Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

SMESEC

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

# D5.2 System readiness for validation activities

| **Document Identification** | | | |
|---|---|---|---|
| **Status** | Final | **Due Date** | 31/08/2019 |
| **Version** | 1.0 | **Submission Date** | 02/10/2019 |

| | | | |
|---|---|---|---|
| **Related WP** | WP4, WP5 | **Document Reference** | D5.2 |
| **Related Deliverable(s)** | D5.1 | **Dissemination Level (*)** | PU |
| **Lead Organization** | SCYTL | **Lead Author** | Noemi Folch, SCYTL |
| **Contributors** | Noemi Folch, SCYTL | **Reviewers** | M. Athanatos (FORTH) |
| | | | F. Hernández (WOS) |

| **Keywords:** |
|---|
| Trial, Evaluation, Testing, Planning |

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.

# Document Information

| List of Contributors | |
|---|---|
| Name | Partner |
| Noemi Folch | SCYTL |
| Francisco Hernández | WORLDSENSING |
| Adam Nawarycz | GRIDPOCKET |
| Kostas Lampropoulos | UNIVERSITY OF PATRAS |
| Jordi Cucurull | SCYTL |

| Document History | | | |
|---|---|---|---|
| Version | Date | Change editors | Changes |
| 0.1 | 26/7/19 | N. Folch, SCY | First draft |
| 0.2 | 30/7/19 | F. Hernández, WOS | Comments and suggestions |
| 0.3 | 07/8/19 | N. Folch, SCY | Second draft with improvements and extensions |
| 0.4 | 12/8/19 | F. Hernández, WOS | WOS Pilot contribution |
| 0.5 | 26/8/19 | A. Nawarycz | GP Pilot Contribution |
| 0.6 | 03/9/19 | K.Lampropoulos | UoP Pilot Contribution |
| 0.7 | 05/09/19 | M. Athanatos | QA1 |
| 0.8 | 05/09/19 | F. Hernández, WOS | QA2 |
| 0.9 | 06/09/19 | N.Folch, J.Cucurull, SCY | Adjustments after QA reviews |
| 1.0 | 02/10/19 | R. Valle | Quality review + submission to EC. |

| Quality Control | | |
|---|---|---|
| Role | Who (Partner short name) | Approval Date |
| Deliverable leader | Noemi Folch (SCY) | 02/10/2019 |
| Technical manager | Christos Tselios (Citrix) | 02/10/2019 |
| Quality manager | Rosana Valle | 02/10/2019 |
| Project Manager | Jose Francisco Ruiz | 02/10/2019 |

# Table of Contents

# List of Tables

# List of Figures

# List of Acronyms

| Abbreviation / acronym | Description |
|---|---|
| GW | Gateway |
| 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 | Test as a Service |
| WP | Work Package |
| OWASP | Open Web Application Security Project |
| ITU | International Telecommunications Union |
| OSI | Open Systems Interconnection model |
| WHOIS | Query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block or an autonomous system |
| ICMP | Internet Control Message Protocol |
| ARP | Open Web Application Security Project |
| TCP | Transmission Control Protocol |
| UDP | User Datagram Protocol |
| IDLE scan | TCP port scan method that consists of sending spoofed packets to a computer |
| ARP | Address Resolution Protocol |
| DNS | Domain Name System |
| IP | Internet Protocol |
| SSL | Secure Socket Layer |
| DHCP | Dynamic Host Configuration Protocol |
| DOS | Denial of Service |

| | |
|---|---|
| DDOS | Distributed Denial of Service |
| IDS | Intrusion Detection System |
| IPS | Intrusion Prevention System |
| IRS | Intrusion Recognition System |
| SWG | Secure Web Gateway |
| LDAP | Lightweight Directory Access Protocol |
| RADIUS | Remote Authentication Dial In User Service |
| TACACS+ | Terminal Access Controller Access |
| Negotiate | Microsoft Windows authentication mechanism |
| FPR / TPR | False Positive Rate / True Positive Rate |

# Executive Summary

The purpose of the task T5.2 is to prepare and configure the use cases for the execution of the validation campaign designed and planned in T5.1 (and reported in D5.1 [2]). After the definition of the trial scenarios in the task T5.1, and using the second iteration of the SMESEC Framework, we plan to execute and report the results of the specific tests that have been adapted to the requirements of each pilot aiming to validate the cyber security status, awareness and training capabilities of the SMESEC approach as well as the business advantages of the framework. As abovementioned, the testing campaign has been planned carefully in advance in order to cover all the needs and characteristics of the systems and SMESEC Framework together with the dependencies of each pilot.

This task has strong dependencies with previous ones, not only of WP5 but also WP2 (requirements), WP3 (SMESEC Framework) and WP4 (integration of SMESEC in use cases). For this reason, it has been slightly delayed during its execution but it will result in no impact in the final implementation and the fulfilment of the initial objectives.

The deliverable D5.2 complements the work described in D5.1 and will be fully extended in the upcoming D5.3. All three of them provide a broader picture of the work done in the project.

# 1 Introduction

## 1.1 Purpose of the document

This is the second deliverable of WP5 "Refinement, Evaluation, Demonstration and Security Assessment of the SMESEC platform in operational environment". The role of this WP is to evaluate and demonstrate the SMESEC security framework, from the prototype designed and developed in WP3, and its application to the four pilots in WP4.

After the definition of the trial scenarios in task T5.1, this document describes the work done in task T5.2 to prepare the four pilots for the system demonstration and the evaluation in the frame of the task T5.3. This has resulted in the final configuration of the experiments to be done in each pilot, the schedule of the trials, and the execution and recording of the first proofs, overlapping with T5.3.

For the sake of completeness, full details of the tests and the obtained results are given in the deliverable D5.3.

## 1.2 Relation to other project work

As described before, this document covers the advanced efforts carried out to prepare the use case scenarios for the system demonstration to be done in the task T5.3.

The work done in this task has relied extensively in the work done in the task T5.1 and documented in D5.1 "Trial scenario definition and evaluation methodology specification". Of course, the work done in WP4 has been essential to have the four pilots' systems ready, with the different components of the SMESEC framework integrated, and the proof of concept scenarios definition.

The work described here will be used for other deliverables and work packages such us:

- D5.3: Prototype Demonstration: Field trial results;
- D5.4: SMESEC Security Framework Assessment report;
- WP3: the feedback of the testing will be used to further refine the SMESEC Framework
- WP6: the results of this deliverable will be used for the exploitation and dissemination activities.

## 1.3 Structure of the document

The document is divided in three parts.

**Chapter 1** presents an introduction of the deliverable;

**Chapter 2** overview of the tests planning process and the preparation of the testing campaign for each pilot;

**Chapter 3** summarizes the conclusions of the task.

# 2 Test preparation

This chapter will focus on the tests to be done in the four pilots, the initial planning of the individual testing campaign, and the dependencies and support needed in each case.

Actually, the list of tests identified in deliverable D5.1 (Table 26) is the basis one assuming that all the SMESEC tools are operative in the same venue. This means the planned testing and validation is an ideal scenario and it was required work for adapting it to the reality, needs and technologies of the pilots.

Following we present the different tests that are planned for each of the pilots (following the list presented in D5.1) and then a description of the adaptation done in the use cases. The adaptation includes fulfilment of requirements and the deployment of new technologies for using the solutions provided by SMESEC.

## 2.1 Tests

The following table summarizes the full list of tests that were defined in the task T5.1 to evaluate the components integrated in the SMESEC framework. It should be pointed out that they were intended to validate the functioning of the SMESEC tools and their orchestration, but not the specific framework modules, such as the SMESEC Hub, that will be evaluated in the frame of the tasks T5.3 and T5.4.

**Table 1 Planned tests for SMESEC framework**

| Trials | | | |
|---|---|---|---|
| **Test-Codes** | **I/ J** | **Provider** | **Description** |
| IT_01_XL-SIEM | Individual | ATOS | General test of relevant alerts |
| IT_01_2_XL-SIEM | Individual | ATOS | Test of test plugin |
| IT_01_3_XL-SIEM | Individual | ATOS | Test of SSH plugin |
| IT_01_4_XL-SIEM | Individual | ATOS | Test of FORTH EWIS plugin |
| IT_01_5_XL-SIEM | Individual | ATOS | Test of ADC plugin |
| IT_02_1_GravityZone | Individual | Bitdefender | Malware detection in clients and servers, deployment and detection of test malware, alerts in relation to detected malware send and represented in GravityZone |
| IT_02_2_GravityZone | Individual | Bitdefender | Detection of downloaded malware |

| | | | |
|---|---|---|---|
| IT_02_3_GravityZone | Individual | Bitdefender | Accessing a blacklisted URL |
| IT_02_4_GravityZone | Individual | Bitdefender | Inserting an USB stick with a malicious file |
| IT_02_5_GravityZone | Individual | Bitdefender | Detection of port scanning |
| IT_03_1_Honeypot | Individual | FORTH | Detection of DDoS attack |
| IT_03_2_Honeypot | Individual | FORTH | Detection of SQL-Injection attack |
| IT_03_3_Honeypot | Individual | FORTH | Detection of brute force attacks |
| IT_04_1_AntiROP | Individual | IBM | Validate that antiROP unique copies do not change executable functionality |
| IT_04_2_AntiROP | Individual | IBM | Validate that antiROP unique copies defend against ROP attack |
| IT_05_1_TaaS | Individual | EGM | Lora testing |
| IT_05_2_TaaS | Individual | EGM | API testing |
| IT_05_3_TaaS | Individual | EGM | Check if user is authorized to access the TaaS platform |
| IT_05_4_TaaS | Individual | EGM | Show all reports |
| IT_06_CITRIX-ADC | Individual | CITRIX | Detects malicious or improper network traffic and blocks it before reaching the backend application servers, potentially causing service downtime. stops it |
| IT_07_1_IDS | Individual | FORTH | Scanning detection |
| IT_07_2_IDS | Individual | FORTH | DDoS attack detection |
| IT_08_1_Virtual_Patching | Individual | IBM | Validate that the predictive model provides reasonable FPR/TPR rates on input-samples |
| IT_08_2_Virtual_Patching | Individual | IBM | Validate that the Integration into custom log file analysis produces the same results as in T_08_01_Virtual_Patching |
| IT_09_1_CYSEC | Individual | FHNW | Validation of the installation and login functionality of the CYSEC tool |
| IT_09_2_CYSEC | Individual | FHNW | Validation of the on boarding, assessment, learning, control and practice implementation, |

| | | | |
|---|---|---|---|
| | | | reporting, and recommendation functionalities of the CYSEC tool |
| IT_09_3_CYSEC | Individual | FHNW | Validation of CYSEC coaches |
| IT_09_4_CYSEC | Individual | FHNW | Validation of the insight stream functionality of the CYSEC tool |
| IT_10_1_ExpliSAT | Individual | IBM | Validate that testing platform does not produce false alerts |
| IT_10_2_ExpliSAT | Individual | IBM | Validate that testing platform covers common vulnerability families |

| **Trials** | | | |
|---|---|---|---|
| **Test-Codes** | **I/ J** | **Provider** | **Description** |
| JT_01_XL-SIEM_GravityZone | Joint | ATOS & Bitdefender | Malware detection, reporting on the XL-SIEM system and alerts rising |
| JT_02_XL-SIEM _Honeypot | Joint | ATOS & FORTH | Possible attacks on the honeypot reported on the XL-SIEM system |
| JT_03_CITRIX-ADC_Honeypot_XL-SIEM | Joint | CITRIX & FORTH | Citrix ADC is deployed in front of an application server and intercepts all inbound traffic. Traffic is inspected based on predefined policies and discarded if found inappropriate. Inappropriate traffic is forwarded to the Honeypot while generic reports are issued to the XL-SIEM. |
| JT_04_XL-SIEM_IDS_Honeypot | Joint | ATOS & FORTH | The Cloud-IDS and Honeypot detect a DoS attack and reports the XL-SIEM about it |

## 2.2 Planning

To establish the final work plan for the trials, a set of meetings were organized, involving each of the pilots with the tool owners of interest for each case. The objectives of these meetings were:

- To determine which tests among the list in section 2.1 applied to the pilot;
- To schedule the testing plan;
- To determine the support needed and the dependencies for each test;

**Table 2 Planning meetings**

| Use case | Date | Attendants |
|---|---|---|
| Scytl e-Voting | 14/05/19 | SCYTL: J. Cucurull, C. Rueda, N. Folch<br>ATOS: P. Barrientos<br>WOS: F. Hernandez<br>CITRIX: C. Tselios<br>FORTH: M. Athanatos<br>IBM: B. Zeltser<br>EGM: H. Baqa |
| Worldsensing Industrial Services | 15/05/19 | SCYTL: N. Folch<br>ATOS: P. Barrientos<br>WOS: F. Hernandez, O. Rayon<br>FORTH: A. Krithinakis<br>IBM: B. Zeltser<br>EGM: H. Baqa<br>BITDEFENDER: G. Mazarache |
| GridPocket Smart Grid | 15/05/19 | SCYTL: N. Folch<br>ATOS: P. Barrientos<br>WOS: F. Hernandez<br>CITRIX: C. Tselios<br>FORTH: A. Krithinakis<br>EGM: H. Baqa<br>BITDEFENDER: G. Mazarache<br>GRIDPOCKET: A. Nawarycz |
| University of Patras Smart City | 21/05/19 | SCYTL: N. Folch<br>WOS: F. Hernandez<br>FORTH: M. Athanatos<br>EGM: H. Baqa<br>BITDEFENDER: G. Mazarache<br>UOP: K: Lampropoulos |

For discussions about CYSEC tool, a dedicated meeting took place with representatives of the four pilots and FHNW:

| Subject | Date | Attendants |
|---|---|---|
| Cysec tool tests | 24/05/19 | SCYTL: J. Cucurull, N. Folch<br>WOS: F. Hernandez, O. Rayon<br>UOP: K: Lampropoulos<br>GRIDPOCKET: M. Burdy<br>FHNW: A. Shojaifar, S. Fricker |

As a result of these planning meetings, an initial calendar was set up for all pilots with four different phases:

- **Final integration work**: during this phase, pilots were expected to finalize the integration tasks as planned in the scope of WP4. At the end of this phase, all the tools to be used by each pilot were presumably fully integrated and deployed in the use case, so that the test campaign could start as normal.
- **First tests lab prototype:** during this phase, pilots were expected to conduct the tests defined in T5.1 to evaluate the components integrated in the SMESEC framework. At the end of this phase, pilots should have gathered evidences (videos, logs) of the performance of the different tests. Outputs will be presented in the deliverable D5.3.
- **Joint functionalities validated:** during this phase, pilots were expected to conduct the specific tests that are designed to validate the joint functionalities of different tools, i.e. XL-SIEM and Honeypot. At the end of this phase, pilots should have gathered evidences (videos, logs) of the performance of the different tests in a similar approach to the previous phase. Outputs will be presented in the deliverable D5.3.
- **Reporting:** during this phase, pilots were expected to report the planning and testing efforts done during the whole task. The summary of results is presented in this deliverable.

The result of the test adaptation to each pilot is summarized in the following subsections:

### 2.2.1 e-Voting

#### 2.2.1.1 Tests

According to what was described in document D4.2 [1], Scytl has integrated the following tools in its e-Voting pilot: XL-SIEM, EWIS HoneyPot, Citrix ADC and Angeleye Virtual Patching. Cysec tool is also used as a service, but it is not installed on premises.

For this reason, the tests that apply to e-Voting use case are detailed in the table below, together with some remarks useful to understand the full context:

**Table 3 e-Voting pilot tests**

| Test-Codes | I/ J | Provider | Comments |
|---|---|---|---|
| IT_01_XL-SIEM | Individual | ATOS | Planned |
| IT_01_2_XL-SIEM | Individual | ATOS | Planned |
| IT_01_3_XL-SIEM | Individual | ATOS | ATOS: Testing application is under development |
| IT_01_5_XL-SIEM | Individual | ATOS | Planned |
| IT_03_1_Honeypot | Individual | FORTH | Forth will provide the necessary scripts |

| | | | |
|---|---|---|---|
| | | | ATOS advise warning Amazon before doing a DDOS attack. Otherwise machines can be blocked by Amazon. |
| IT_03_2_Honeypot | Individual | FORTH | Forth will provide the necessary scripts |
| IT_03_3_Honeypot | Individual | FORTH | Planned |
| IT_06_CITRIX-ADC | Individual | CITRIX | Planned |
| IT_08_1_Virtual_Patching | Individual | IBM | Planned |
| IT_08_2_Virtual_Patching | Individual | IBM | Scytl: Some concerns about the feasibility of this tests, because of the presence of Netscaler.<br>IBM provides some feedback to overcome the potential issues. |

| Test-Codes | I/ J | Provider | Comments |
|---|---|---|---|
| JT_02_XL-SIEM_Honeypot | Joint | ATOS & FORTH | Planned |
| JT_03_CITRIX-ADC_Honeypot_XL-SIEM | Joint | CITRIX & FORTH | Full test will be completed once the final integration of Citrix ADC, Honeypot and XL-SIEM is achieved |

#### 2.2.1.2 Requirements

Before conducting the tests and thus to evaluate the integration of the SMESEC functionalities in the pilot, there have been some dependencies to be tackled:

- **Functional dependencies**:
    - Citrix ADC final deployment: the application firewall rules to be executed by Citrix ADC had to be carefully created and tested.
    - IBM Angeleye final deployment: the client application of IBM AngelEye that evaluates the registered HTTP Requests required a full integration in the web server.
    - Final integration of Citrix ADC – Honeypot – XL-SIEM: Citrix ADC was not fully connected to the XL-SIEM agent and the plugin for this agent, required for the interpretation of the logs sent by Citrix ADC, was under development.
    - Amazon permission to run DDOS attacks in AWS instances: SCYTL has been waiting for a response from Amazon regarding the suitability or not of doing DDoS attacks

against the deployed instances. At the end, we confirmed that this type of attack was forbidden by Amazon so it was pulled over.
  - XL-SIEM testing application to be updated: the testing application for issuing XL-SIEM messages required modifications to address the requirement of WP5.
  - Honeypot testing scripts: the scripts to test the honeypot were not ready at the beginning of the task. FORTH has correctly amended the drawback as this is being written.

- **Technical dependencies**:
  - None: no additional software or hardware was needed in order to conduct the tests.

To circumvent these dependencies, some actions were taken. The final integration efforts in eVoting scenario are described in document D4.2 – *Final integration report on e-Voting SME pilot*. The applications and scripts needed to run the tests have been duly provided by the involved tool owners.

Regarding the DDOS attacks to be performed in AWS instances, permission was requested to Amazon, but it was denied, as this kind of attacks are not allowed by Amazon policies, not even for testing purposes. Consequently, test IT_03_1_Honeypot had to be finally discarded.

#### 2.2.1.3 Planning

The following image shows the initial testing planning and its connection with the project schedule:


**Figure 1 e-Voting pilot tests' planning**

### 2.2.2 Industrial Services

Worldsensing's use case has the particularity that some elements have been physically deployed in Patras (Greece). This fact has resulted in a challenge for the test campaign since the access to the venue

suffers some restrictions. To circumvent this drawback, the proof schedule has been designed to be performed in different steps, and it will last until the fourth quarter of 2019, when the last elements (honeypots) will be finally installed in Patras. Actually, they are already working in lab premises at Forth with preliminary promising results. Due to the combination of physical (OT) and IT elements, the tests to be done could find some particular problems that will be carefully handled. A full description of the main particularities of the on-site tests will be duly provided in the deliverable D5.3.

#### 2.2.2.1 Tests

According to what was described in document D4.6, Worldsensing Industrial Services has integrated the following tools in its pilot: XL-SIEM, GravityZone, EWIS HoneyPot, AntiRop, TaaS, and Cysec.

For this reason, the tests that apply to e-Industrial Services' use case are detailed in the table below, together with some remarks useful to understand the full context:

**Table 4 Industrial Services pilot tests**

| Test-Codes | I/ J | Provider | Comments |
|---|---|---|---|
| IT_01_XL-SIEM | Individual | ATOS | Planned |
| IT_01_2_XL-SIEM | Individual | ATOS | Planned |
| IT_01_4_XL-SIEM | Individual | ATOS | Planned |
| IT_02_1_GravityZone | Individual | Bitdefender | Planned |
| IT_02_2_GravityZone | Individual | Bitdefender | Planned |
| IT_02_3_GravityZone | Individual | Bitdefender | Planned |
| IT_02_4_GravityZone | Individual | Bitdefender | Planned |
| IT_02_5_GravityZone | Individual | Bitdefender | Planned |
| IT_03_1_Honeypot | Individual | FORTH | Partially delayed: successful lab test proofs have been conducted in Forth premises (Crete), but real DDOS attacks to be completed in the real pilot venue (Patras) once the full hardware deployment is completed. |
| IT_03_3_Honeypot | Individual | FORTH | Partially delayed: successful lab test proofs have been done in Forth premises (Crete), real tests to |

| | | | |
|---|---|---|---|
| | | | the pilot's venue will happen, once the full on-site deployment is completed. |
| IT_04_1_AntiROP | Individual | IBM | Planned |
| IT_04_2_AntiROP | Individual | IBM | Planned |
| IT_05_1_TaaS | Individual | EGM | Planned |
| IT_05_2_TaaS | Individual | EGM | Planned |
| IT_05_3_TaaS | Individual | EGM | Planned |
| IT_05_4_TaaS | Individual | EGM | Planned |
| IT_09_2_CYSEC | Individual | FHNW | Stopped until the final version of CYSEC is available |
| IT_09_3_CYSEC | Individual | FHNW | Stopped until the final version of CYSEC is available |
| IT_09_4_CYSEC | Individual | FHNW | Stopped until the final version of CYSEC is available |

| Test-Codes | I/ J | Provider | Comments |
|---|---|---|---|
| JT_01_XL-SIEM_GravityZone | Joint | ATOS & Bitdefender | Planned |
| JT_02_XL-SIEM _Honeypot | Joint | ATOS & FORTH | Delayed: assistance form Forth needed once the full deployment in Greece is completed. |

#### 2.2.2.2 Requirements

Before conducting the tests and thus to evaluate the integration of the SMESEC functionalities in the pilot, there have been some dependencies to be tackled:

- **Functional dependencies:**

  - XL-SIEM integration was not in production stage at M24;
  - Gravityzone adaptation has resulted more complex than initially envisaged. To avoid blocking other working areas, the adoption of Gravityzone has been temporary blocked;
  - Cysec final version to be released.
  - Physical deployment of pilot's elements split in two installation campaigns due to restrictions from the stadium operator.

- **Technical dependencies:**
    - Honeypots not physically installed at Patras. Besides, need for adapting the testing scripts to the IoT architecture of the pilot and its particularities;

To circumvent this adverse scenario, the test campaign has been adapted to the external restrictions and as result, it will be finally conducted in two different stages. In any case, the adopted plan is in line with the grant agreement provisions and the project objectives. Actually, the necessary input to complete the task T5.4 will be duly delivered in line with the grant agreement provisions.

#### 2.2.2.3 Planning

The following image shows the initial testing planning and its connection with the project schedule:

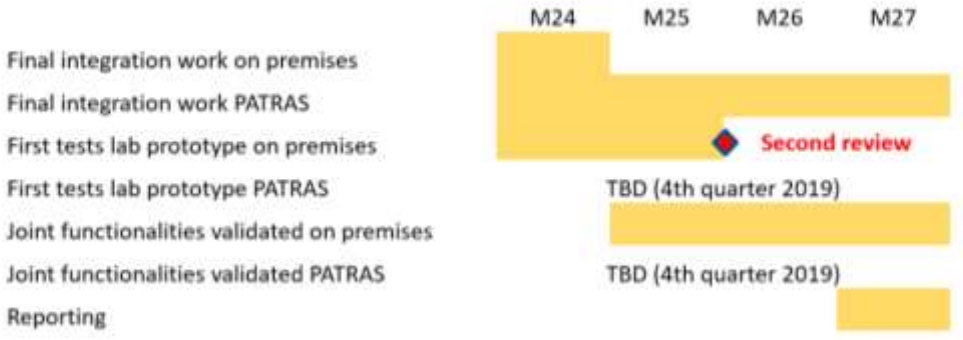


**Figure 2 Industrial Services pilot tests' planning**

### 2.2.3 Smart city

#### 2.2.3.1 Tests

According to what was described in document D4.4, University of Patras has integrated the following tools in its Smart City pilot: XL-SIEM, GravityZone, EWIS HoneyPot, TaaS, Cloud IDS and Cysec.

For this reason, the tests that apply to Smart City use case are detailed in the table below, together with some remarks useful to understand the full context:

Table 5 Smart City pilot tests

| Test-Codes | I/ J | Provider | Comments |
|---|---|---|---|
| IT_01_XL-SIEM | Individual | ATOS | Planned |
| IT_01_2_XL-SIEM | Individual | ATOS | Planned |
| IT_01_3_XL-SIEM | Individual | ATOS | Planned |
| IT_01_4_XL-SIEM | Individual | ATOS | Planned |
| IT_02_2_GravityZone | Individual | Bitdefender | Planned |
| IT_02_3_GravityZone | Individual | Bitdefender | Planned |
| IT_02_5_GravityZone | Individual | Bitdefender | Planned |
| IT_03_1_Honeypot | Individual | FORTH | Planned |
| IT_03_2_Honeypot | Individual | FORTH | Planned |
| IT_03_3_Honeypot | Individual | FORTH | Planned |
| IT_05_2_TaaS | Individual | EGM | Planned |
| IT_05_3_TaaS | Individual | EGM | Planned |
| IT_05_4_TaaS | Individual | EGM | Planned |
| IT_07_1_IDS | Individual | FORTH | Planned |
| IT_07_2_IDS | Individual | FORTH | Planned |
| IT_09_1_CYSEC | Individual | FHNW | Blocked: waiting for the final version of CYSEC platform |
| IT_09_2_CYSEC | Individual | FHNW | Blocked: waiting for the final version of CYSEC platform |
| IT_09_3_CYSEC | Individual | FHNW | Blocked: waiting for the final version of CYSEC platform |
| IT_09_4_CYSEC | Individual | FHNW | Blocked: waiting for the final version of CYSEC platform |

| Test-Codes | I/ J | Provider | Comments |
|---|---|---|---|

| | | | |
|---|---|---|---|
| JT_01_XL-SIEM_GravityZone | Joint | ATOS & Bitdefender | Planned |
| JT_02_XL-SIEM _Honeypot | Joint | ATOS & FORTH | Planned |
| JT_04_XL-SIEM_IDS_Honeypot | Joint | ATOS & FORTH | Planned |

#### 2.2.3.2 Requirements

Before conducting the tests and thus to evaluate the integration of the SMESEC functionalities in the pilot, there have been some dependencies to be tackled:

- **Functional dependencies:**
  - XL-SIEM integration with Bitdefender reports from Linux agents.
  - GravityZone Linux agents provide protection only against malware attacks.
  - Honeypot testing scripts.
  - Cloud IDS solution requires the installation of software components in UOP private cloud's hypervisor.
  - Cysec new version to be released.
  - EGM TaaS requires a description of UOP's API that will be tested for smart city pilot.
  - IBM requested from UOP the sense.city platform in docker for further analysis.

- **Technical dependencies:**
  - None: no additional software or hardware was needed in order to conduct the tests.

To address the required dependencies and initiate the testing process, UOP in collaboration with the SMESEC partners involved in Smart City pilot performed the following actions:

- XL-SIEM integration with GravityZone reports from Linux agents: ATOS and Bitdefender worked together to identify the format of GravityZone reports from Linux agents. A new XL-SIEM agent was created and installed in UOP private cloud.
- GravityZone Linux agents provide protection only against malware attacks: Since GravityZone Linux agents are not capable of identifying phishing and port scanning attacks (tests IT_02_3_GravityZone and IT_02_5_GravityZone), a new testing machine was deployed in UOP with Windows OS.

- Honeypot testing scripts: FORTH has prepared and will execute all necessary scripts during the testing phase.
- Cloud IDS solution requires the installation of software components in UOP private cloud's hypervisor: UOP decided not to install Cloud IDS solution in its private cloud since the whole process might affect components which are used in the production environment. To address this, UOP deployed a new isolated physical machine which replicates its cloud. The Cloud IDS solution was installed on this new machine and all tests will be executed there.
- Cysec new version to be released: FHNW will organize a workshop where UOP will evaluate and test the Cysec tool.
- EGM TaaS requires a description of UOP's API that will be tested for smart city pilot: EGM requested from UOP to provide its API collection (e.g. postman, swagger). UOP created and provided to EGM a postman collection.
- IBM requested from UOP the sense.city platform in docker for further analysis: Due to the fact that sense.city is a large platform with multiple interconnected components and systems, UOP discussed with IBM and agreed on a set of components and functionalities that must be included in the docker in order for the code analysis to produce valuable results. A testing platform was created and provided to IBM in docker.

#### 2.2.3.3 Planning

The following image shows the initial testing planning and its connection with the project schedule:


**Figure 3 Smart City pilot tests' planning**

### 2.2.4 Smart Grid

#### 2.2.4.1 Tests

According to what was described in document D4.8, GridPocket has integrated the following tools in its Smart Grid pilot: XL-SIEM, GravityZone, EWIS HoneyPot, TaaS, Cloud IDS and Cysec.

For this reason, the tests that apply to Smart City use case are detailed in the table below, together with some remarks useful to understand the full context:

**Table 6 Smart Grid pilot tests**

| Test-Codes | I/ J | Provider | Comments |
|---|---|---|---|
| IT_01_XL-SIEM | Individual | ATOS | Blocked: testing application from Atos under development |
| IT_01_2_XL-SIEM | Individual | ATOS | Blocked: testing application from Atos under development |
| IT_01_3_XL-SIEM | Individual | ATOS | Blocked: testing application from Atos under development |
| IT_01_4_XL-SIEM | Individual | ATOS | Blocked: testing application from Atos under development |
| IT_01_5_XL-SIEM | Individual | ATOS | Blocked: testing application from Atos under development |
| IT_02_1_GravityZone | Individual | Bitdefender | Planned |
| IT_02_2_GravityZone | Individual | Bitdefender | Planned |
| IT_02_3_GravityZone | Individual | Bitdefender | Planned |
| IT_02_4_GravityZone | Individual | Bitdefender | Planned |
| IT_02_5_GravityZone | Individual | Bitdefender | Partially Blocked: scan not detected. Interaction with Bitdefender to solve the problems |
| IT_03_1_Honeypot | Individual | FORTH | Blocked: Waiting for the final XL-SIEM plugins |
| IT_03_2_Honeypot | Individual | FORTH | Blocked: Waiting for the final XL-SIEM plugins |
| IT_03_3_Honeypot | Individual | FORTH | Blocked: Waiting for the final XL-SIEM plugins |

| | | | |
|---|---|---|---|
| IT_05_2_TaaS | Individual | EGM | Planned |
| IT_05_3_TaaS | Individual | EGM | Planned |
| IT_05_4_TaaS | Individual | EGM | Planned |
| IT_06_CITRIX-ADC | Individual | CITRIX | Blocked: Citrix ADC installed, waiting for configuration to be done |
| IT_07_1_IDS | Individual | FORTH | Planned |
| IT_07_2_IDS | Individual | FORTH | Planned |
| IT_09_1_CYSEC | Individual | FHNW | Blocked: waiting for the final version of CYSEC platform |
| IT_09_2_CYSEC | Individual | FHNW | Blocked: waiting for the final version of CYSEC platform |
| IT_09_3_CYSEC | Individual | FHNW | Blocked: waiting for the final version of CYSEC platform |
| IT_09_4_CYSEC | Individual | FHNW | Blocked: waiting for the final version of CYSEC platform |

| Test-Codes | I/ J | Provider | Comments |
|---|---|---|---|
| JT_01_XL-SIEM_GravityZone | Joint | ATOS & Bitdefender | Planned |
| JT_02_XL-SIEM _Honeypot | Joint | ATOS & FORTH | Blocked: Waiting for the final XL-SIEM plugins |
| JT_03_CITRIX-ADC_Honeypot_XL-SIEM | Joint | CITRIX & FORTH | Blocked: Waiting for the final integration of Citrix ADC |

#### 2.2.4.2 Requirements

Before conducting the tests and thus to evaluate the integration of the SMESEC functionalities in the pilot, there have been some dependencies to be tackled:

- **Functional dependencies**:
  - GridPocket is missing the file xl-siem-logger-6.0.0.jar file to run the test.

- GridPocket is working on implementing correctly Honeypot on its OVH server. The specifications of the server should be adapted to the specific configuration that is asked by Forth.
- GridPocket is waiting for the new configuration of Citrix ADC that would make it compatible with GridPocket OVH servers.
- GridPocket is waiting to have access to the final version of Cysec.
- GridPocket is waiting for the requested technical elements from the different tool collaborators to finalize the integration and the testing steps of the prototype.

- **Technical dependencies**:
  - None: no additional software or hardware was needed in order to conduct the tests.

#### 2.2.4.3 Planning

The following image shows the initial testing planning and its connection with the project schedule:


**Figure 4 Smart Grid pilot tests' planning**

### 2.2.5 Testing of the SMESEC framework

#### 2.2.5.1 Tests

Due to the extended time used for the refinement of the second iteration of the SMESEC Framework the testing definition of the SMESEC solution as a whole have been shifted within the scope of the task T5.3. Furthermore, SMESEC framework had to be validated at Second Project Review in order to start the framework test campaign. This change has been informed during the Second Project Review and it does not jeopardize the project objectives.

Tests are already being defined, as shown in the table below.

| Test-Codes | Description | Comments |
|---|---|---|
| SF_01_Security | General security tests (both web and infrastructure) | Blocked: Waiting for new framework version |
| SF_02_Performance | Performance measures and acceptable load time set | Blocked: Waiting for new framework version |
| SF_03_Access_Control | Check that each role can access only their granted actions | Blocked: Waiting for new framework version |
| SF_04_Configuration | Check that changes in configuration made in the framework are correctly reflected | Blocked: Waiting for new framework version |
| SF_05_Resiliency | Check that framework is still working when one of its components is out of service | Blocked: Waiting for new framework version |
| SF_06_Acceptance | Functional tests performed by pilots to check that UX is well implemented | Blocked: Waiting for new framework version |
| SF_07_External_API | Check that data coming from external tools are correctly integrated using the external API. | Blocked: Waiting for new framework version and for the external API |

Tests with more technical complexity will be performed by Atos, while functional tests will be performed by pilots. The final scope of this part of the test campaign will be decided in the frame of T5.3.

#### 2.2.5.2 Requirements

Before we are able to execute the tests and evaluate their results, the new version of the SMESEC Framework developed after the second review's comments must be ready.

Also, this new version of the SMESEC Framework has some dependencies that needs to be tackled before the release:

- The training platform must provide the API for accessing the data about trainings.
- The Cysec tool must provide the API for accessing the tool data.
- The external API must be developed and used by an external tool.

# 3 Test management

All use cases are conducting the tests that apply to their pilot, with their own particularities, according to section 2.2 of present document.

All tests are to be recorded, and the videos as well as the logs (when it applies) will be stored in SMESEC repository in Owncloud. The results of the tests will be reported in D5.3.

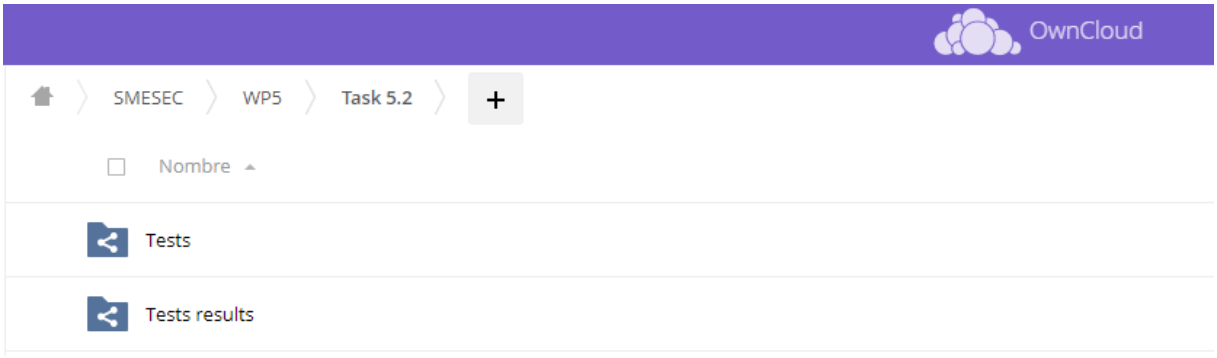


**Figure 5 Owncloud folder for test management**

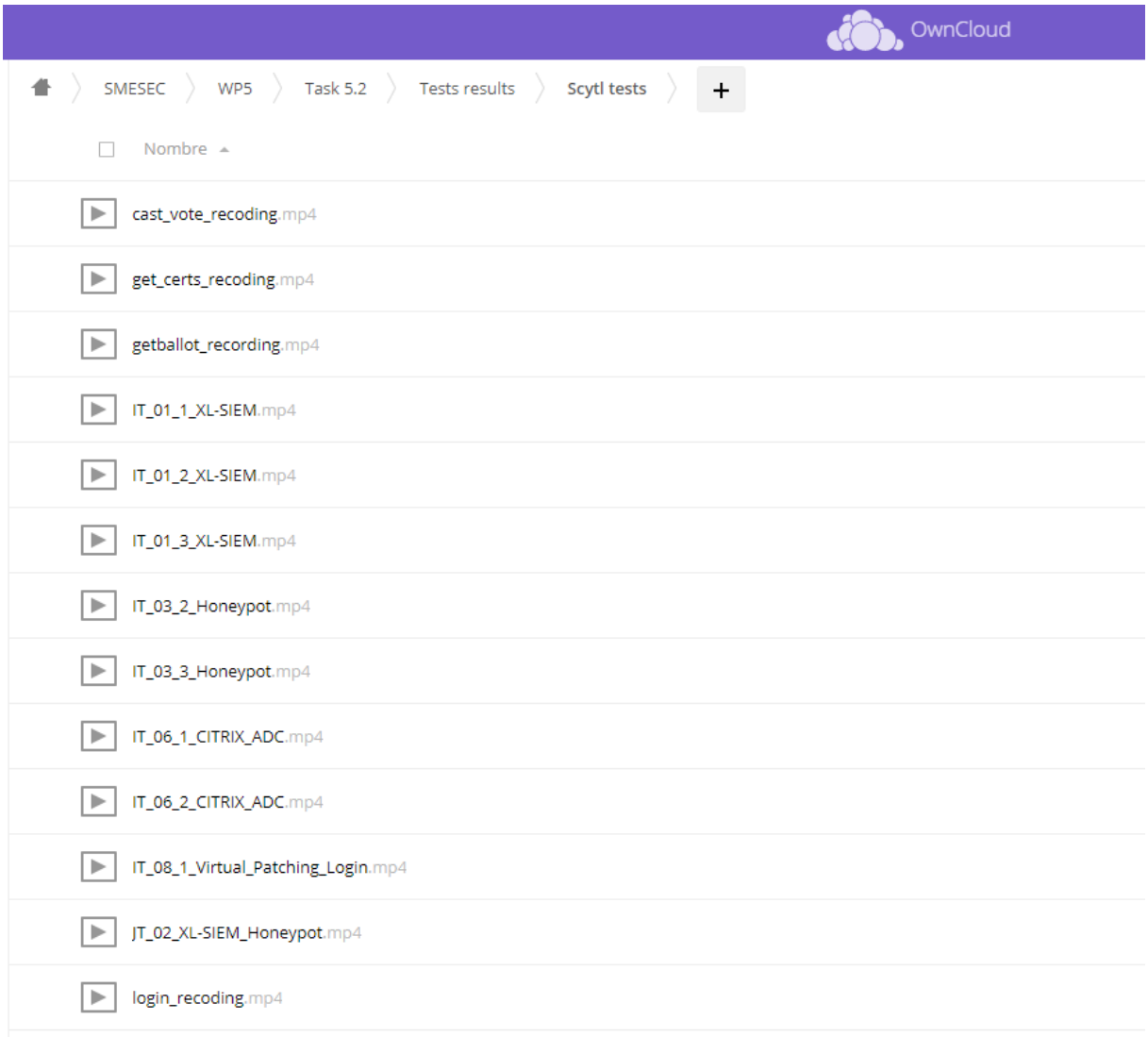


**Figure 6 Owncloud folder with some tests results**

# 4 Conclusions

This document describes the activities done in the framework of task T5.2. The main objective of this task has been to ensure that all pilots are prepared for the full SMESEC system evaluation and demonstration in real conditions, to be later performed during task T5.3.

After the definition of the trial scenarios in task T5.1, several meetings were maintained within each of the pilots and the relevant tool owners, to agree on the tests to be done. The agenda for the tests was also discussed, as well as the dependencies and the supports and collaborations needed.

This has resulted in the final configuration of the experiments to be done in each pilot, the schedule of the trials, and the execution and recording of the first proofs, overlapping with task T5.3.

# 5 References

[1] **Deliverable:** SMESEC. *D.4.2 – Final Integration Report on e-Voting.* Folch, Noemi. 2019

[2] **Deliverable:** SMESEC. *D.5.1.– Trial scenario definitions and evaluation methodology specification.* Last, Andreas. 2019