Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

SMESEC

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

D4.8 Final integration report on Smart Grid pilot

Document Identification			
Status	Final	**Due Date**	31/05/2019
Version	1.0	**Submission Date**	17/06/2019

Related WP	WP4	**Document Reference**	D4.1, D4.3, D4.5, D4.7
Related Deliverable(s)	D2.1, D3.1, D3.2 D3.4, D3.5	**Dissemination Level (*)**	PU
Lead Organization	GridPocket	**Lead Author**	Michał Burdzy (GRID)
Contributors	GridPocket	**Reviewers**	Jose Francisco Ruiz Rodriguez (ATOS)
			Francisco Hernandez (WoS)

Keywords:
security, system, design, architecture, integration, WP4, requirements, goals, innovation, use case, e-voting, 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.

Document Information

List of Contributors	
Name	Partner
Jose Fran. Ruiz	Atos
Michał Burdzy	GridPocket

Document History			
Version	Date	Change editors	Changes
0.1	17/04/2019	Michał Burdzy (Gridpocket)	Document initialization
1.0	17/06/2019	ATOS	Quality review and submission to EC

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	GridPocket (GRID)	17/06/2019
Technical manager	Christos Tselios (Citrix)	17/06/2019
Quality manager	Rosana Valle Soriano (Atos)	17/06/2019
Project Manager	Jose Fran. Ruíz (Atos)	17/06/2019

Table of Contents

List of Tables

List of Figures

List of Acronyms

Abbreviation / acronym	Description
AMI	Amazon Machine Image
API	Application Programing Interface
AWS	Amazon Web Service
CRM	Customer Relationship Management
Dx.y	Deliverable number y belonging to WP x
DoA	Document of Action
GDPR	General Data Protection Regulation
HTTPS	Hyper Text Transfer Protocol Secure
IoT	Internet of Things
IP	Internet Protocol
PowerVAS	Power for Value Added Services
REST	Representational State Transfer
SaaS	Software as a Service
SIEM	Security Information and Event Management
TaaS	Test as a Service
UI	User Interface
URL	Uniform resource Locator
VM	Virtual Machine
WAF	Web Application Firewall
WP	Work Package

Executive Summary

This deliverable describes the work done at M24 of the integration of the SMESEC Framework in the Smart Grid 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 also report the final analysis and next steps to be done in the project for the work with the SMESEC Framework and how so far it fulfilled the objectives of the use case. We also described 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 Grid 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 Grid 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.

For a better understanding of the integration of SMESEC, an initial description of the use case of the pilot, the scenarios of application and its technical architecture were described in previous report (D4.7). This will help understand the specific needs of the pilot and the process of selection of the tools of the framework that will be integrated. Also, it presents the initial feedback of the training and awareness process in the organization, identifying the needs for courses and training tools offered in the project.

Finally, the information contained here is an extension, updated, from the previously presented work in D4.7. That way, both deliverables complement and can be seen as a life report of the work done for integration of SMESEC, experience of the process and feedback.

1 Introduction

1.1 Purpose of the document

This is the second deliverable of WP4 "Final Integration report Smart Grids SME pilot" related to the Smart Grid pilot. The role of this WP in the SMESEC project is to adapt the SMESEC Framework prototype to the different pilots proposed in the project.

Specifically, D4.8 provides an in-depth description of the integration of SMESEC in the 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.

The aim of this document is to describe the results of efforts conducted to integrate the final version of the SMESEC Framework into the Smart Grids Pilot product called PowerVAS (Power for Value Added Service). The document provides the different steps of the integration, from the description of the use case, the initial technical architecture, the current needs, the upgraded architecture with required tools of the framework to the installation and initial tests processes.

1.2 Relation to other project work

The work described in this deliverable will be used for other deliverables and work packages such as:

- D3.3 - Final Version of the SMESEC security framework Unified Architecture and Initial Version of the SMESEC Framework Prototype.
- D4.9 - Overall Pilot alignment and integration process report.
- D5.1 - Trial scenario definitions and evaluation methodology specification.
- D5.2: - System readiness for validation activities.
- D5.3: - Prototype Demonstration: Field trial results.
- WP6: - Exploitation, dissemination and standardization 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, review and extension of the requirements and needs identified in the first year.

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.

2 Requirements and needs: from planning to action

Working in SMESEC project allowed us to verify and confirm our apprehension of cybersecurity threats we are facing as a company. We understood that cybersecurity is critical for SME performing actions on the field of user data processing. In order to gain better protection, we expanded the initial list of tools we planned to integrate. This gave us the best possible protection from any cyberthreats.

During the first year of the project, Gridpocket defined a set of requirements to be fulfilled by the SMESEC Framework. They are described in D2.1 document, and they include necessity of protecting several components of Smart Grid architecture, such as:

- OVH Cloud interface.
- UI server.
- Reverse Proxy server.
- Database server.
- API server.

On the second year of the project, Gridpocket validated and enhanced the requirements to be covered by the SMESEC Framework in the architecture of the pilot. The company decided to add a protection layer to its inner network, as well as to individual computers used for connecting with pilot infrastructure.

Identifier	Description	Asset Impacted
Company inner network	Inner network at main Gridpocket had little or no protection in case of running malicious code inside it.	Another local server was installed in order to host FORTH IDS on it. IDS perform routine scans to detect any abnormal behaviour inside the local network.
Individual computers	Some laptops used by Gridpocket had no or weak antivirus protection.	Computers were equipped with Bitdefender antivirus in order to prevent possible infection of the Pilot infrastructure by computer attacked by virus.
Employees awareness	Cybersecurity awareness of employees plays crucial role in cybersecurity	No asset impacts. Trainings organised for employees in order to rise their consciousness

Table 1: New requirements of Pilot

In the current status of integration, Gridpocket assesses that all requirements were fulfilled by the application of SMESEC components. Further details are described in the following sections.

3 Scenarios and usability

3.1 Updates and enhancement

GridPocket planned to implement several components of the SMESEC Framework into company's main product – PowerVAS. PowerVAS is a 'white label' Value Added Service platform, which provides customer management and churn reduction for utility companies, and reduction of energy consumption to end users. It is based on processing huge amounts of sensitive data, obtained from smart meters installed in customers' houses. Therefore, cybersecurity plays a crucial role in its functioning and resilience. Any potential security corruption in PowerVAS can lead to serious consequences, such as compromising our client – utility company – and GridPocket as well.
Initially, GridPocket planned to use only four tools: XL-SIEM, NetScaler WAF, IDS and TaaS. During the integration of these tools, Gridpocket noticed some remaining gaps in cybersecurity defence, such as lack of network-scanning protective tool and absence of antivirus protection of computers connecting pilot infrastructure. To improve pilot security, company decided to extend the usage of SMESEC with other tools: Bitdefender Gravityzone antivirus and Honeypot.

As an update from the previous integration, as reported in D4.7, Citrix ADC WAF was hosted on Amazon cloud. This turned out to be too expensive solution, so GridPocket made plans to integrate ADC into OVH cloud, where the Smart Grid architecture is hosted. Currently ADC is installed on separate server in Smart Grid pilot cloud infrastructure. It filters all incoming traffic and passes it directly to PowerVAS – Smart Grid application.

3.2 Architecture

Schema of Smart Grid pilot architecture, before integrating SMESEC framework is as below:

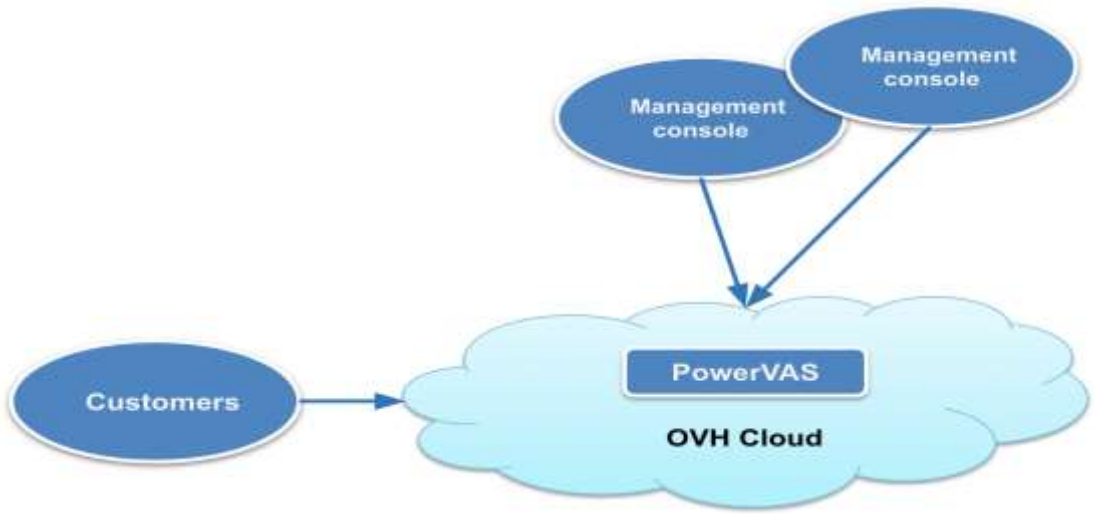

Figure 1: Initial PowerVAS architecture

The SmartGrid application is hosted on OVH cloud. It consists of several virtual machines, acting as User Interface, API, and Database servers. Customers can access a web interface using Internet. Developer access servers with different Management consoles - usually laptops or PC's

This architecture has several pros and cons. The main good point is that it is very simple and easy to deploy and administer, especially when using tools such as Ansible. Each PowerVAS instance can have multiple instances of UIs, APIs and Databases linked together with Load Balancers, which makes the architecture really robust with no-single point of failure.

On the other hand, this architecture could be improved with several layers of protection that would greatly improve the concept of defence in depth, such as strong Web Application Firewall (ADC), network scanner (IDS), antivirus (Gravityzone), central logging console for cybersecurity events (XL-SIEM) and authentication testing (TaaS).

Cloud is protected by its default firewall, but besides that, PowerVAS is not protected in any other way.

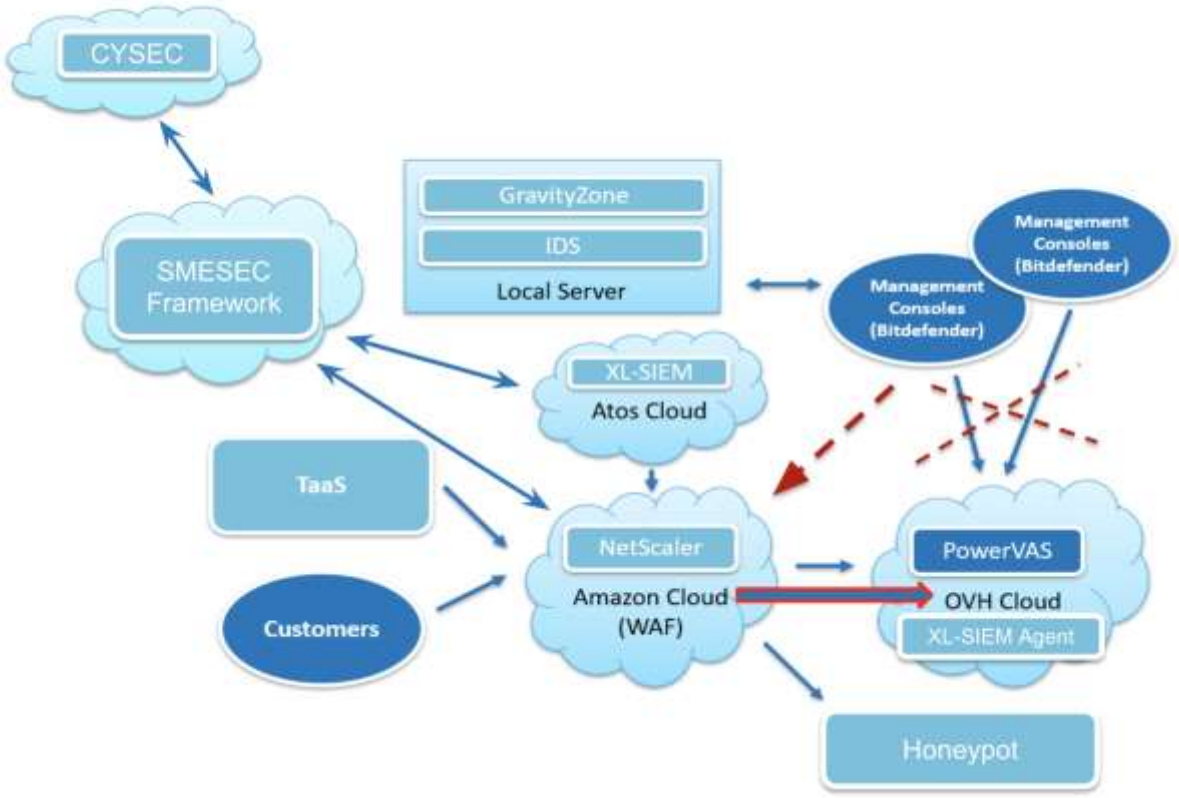

Figure 2: Enhanced architecture with SMESEC tools

Using SMESEC, the Smart Grid pilot received several additional security layers. Previous cloud firewall was extended by Citrix ADC WAF (Netscaler), user authentication mechanisms are ensured by TaaS, inner communication between different components of network is secured by IDS, each Management.

Console accessing network is protected by GravityZone Antivirus, and in case of intrusion, Honeypots will provide additional protection. All cybersecurity can be controlled from the level of the SMESEC Framework. Overall cybersecurity level is described by CySec.

This upgraded security concept was not perfect though. Citrix ADC had to run on a separate cloud, preferably hosted by AWS. This solution caused significant drop of network connections speed. It had also negative financial impact, because required costly cloud solution only for hosting ADC there. That's why, with help of Citrix, this architecture was updated. In the final version, both PowerVAS and Citrix ADC are hosted on the same OVH cloud. This makes our product fast and affordable at the same time.

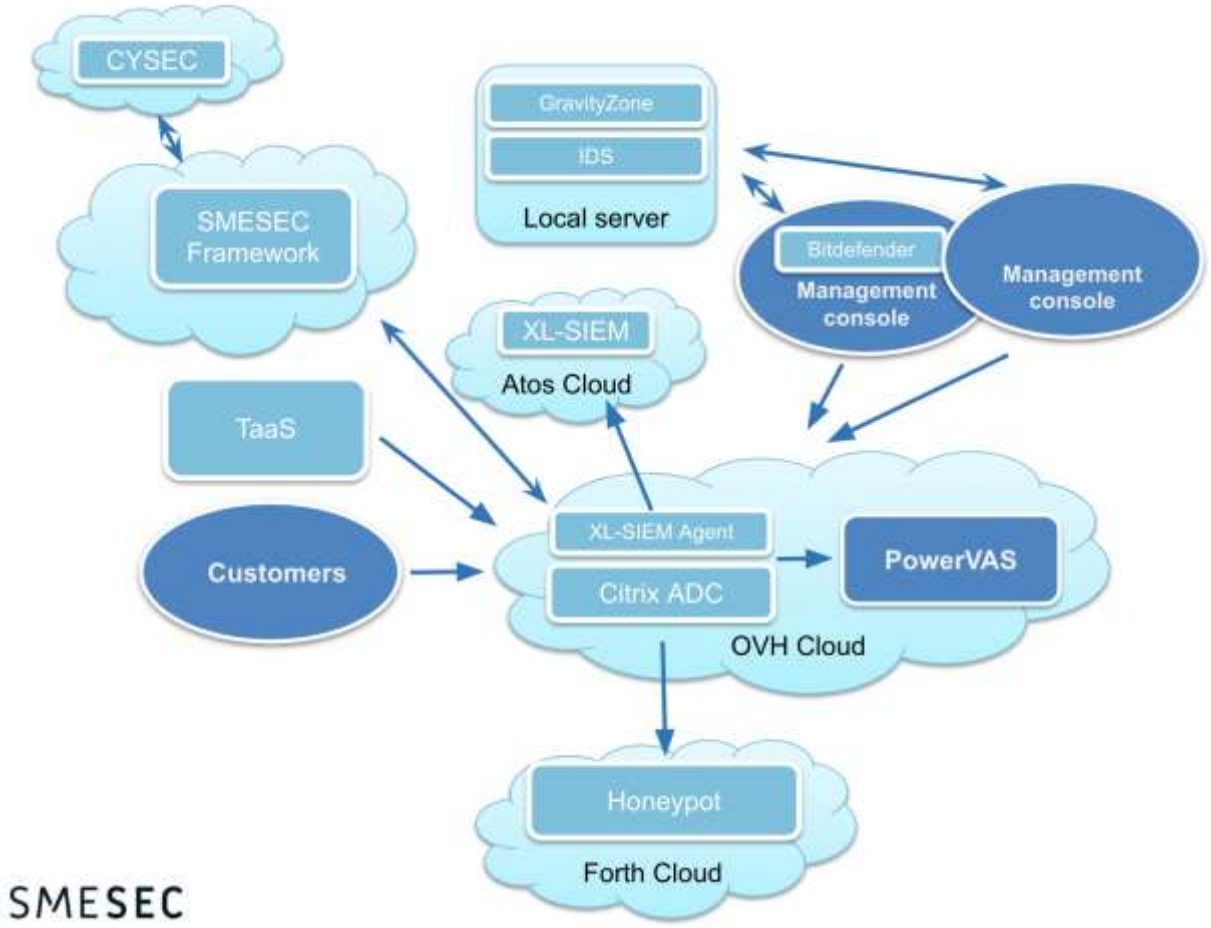

Figure 3: Final architecture with SMESEC tools

3.3 Scenarios of SMESEC

Scenarios were described in D4.7 document "Preliminary Integration report on Smart Grids SME pilot". No update since the last described version.

3.4 Impact of SMESEC in the use case

Implementing SMESEC helps protecting some crucial points in the SmartGrid pilot. Those are specifically:

- User authentication (TaaS) - Automated tests of user authentication mechanism ensures correct authorisation management. Example tests are attached in Annex.
- Inner network communication (IDS) - IDS carries out casual network scanning in order to find any suspicious traffic.
- Connecting with third-party providers and Internet (Citrix ADC) - ADC WAF filters all incoming network traffic and filters out potential malicious requests.
- General security maintenance (GravityZone) - provides antivirus and antimalware protection for computers used to manage pilot servers.
- Protection in case of breach into company network (Honeypot) - used to mislead attacker and draw him away from real pilot servers.
- Overall cybersecurity awareness (CySec) - helps estimate overall cybersecurity status of the company in order to provide better security solutions.
- Controlling cybersecurity status (XL-SIEM) - gathers all cybersecurity data from all tools integrated into pilot except for CYSEC tool.

3.5 Business impact

Business impact was described in D4.7 document "Preliminary Integration report on Smart Grids SME pilot"

4 Technical integration of SMESEC

4.1 Integration of SMESEC in the use case

According to the description of the final architecture above, the selected and integrated tools are:

Tool	Expected usage
XL-SIEM	The SIEM is used as the central component of the SMESEC architecture. It allows the analysis of suspicious pattern of traffic and sending of alarms.
Citrix ADC WAF	The WAF is used to filter out malicious requests coming from attackers or misconfigured hosts on the Internet. Examples of such requests include SQL injection attempts, filesystem information gathering, and cross site scripting.
IDS	The SNORT IDS perform a crucial monitoring of the GridPocket Intranet from within and thus from a privileged observation point. It routinely scans local traffic with the aim of matching it with known patterns of malicious traffic, detecting malicious intrusions in the private network
TaaS	The TaaS system is used to test one of the most crucial API of the whole PowerVAS platform called MS_AUTH, which is responsible for identification and authorization of the different users of the platform.
CYSEC	CySec tool is used to evaluate the level of security awareness of the employees.
GravityZone	GravityZone Antivirus protects devices used to access the pilot infrastructure. GravityZone console is used to manage the protection of devices that have an antivirus installed
Honeypot	Honeypot in the cloud will connect to Citrix ADC. All malicious traffic will be redirected to the Honeypot in order to mislead attackers

Table 2: Tools usage

The description of their installation, integration and tests can be found below.

4.2 Analysis and evaluation of SMESEC

4.2.1 XL-SIEM

GridPocket received the agent from Atos and the credentials for the cloud Web Portal. Following this, the agent has been installed in the pilot infrastructure. Once this activity was completed, Gridpocket verified if the monitoring was working correctly and provided the expected functionality.
XL-SIEM is the central component of the updated architecture of our pilot. It gathers the information from all other SMESEC monitoring tools. Implementing XL-SIEM made easier managing and supervising security of company network.

The main impact of using this tool in our pilot is the increased awareness and control over all network events connected to cybersecurity of the company, as it accumulates data from all other SMESEC tools. This substantially increases level of overall cybersecurity of the pilot.
Here the Cloud Portal for GridPocket can be seen below with the Alarms Threat Level (Right) at a low level:

Figure 4: SIEM - GridPocket cloud portal

Below is the view of the XL-SIEM Events page. It presents the detailed log of received data from the cloud SIEM. Main section presents list of all network events collected by XL-SIEM with their date, signature, source and risk assessment. Upper section allows for searching and filtering all events according to various criteria.

Figure 5: SIEM – Example of logs

Network Traffic page depicts the traffic pattern analysis performed by XL-SIEM. It allows displaying different connection protocols and presents the statistics of the network.

Figure 6: Traffic pattern analysis

4.2.2 TaaS

One of the main functionalities of the Smart Grid pilot that needs to be tested is the authentication process and restriction access. In our use case, user can see and manage his private consumption data after logging into the PowerVAS service. The authentication is done through a REST API using credentials (username & password). As there are different types of users (normal user, admin, public…), there will be customized access rights such as read only, update, deletion. TaaS is used as a quick and secure authentication testing tool. It increases security confidence of PowerVAS, contributing to better overall security of our pilot.

TaaS is currently working and allows testing user authentication of SmartGrid Pilot. EGM prepared and shared with GRID test configuration files that define basic tests of user authentication workflow. Those files allow to run all test cases using the online SMESEC console.

Implementation of TaaS helped Gridpocket to assure that company's authentication mechanisms, based on ms_auth microservice, are working exactly like they are supposed to, which makes user authentication process secure and safe.

A certain number of scenarios were created during the training session with EGM as described in the picture below:

Scenarios			Status
▸ Sprint 1/Login NOK			Not Run
	Actions	Expected Results	
1	Login with: id: incorrect pwd: incorrect	User not redirect to dashbord	Not Run
▸ Sprint 1/Login OK			Not Run
	Actions	Expected Results	
1	Login with: id: correct pwd: correct	User redirect to dashbord	Not Run
2	Dashboard open	We are authenticated	Not Run
▸ Sprint 2/Login NOK			Not Run
	Actions	Expected Results	
1	Login with: id: incorrect pwd: incorrect	User not redirect to dashbord	Not Run
2	Login with incorrect login	Authentication Failed	Not Run

Figure 7: Test scenarios publication

The main task of TaaS in the Smart Grid pilot is to mimic all the possible paths of the authentication process that user can encounter and ensure that they are properly secured. The scenarios currently implemented are:

- User trying to login with incorrect identifier and password is not redirect to the dashboard with a status result set as "Authentication failed".
- Regular user trying to access some admin functionality is not allowed to do it.
- User trying to login with correct identifier and password redirect the dashboard with a status result set as "We are authenticated".

4.2.3 Citrix ADC WAF

WAF stands for Web Application Firewall. Citrix ADC prevents any suspicious traffic from accessing the PowerVAS. It significantly increases the security level of our pilot, by filtering out most of potential threats. Any potential malicious traffic will be either blocked by ADC or redirected to Honeypot server in order to mislead attackers. Including Citrix ADC improved credibility of product, which will have a positive impact on further client acquisition by GridPocket.

The first step was the installation of the software obtained from an AMI provided by the Amazon AWS cloud platform. As the platform supports one click deployment, this was quite easy to perform.

The deployment overview can be seen here:

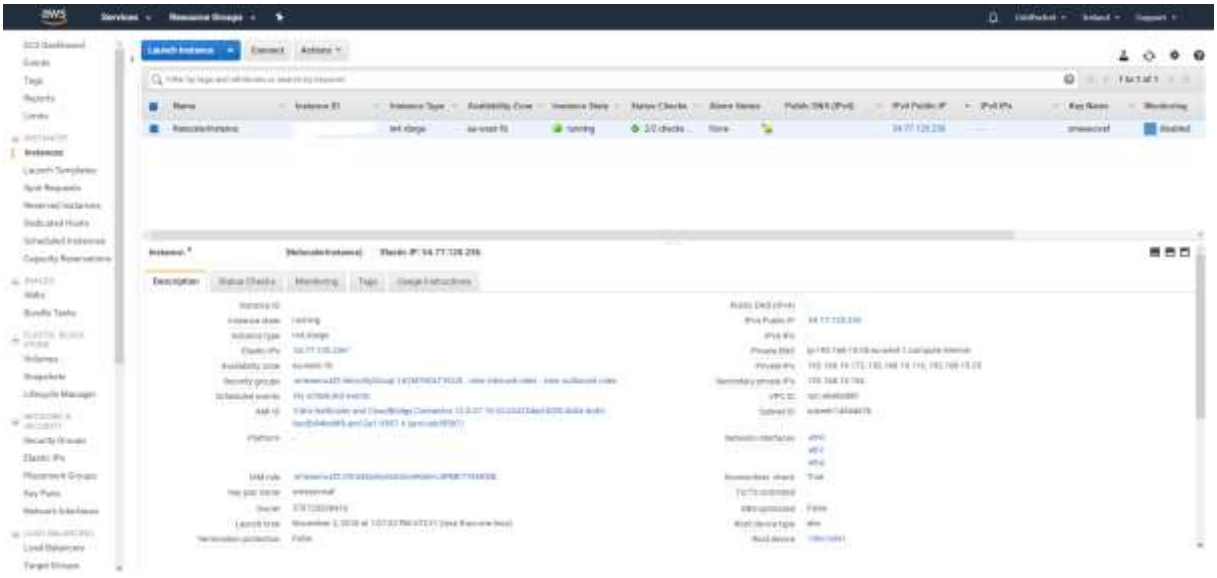

Figure 8: Citrix WAF deployment overview

The license code provided by Citrix was used during the installation process to achieve all the needed functionalities, as can be seen here:

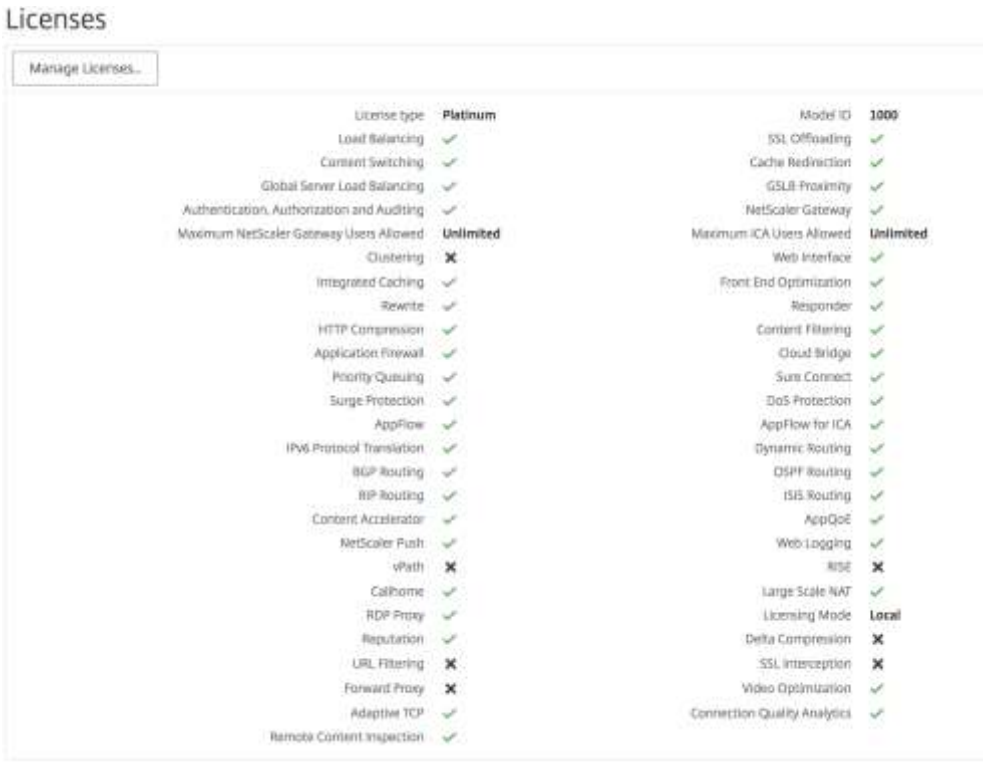

Figure 9: Functionalities available according to the license

Then GridPocket had to configure the reverse proxy, for which it was necessary to look for documentation in the internet and on the Citrix knowledge base.
Overview of the WAF console can be seen here:

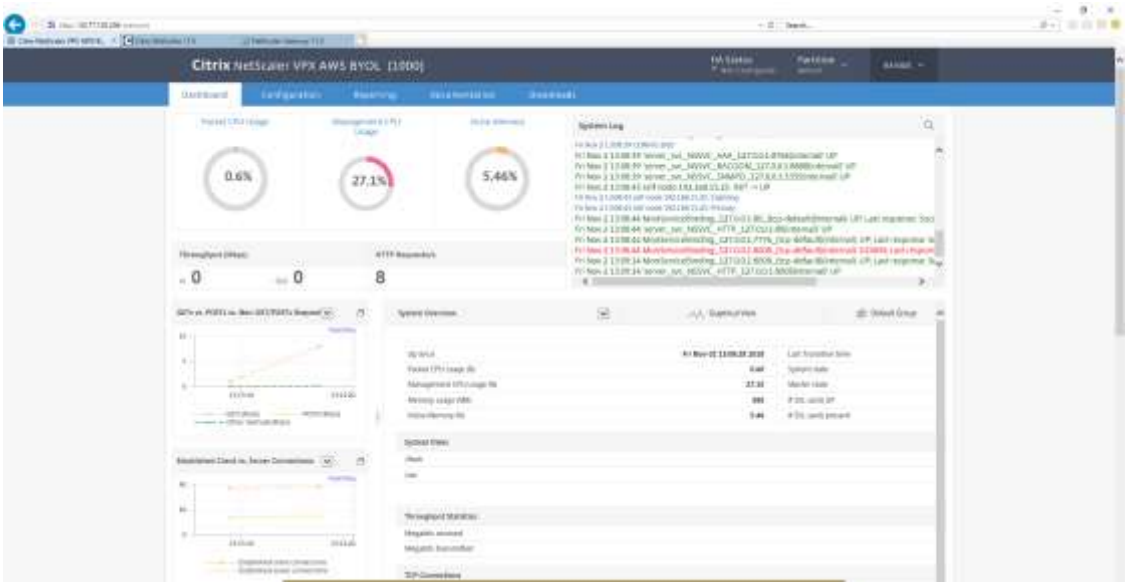

Figure 10: Citrix WAF final overview

After initial integration phase, for the reasons described in chapter 3.1, Gridpocket decided to move Citrix ADC solution from AWS cloud to OVH cloud. Installation was done with support of Citrix.

4.2.4 IDS

Intrusion Detection System is tool monitoring our inner network from within. It scans the inner traffic in search of any suspicious patterns. IDS adds another security layer to Smart Grids pilot in case other external security layer fail. It is yet another tool raising the security, confidence and reliability of our solution.

Implementing IDS significantly improved overall security of Gridpocket inner network, which before was missing any network monitoring tool. Using IDS not only makes Smart Grid pilot safer, it also creates added value for whole company, by making it safer and more reliant.

IDS provides good quality documentation and requires a medium level of expertise in order to be implemented. It has to be run on Xen hypervisor, with SNORT installed on it. Implementation of IDS doesn't affect an overall company network, as it is running on just another machine connected to it.

After getting installation instructions the first attempt of installation failed because of missing resources (libraries, urls etc). FORTH provided us a feedback in order to get more up specific instructions, which lead to an installation success. The IDS can be seen up and running in the picture below:

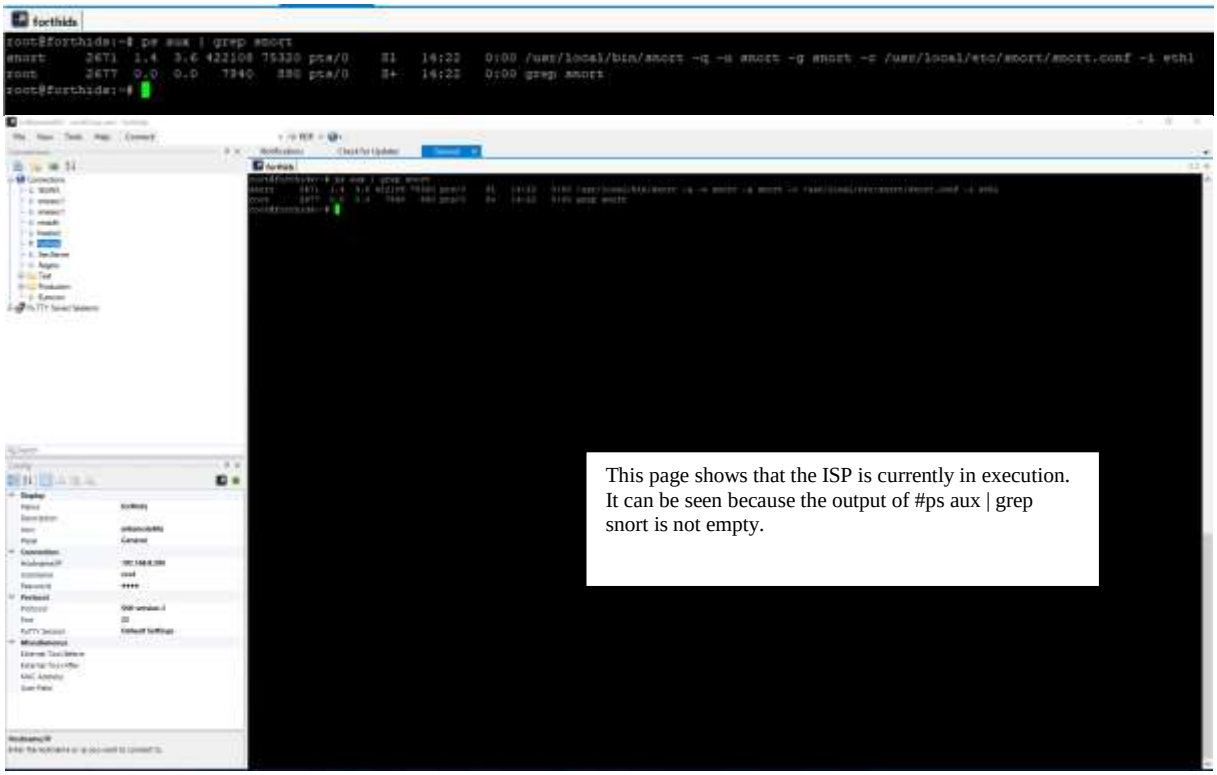

Figure 11: Forth IDS running

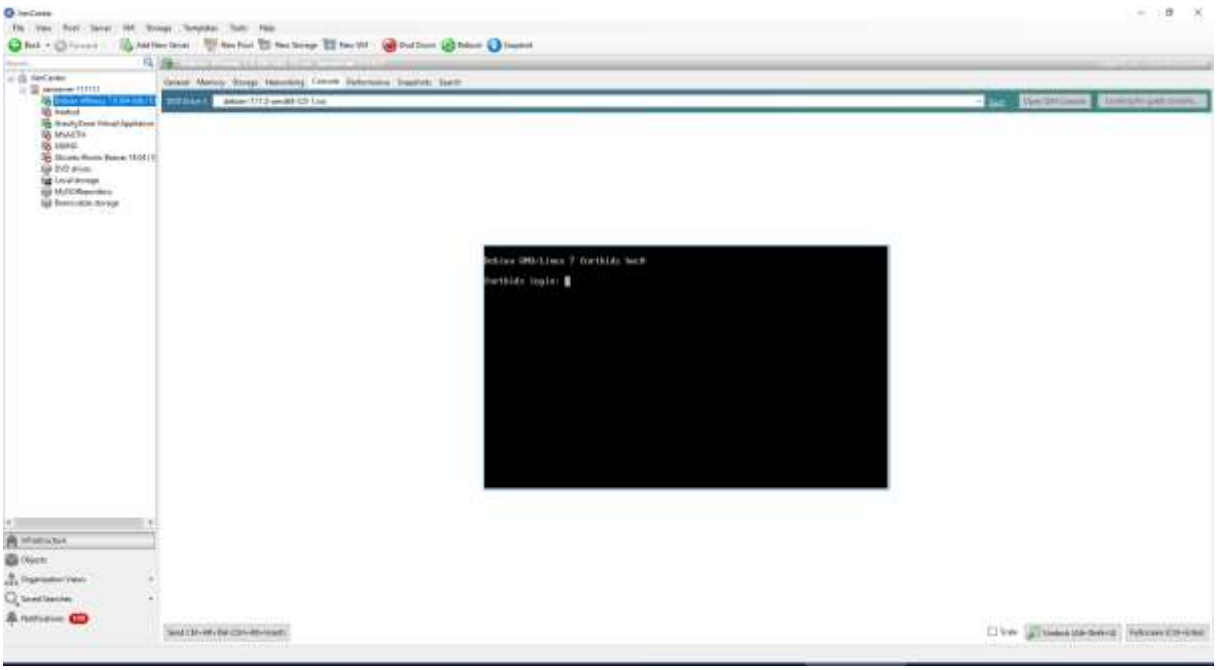

Figure 12: Forth IDS running on XEN VM

4.2.5 CySec

During a meeting between FHNW and GRID organized in Gridpocket main office, main IT security manager of the company used and the evaluated CySec tool. It allowed to estimate overall cybersecurity level of company infrastructure. Meeting was followed by discussion about ways of improving the level of protection of the network of Gridpocket.
Using the CySec tool induced a discussion about IT security in company, which led to important decisions, such as organising cybersecurity training, and making further plans of extending company cybersecurity strategies.
Following a constant evolution of company's infrastructure and personnel changes, Gridpocket plans to use CySec tool regularly in order to keep improving cybersecurity awareness.

4.2.6 GravityZone

Two computers, which are usually connecting with Smart Grid cloud, are protected by Bitdefender Antivirus. GravityZone console, installed on local server in main Gridpocket office, allows for protection management of those devices. Installation and connection were easy, but required communication with Bitdefender in order to configure the connection between GravityZone console and computers using Bitdefender Antivirus.
Implementing Bitdefender antivirus has brought added value to Gridpocket by protecting several computers, which play a crucial role in the management of the company cloud infrastructure. Not only Smart Grid pilot has gained from this, but also other servers that are administered from those devices. Now any potential threat is blocked and reported by antivirus on computer, which makes unintentional infection of servers almost impossible.

4.3 Testing and feedback provided

As the tools are installed separately, initial tests need to be run independently to make sure each of them are working as expected. The description of these tests is as followed:

1. XL-SIEM: The agent was provided by Atos with a test mode. We tested if events sent by the agent are being correctly registered in the system. This test was run successfully to make sure the events were sent to the Web Portal.
2. EGM TaaS: Test configuration file was deployed to the TaaS using the SMESEC console. Configuration file contained definitions of tests of various authentication scenarios. Then the test was run, and the result was success.
3. Forth IDS: The IDS aims to detect the presence of malicious agents inside the network. To test the installation, malicious agents were artificially generated from inside the private network and check if the IDS detects them. Gridpocket faced several small issues during integration and testing, but FORTH provided feedback and documentation that made everything clear.
4. Citrix WAF: Testing the WAF was quite easy as GridPocket just had to send malicious requests to the system and check if the requests are blocked by the WAF. Further tests were defined by Citrix and will be conducted during the next phase of the project. Theyr definitions are described in D5.1 document, and output will be documented in D5.2.
5. GravityZone: tested the connection between managing console and devices protected by Bitdefender Antivirus. Checking if the console allows management of security layers on the devices.

5 Cybersecurity awareness and training

5.1 Training and awareness

Participation in the SMESEC project helped Gridpocket discover threats associated with lack of cybersecurity and awareness among its employees, especially apprentices without any commercial experience. They access company internal network, and often don't realise the risks of malicious code and social engineering. Our company has one cybersecurity expert who monitors and audits GridPocket's platform. This expert organises training sessions to let all the teams be aware of the different possible threats and the good practices to apply to protect ourselves or to mitigate them. This process helped GridPocket maintain a very low rate of the number of cybersecurity incidents over time, despite of the different scenarios of processing confidential data in company products and personnel rotation. It is worth mentioning, that none of those incidents led to a leak of confidential data of end users.

Apart from that Gridpocket makes use of opportunities given by SMESEC to improve the cyberthreats awareness among its workers. Various training sessions are designed for different groups of employees: general cybersecurity trainings for office workers and more focused on technical aspects for developers. Company finds SMESEC training platform useful, nevertheless resources available there are not enough to cover all aspects of cybersecurity. For example, there are attacks on SQL databases only, but no attacks on no-SQL databases presented. Moreover, XSS attacks, which are very common attack type, are presented only in the context of SQL injection scenario. Other XSS examples such as phishing or session hijacking would be helpful in training practice.

Furthermore, part of the team took part in cybersecurity course 'Front-end security' organised by Securitum and 'Attacking and defending web applications' organised by Niebezpiecznik.pl. Courses were led by top cybersecurity specialists and covered all possible attack examples in practice. This let to implementing good practices and additional security layers to company products.

6 Conclusions

6.1 Final analysis and next steps

The components installed until now are:

- **ATOS XL-SIEM**: The installation was quite easy, also the link to the Web Portal. The package provided by Atos self-installed, and then minimal configuration was needed.
- **EGM TAAS**: To properly manage this component, the administrator had to attended two days training at EGM. Later when EGM created test files, running TaaS by SMESEC console is quick and easy.
- **Citrix ADC WAF**: This software was installed using an AMI on AWS provided by Citrix. So, the installation was very easy. The configuration was more complex and required much experience and effort. Next ADC will be moved to OVH cloud. It requires connecting to specific addresses in our pilot, but with the help of Citrix it shouldn't be too complicated.
- **FORTH IDS**: The main difficulty was the missing of some resources and libraries. After few clarifications and discussions with Forth, the installation was completed.
- **CYSEC**: Tool is easy to use and intuitive. Requires no preparations or expertise.
- **Honeypot**: Still requires connecting to Citrix ADC.

SMESEC framework fulfilled all cybersecurity requirements defined by Gridpocket, moreover it contributed to rise of the cybersecurity level of whole company infrastructure by offering several comprehensive tools improving the protection of different systems.

From SME point of view, SMESEC framework is a robust and exhaustive solution for common cybersecurity issues among all SMEs. It provides a wide range of protective tools and scenarios, which cover most possible attacks and exploits. Its testing platform rises the level of awareness among the employees, and CYSEC helps evaluate security status of the company, and match the best solution for it.

Thanks to SMESEC, Gridpocket gained a versatile and reliable cybersecurity protection, which raised the value of company products on the market.

6.2 Fulfilment of objectives

Initially, GridPocket planned to make a full integration of the Citrix ADC, the XL-SIEM, EGM TaaS, GravityZone, IDS and Honeypot. Most of the component were installed and integrated and are full functional now. Final integration of Citrix ADC and FORTH Honeypot was delayed, but with help of Cintrix and FORTH, those tools will gain full functionality in a matter of days.
SMESEC framework fulfilled all initial objectives defined by Gridpocket in D2.1, as well as additional requirements defined during second year of the project. List of all requirements, tools fulfilling them and fulfilment status:

Requirement	Tools used	Description
Cloud platform, UI server, API layer server, DB server, Reverse Proxy server	ATOS XL-SIEM, FORTH Honeypot, Citrix ADC,	Requirements fulfilled
Compay inner network	FORTH IDS	Requirement fulfilled
Individual computers	Bitdefender GravityZone	Requirement fulfilled
Employees awareness	Training platform, CYSEC	Requirement fulfilled

6.3 Future outcomes and business development

Using SMESEC Framework places Gridpocket in the lead of companies of our sector because other competitors in this field don't have such robust and sophisticated cyberthreats security, like those provided by SMESEC. It also allows to enhance company's systems and methodology of work thanks to interactions with other partners, which are all highly developed IT companies and universities. Communication with consortium partners allows us to look up to their technical solutions, technology stack and general approach to different IT fields. Such collaboration allows Gridpocket to rise its standards in a field of cybersecurity and international cooperation. The company predicts that implementing SMESEC into its systems will result with additional business opportunities and higher customers interest thanks to higher reliability and improved cybersecurity of its products. This places Gridpocket among the leading companies in utilities field on European market.

PowerVAS is and will stay the core of the product. Accordingly, there will be no modifications on its basic functionality which is to provide energy value added services such as energy consumption monitoring, energy comparison, electric device control, bill payment and others to end-users.
The SMESEC Framework should be considered as an additional security layer, imperceptible to end-user's experience. The main modifications will be on the technical architecture, implementation and deployment side. All the details of the events gathered by the framework should be available in a dedicated Web page/interface. Hence, no training is expected for end-users but for the employees (developers, project managers, architects…).
SMESEC framework and the training & awareness platform helped GridPocket enhance not only the level of security of its platform, but also its credibility with its current and future clients. They will help avoid reputational damage in case of potential breach.
SMESEC Framework helped to solve cybersecurity problems that Gridpocket was facing before: poor or no antivirus protection, weak basic firewall, missing network scanner, no authentication testing and no central point of gathering all cybersecurity events information. All those flaws were covered by SMESEC components implemented in Smart Grid pilot.
Our efforts towards improving security of GridPocket products are supposed to bring a tangible benefit for the company. We predict that more secure solutions will help us gain more customers, and draw attention of potential investors, which will translate into higher revenue of the company. Our main strategy is to promote our company as the most secure utility Value Added Services company on the market. Also, our long-term cooperation with leading IT companies from all over the Europe will be proof of solidity of our solutions for potential customers.

7 Annex

7.1 TaaS test example

```
test_name: "API test of gridvalley.eu"
stages:
 - name: Login
   request:
     headers:
       content-type: application/json
     json:
       password: [CONFIDENTIAL]
       remember: true
       username: [CONFIDENTIAL]
     method: POST
     url: "https://gridvalley.eu/api/signin"
     response:
       status_code: 200
       cookies:
         - token

 - name: Make sure user does not have admin access
   request:
     url: https://gridvalley.eu/admin/data
     method: GET
     response:
       status_code: 403
```