, users and municipality employees.

<b>Document name:</b>	D4.4 Final integration report on Smart City pilot			<b>Page:</b>	15 of 18
<b>Reference:</b>	D4.1, D4.3, D4.5, D4.7	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0
				<b>Status:</b>	Final



## 6 Conclusions

### 6.1 Final analysis and next steps

At M24 the integration of SMESEC framework in the Smart City pilot has a list of products and solutions that are fully installed, configured and integrated and some other solutions that are still in the deployment phase. With the current status of the SMESEC framework, UOP has already increased its security levels. Many nodes are much better protected that they were in the beginning of the project. Also, solutions like the IDS are giving us very good insights on the types of attack attempts we are dealing with. We can say that all partners have done their best to help the UOP team properly install and configure the selected tools in sense.city service. It must be noted that some of the tools of SMESEC are already been used on the production infrastructure.

The next steps are to finalize the deployment of all remaining tools and evaluate what can be then moved to our operational nodes. UOP goal is to be able to have a clear improvement of its security status not only by the end of the project but also long after.

### 6.2 Fulfillment of objectives

UOP's main objectives are not changed since the beginning of the project and are extensively described in section 6.2 on deliverable 4.3. These objectives are:

- a) Protection against untargeted attacks
- b) Increase awareness
- c) Create a market product

As mentioned above UOP hasn't had a major cyber incident in the past year and is already expanding some of the tools of the SMESEC framework from the testing nodes to the operational ones. This is a proof that the owners of sense.city service trust the SMESEC solutions to support its security against untargeted attacks.

Furthermore, the creation of training courses as well as the transformation of the CYSEC solution to a more user-friendly tool will allow UOP to not only promote cybersecurity awareness inside its own institute but also to external collaborative parties like the municipalities and their employees.

Finally, towards our goal for creating a market product, SMESEC is a very strong asset that ensures the quality of our service and its ability to protect its infrastructures and data. This allows UOP to further promote the sense.city service and explore more opportunities for business collaborations.

### 6.3 Future outcomes and business development

As mentioned above, the new features added to sense.city platform for supporting people with special needs have increased the value of the service and also draw the attention of other public services (public protection) except from municipalities. UOP is currently discussing with many stakeholders, exploring various diverse ways to transfer the sense.city to the market. Whatever the final form of the service may

<b>Document name:</b>	D4.4 Final integration report on Smart City pilot			<b>Page:</b>	16 of 18		
<b>Reference:</b>	D4.1, D4.3, D4.5, D4.7	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0	<b>Status:</b>	Final



be, the requirements for strong security and reliable functionality will be critical for the success of the product. SMESEC has already provided a good basis for building our security plans and implementing the first set of security measures. Even after the end of the project UOP aims to take advantage of its connections with the consortium partners and explore additional technical and business collaborations.

<b>Document name:</b>	D4.4 Final integration report on Smart City pilot				<b>Page:</b>	17 of 18	
<b>Reference:</b>	D4.1, D4.3, D4.5, D4.7	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0	<b>Status:</b>	Final

---

## References

---

[1] **Deliverable:** SMESEC. D.4.3 – Preliminary Integration report on Smart City pilot. Lampropoulos, Konstantinos. 2018

<b>Document name:</b>	D4.4 Final integration report on Smart City pilot				<b>Page:</b>	18 of 18	
<b>Reference:</b>	D4.1, D4.3, D4.5, D4.7	<b>Dissemination:</b>	PU	<b>Version:</b>	1.0	<b>Status:</b>	Final