Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

SMESEC

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

D4.7 Preliminary Integration report on Smart Grids SME pilot

Document Identification			
Status	Final	**Due Date**	30/11/2018
Version	1.0	**Submission Date**	20/12/2018

Related WP	WP4	**Document Reference**	D4.7
Related Deliverable(s)	D2.1, D2.2	**Dissemination Level (*)**	PU
Lead Organization	GridPocket	**Lead Author**	Papa Niamadio
Contributors	Atos, GridPocket	**Reviewers**	Sharon Keidar-Barner (IBM)
			Noemi Folch (SCYTL)

Keywords:

Smart Grid, IoT, security, protection, intrusion, API, end-users, SaaS, framework, integration

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.

(*) Dissemination level.-**PU**: Public, fully open, e.g. web; **CO:** Confidential, restricted under conditions set out in Model Grant Agreement; **CI:** Classified, **Int** = Internal Working Document, information as referred to in Commission Decision 2001/844/EC.

Document Information

List of Contributors	
Name	Partner
Jose Fran. Ruiz	Atos
Papa Niamadio	GridPocket
Marco Fiorani	GridPocket

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	06/11/2018	Papa Niamadio, Marco Fiorani (GridPocket)	First draft of the document ready for internal review
0.3	28/11/2018	Sharon Keidar-Barner (IBM)	First review
0.4	29/11/2018	Papa Niamadio (GridPocket)	Update according the review comments
0.5	29/11/2018	Noemi Folch (SCYTL)	Second review
1.0	20/12/2018	ATOS	FINAL VERSION TO BE SUBMITTED

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Papa Niamadio (GridPocket)	20/12/2018
Technical manager	Christos Tselios (Citrix)	20/12/2018
Quality manager	Rosana Valle Soriano (Atos)	20/12/2018
Project Manager	Jose Fran. Ruíz (Atos)	20/12/2018

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

The aim of this deliverable is to describe the preliminary efforts carried out to integrate the SMESEC Framework into Smart Grids Pilot. The framework is not yet packaged as a single component, and it implies a different integration way. In fact, the tools of the framework will be integrated independently during this first step of the integration process.

When all the tools will be finally integrated into one component, Gridpocket will conduct the next phase of integration process, which will cover process of installation the final version of SMESEC framework into Smart Grid Pilot. During this phase Gridpocket will provide feedback on installation and implementation to all partners. Then all the tests will be conducted once again, to prove that SMESEC preserved all its functionality despite of complicated integration process.

For a better understanding of the integration of SMESEC, a first description of the use case of the pilot, the scenarios of application and its current technical architecture will be made. 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.

The document will also present the type of tests to be run to validate the integration and the security level enhancement of the Smart Grids pilot product. Some business aspects of the integration will also be presented.

Additionally, this document will provide feedback about the initial integration process and the skills/expertise required for each tool. It will also provide a proposal of feedback for improvement of SMESEC and the pilot at this initial stage. That way the feedback can be provided in parallel with the continuous work of the project. A more complete report about the final integration and evaluation will be available at month 24 in the deliverable D4.8.

1 Introduction

1.1 Purpose of the document

The aim of this document is to describe the results of efforts conducted to integrate the initial version of the SMESEC security framework and extended tools 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.

By providing initial feedbacks about the work carried out for integration of the tools, this document will help collect news requirements and/or comments that will be useful in the implementation and the validation of the SMESEC framework.

1.2 Relation to other project work

As described in the DoA, this document will provide the roadmap to be used in the integration and adaptation of the SMESEC framework to the Smart Grids pilot. This document takes as inputs the specifications and requirements defined in WP2 and the design of the SMESEC framework in WP3.

The integration of the SMESEC framework or the components of the framework will be followed by an extensive evaluation and demonstration ensured by WP5. This will provide relevant test scenarios to evaluate the framework in terms of KPI, performance and user-friendliness.

1.3 Structure of the document

This document is structured in 5 major chapters.
Chapter 2 presents new requirements of the use case we have identified since the initial ones described in D2.1. [1]
Chapter 3 describes the use case and the usage scenario of the SMESEC framework.
Chapter 4 presents the list of selected tools, the integration process and status.
Chapter 5 presents the future integration plans.
Chapter 6 presents feedback regarding the framework/components integration.

2 Update of requirements and needs

Gridpocket has identified an additional requirement arising from need of extending the protection of our devices. Currently used antivirus software lacks some important functionality, also in case of breach in our inner network, all our data is in great danger, as it is exposed for attackers. Therefore, GridPocket decided to upgrade its security environment and also the devices used by its development and administrative team. For that, it was decided to be able to detect malwares and also to improve the incident response process. To do so, the additional tools expected were an antivirus and a honeypot. This is an update of the initial requirements of the Smart Grid pilot.

As these tools are available in the list of tools proposed by the partners, a plan to integrate them into GridPocket architecture will be made.

Component name	**Description**
GravityZone Antivirus (Bitdefender)	GravityZone Antivirus from Bitdefender will provide us a tool to response in case of infecting one of our devices with malicious code. This may play crucial role in securing our inner network and prevent private data we are processing from being compromised.
Honeypots (Forth)	Honeypots provide additional security layer in case of breaking the outer protection of Gridpocket network. They may prevent intruders from accessing or deleting sensitive data from our database by offering them an easy prey. This solution may greatly improve reliability and security of Smart Grid solution we provide.

3 Description of the use case

GridPocket is a software company specialized in providing SaaS to utilities customers. Due to the nature of these customers its software is used by a high number of people storing their personal data. GridPocket has recently conducted a project to achieve compliance with GDPR and is conducting several initiatives to increase its cybersecurity profile. The SMESEC project, with its possibilities of integration, is an excellent opportunity to join forces with leading companies in the field of security thus obtaining an improved security posture.

GridPocket plans to implement several components of 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 bases on processing huge amounts of sensitive data, obtained from smart meters installed in customers' houses, so cybersecurity plans crucial role in its functioning. Any potential security corruption in PowerVAS can lead to serious consequences, such as compromising our client – utility company – and GridPocket as well.

3.1 Architecture and design

The main goal of the smart grid use case is to provide user friendly web and mobile applications to utilities customers. These applications aim to provide much more details and information to customers about their energy consumption, but also to be able to control their consumption using smart devices.

To make it work, a given number of interactions are expected:

- GridPocket PowerVAS and Utility CRM & Metering Systems: this interaction enables to gather metering readings from smart meters and feed the application with data that will be used to perform analysis.
- GridPocket PowerVAS and 3rd party IoT & Web services: this interaction enables to control smart equipments, check their status, perform actions for energy consumption regulation.
- GridPocket PowerVAS and End-User: This interaction enables end-user to access their personal information, configure actions to be performed, check analysis results.

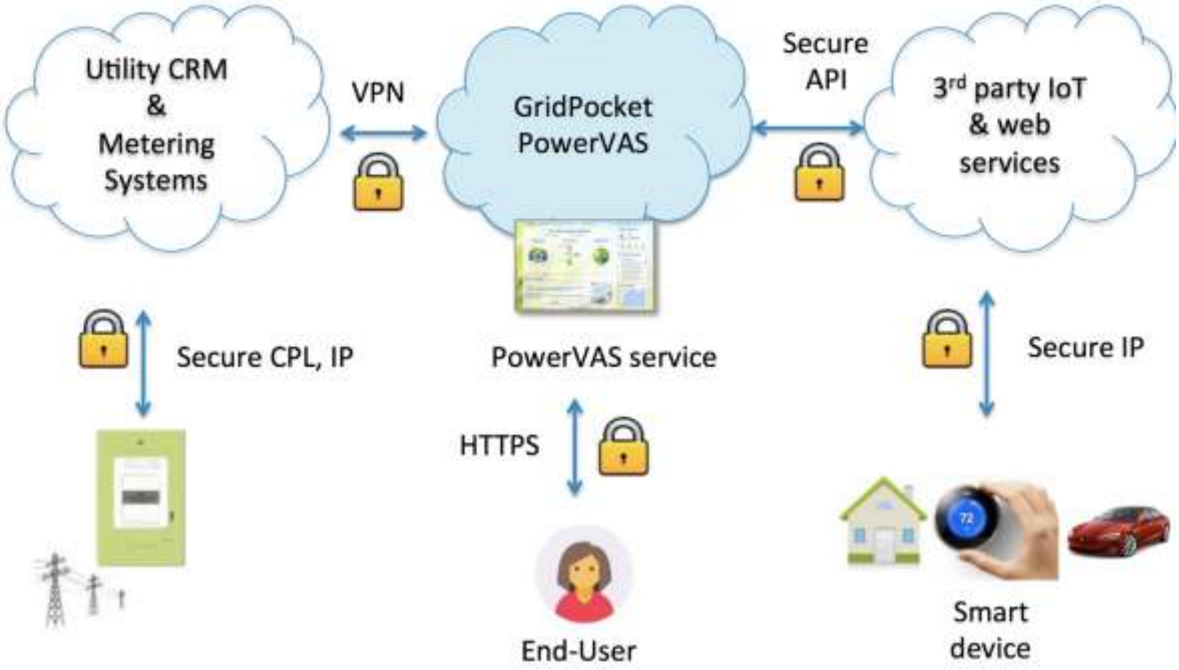


Figure 1: Use case architecture

These interactions described above require an extremely high level of security as PowerVAS represents an entry point to utilities digital resources. Securing these interactions will result in protecting not only users' private data, but also their physical integrity due to the possible control smart equipment.

Various devices connect with our pilot using different routes and endpoints. Those are specifically:

- secure cpl, ip - managed by the utility CRM system.
- vpn - connection between the API server and the utility system that lets us pull data.
- https - website of powervas.
- secure API - API of smart home providers, such as Netatmo and Nest.
- secure IP - managed by the smart home service provider.

Implementing SMESEC will help protecting some crucial points in SmartGrid pilot. Those will be specifically :

- User authentication (TaaS).
- Inner network communication (IDS).
- Connecting with third-party providers and Internet (Netscaler).
- General security maintenance (GravityZone).
- Protection in case of breach into company network (Honeypots).
- Controlling cybersecurity status (XL-SIEM).

3.2 Scenarios of application

The Pilot result will provide the guidelines to exploit the components into real world applications in the following scenarios:

- User accessing internet-based web application (web site).
- Mobile application.
- Exposition of API to third Parties.
- Integration of Smart Home Technologies.

3.3 Cybersecurity threats and impact

As said in chapter 3.1, PowerVAS represents an entry point to utilities resources. So, main cybersecurity threats would be:

- Users private data leak – Threat with the highest probability rate, due to multiple routes of obtaining user data, and the dispersion of the network of smart meters. This risk can lead to serious credibility loss, both for GridPocket and its customer.
- General Data Protection Regulation (GDPR) violation – GDPR violation entails the risks of various types: First and the most obvious is that company may be charged a fine up to 4% of its total annual turnover. Another risk is linked to loss of reputation on the market, leading to decreased income, and potential financial problems.
- Intrusion in GridPocket system enabling taking control of devices – Probably the most dangerous threat, with potentially disastrous consequences, both for company and its customers. In case of obtaining entry to Gridpocket inner network, attacker might gain access to sensitive data of multiple companies cooperating with Gridpocket, as well as the data of their end users. Attacker also could harm company infrastructure, erase all the data from database, or destroy the connection between company machines. In case of such event, company would have to face costly and time-consuming recovery, as well as many hard to predict long-term consequences.

The most important impact will be to make GridPocket and its customers (utilities) lose credibility and clients.

3.4 Cybersecurity training and awareness status

GridPocket has one Cybersecurity expert who monitors and audits GridPocket’s platform. This expert organises regular training sessions to let all the team aware of the different possible threats and the good practice to apply to protect ourselves or to mitigate them. This process helped GridPocket maintain to a very low rate the number of incidents over time. Apart from that Gridpocket will make use of opportunity given by SMESEC to improve the cyberthreats awareness among its workers. Company will appreciate the most courses and materials on securing web and mobile applications, as those are the parts of our product that are used by all of our end users.

3.5 Business opportunity

SMESEC framework and the training & awareness platform will help 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.

It shows our willingness to make our product more and more secure by being engaged in the most cutting-edge technologies integration.

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.

4 Integration of the SMESEC Framework

This chapter will show how the SMESEC framework, or the tools of the framework, enhance the architecture of the pilot and the status of its integration. Additionally, it presents the testing methodology that will be used for each component.

4.1 SMESEC-enhanced business pilot

General architecture of solution used in Smart Grid Pilot contains many dispersed devices providing real time data, that need to be managed and processed by our product. The core component of our Pilot is PowerVAS application. It is a robust technology, collecting and processing data from all inputs. It consists of three main elements: Semantic Machine-to-Machine component, Consumer engagement and behavioral applications and Energy Data Management Platform.

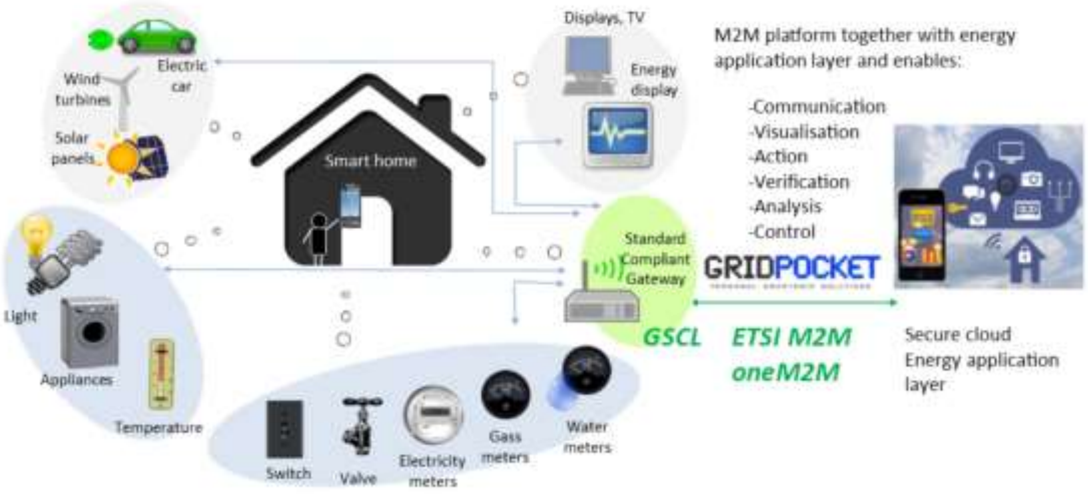


Figure 2: Overall architecture of Smart Grid Pilot

In chapter 3.1, we described the general architecture and the interactions between actors. More detail on initial technical architecture of GridPocket system is as below:

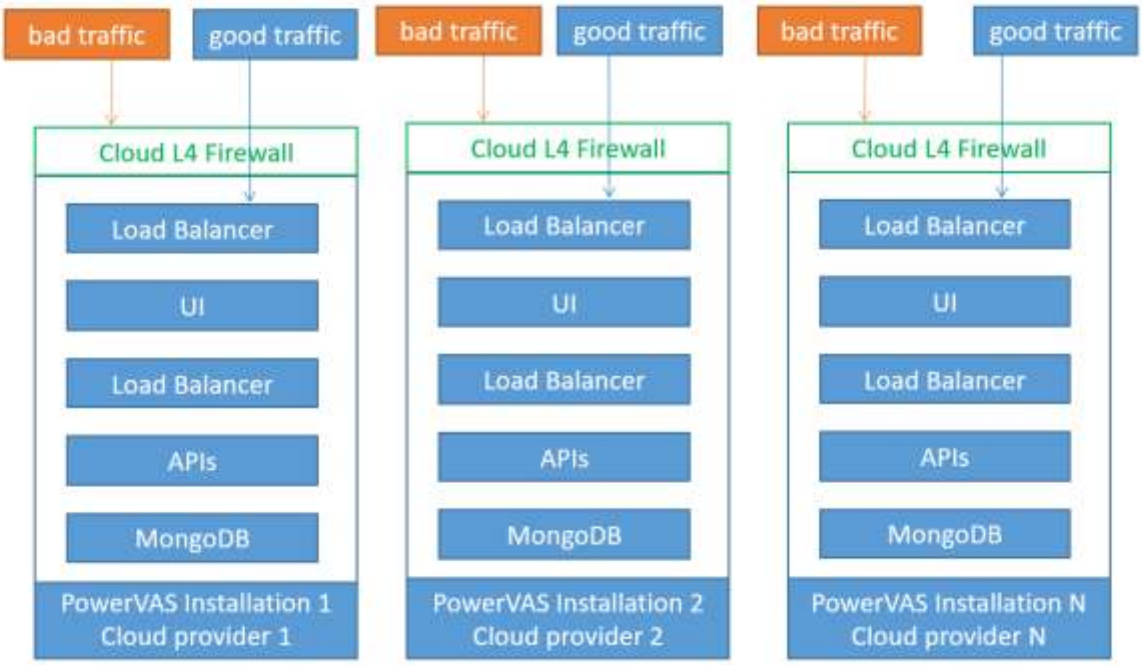


Figure 3: Initial PowerVAS architecture

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. Having multiple instance of UIs, APIs and Databases linked together with Load Balancers, 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 enable to greatly improve the concept of defence in depth. The most important tool missing is a WAF, also called a Layer 7 firewall and a SIEM, which would play a vital role in the incident response process and therefore in the overall GridPocket security strategy/management. Another nice to have tool is a centralized antivirus as the one proposed by Bitdefender and a testing tool as the one proposed by EGM.

The upgraded architecture of GridPocket system with SMESEC tools is:

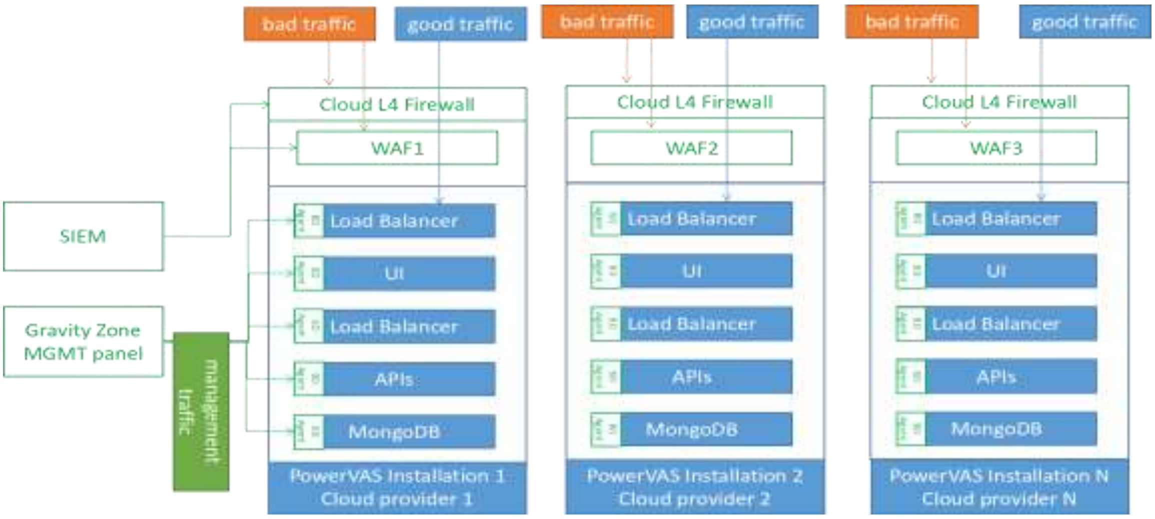


Figure 4: Enhanced architecture with SMESEC tools

With SMESEC, Smart Grid receives several additional security layers. Previous cloud firewall is extended by Netscaler WAF, user authentication mechanisms are ensured by TaaS, inner communication between different components of network is secured by IDS, each machine in the 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 XL-SIEM.

The architecture above doesn't represent the integration of the EGM TaaS. Indeed, the TaaS will not be core part of the technical product that will be deployed in the cloud. It will be mainly used to run scenarios to test the APIs and make sure they work as expected.

4.2 Process and tools integrated

According to the description of the upgraded architecture above, the selected and (partially or fully) integrated tools that are:

Tool	Expected usage
XL-SIEM	The SIEM will be used as the central component of the SEMSEC architecture. It will allow the analysis of suspicious pattern of traffic and it will also send alarm should it detect that an attack event is on-going.
NetScaler WAF	The WAF will be 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, cross site scripting.
IDS	The SNORT IDS will perform a crucial monitoring of the GridPocket Intranet from within and thus from a privileged observation point. It will routinely scan 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 will be used to continuously monitor one 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.

Table 1: Tools expected usage

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

4.2.1 XL-SIEM

GridPocket did receive 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, the verification of the link between the agent and the portal was simply performed by observing the reception of the updated messages from the agent in the cloud portal.

XL-SIEM is the central component of updated architecture of our pilot. It gathers the information from all other SMESEC monitoring tools. Implementing XL-SIEM will make easier managing and supervising security of company inner network.

Here the Cloud Portal for GridPocket can be seen below with the Alarms Threat Level (Right) at a low level:

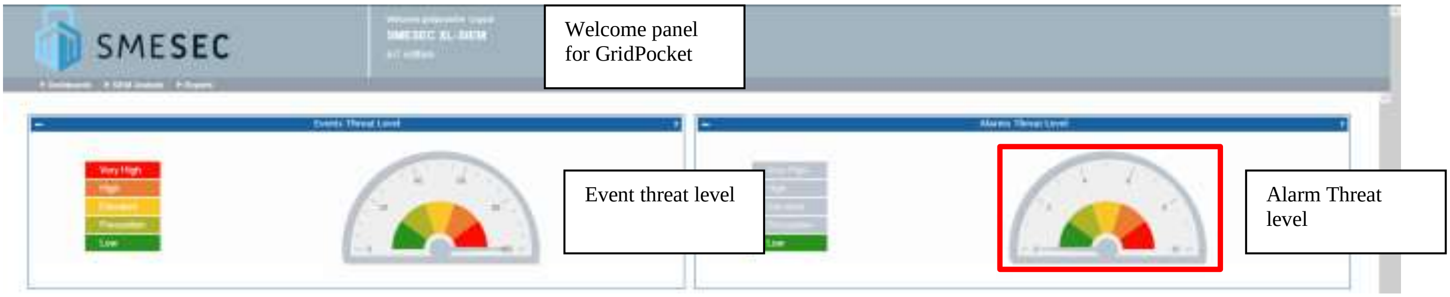


Figure 5: SIEM - GridPocket cloud portal

This is the log of received data from the cloud SIEM:

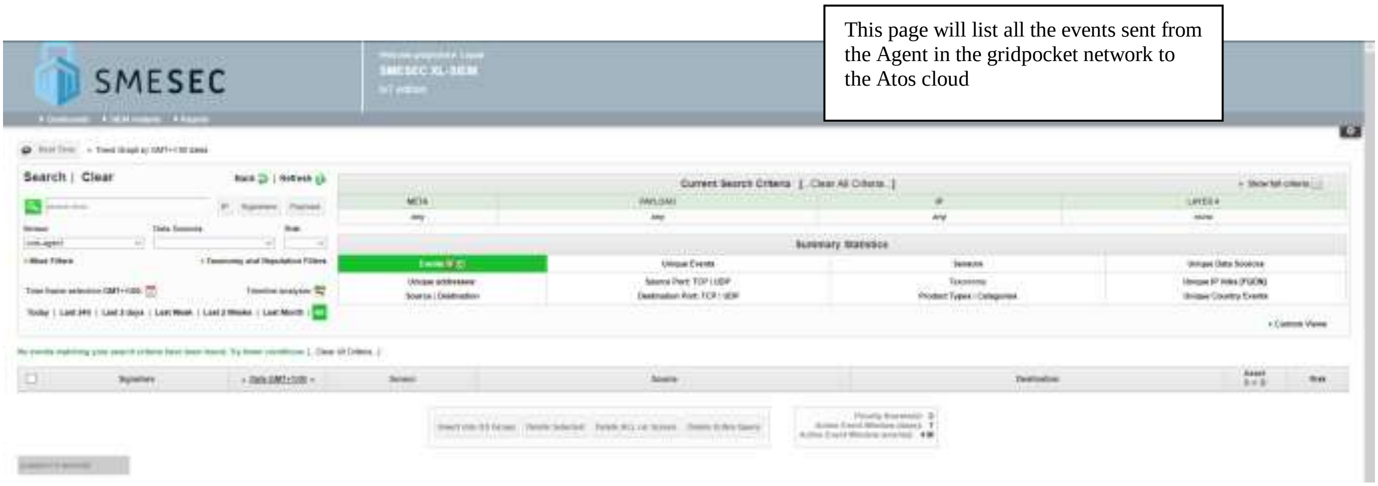
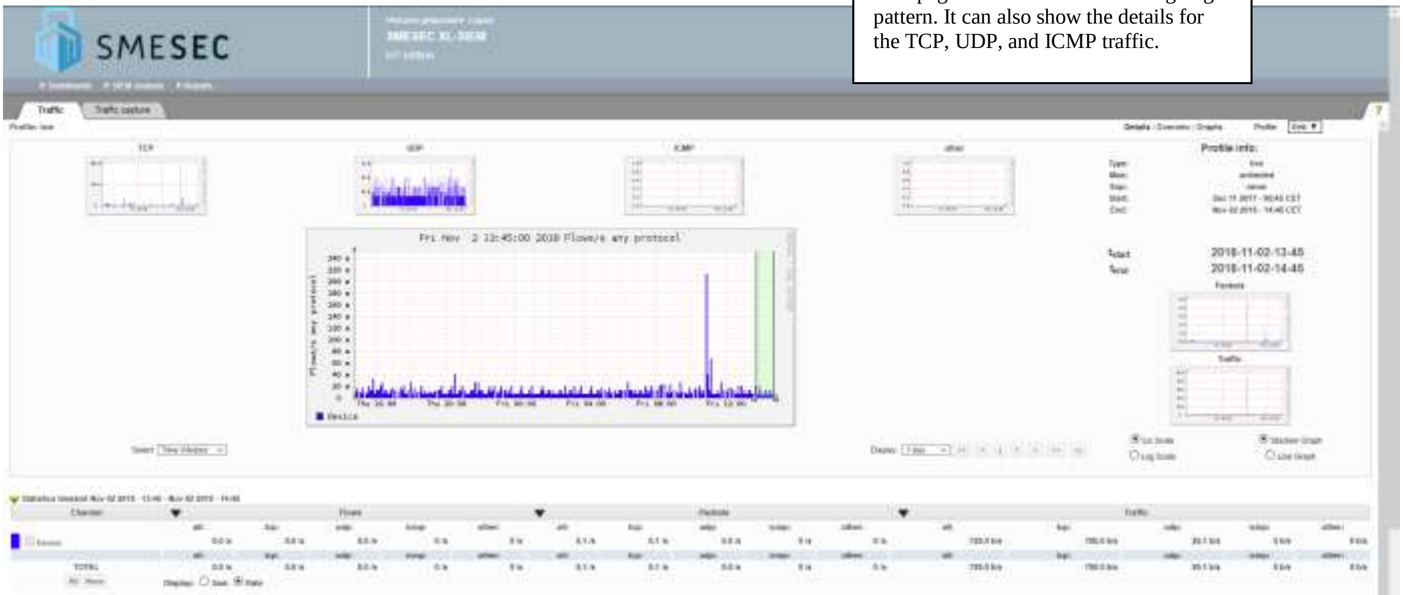


Figure 6: SIEM – Example of logs

This is the traffic pattern analysis:



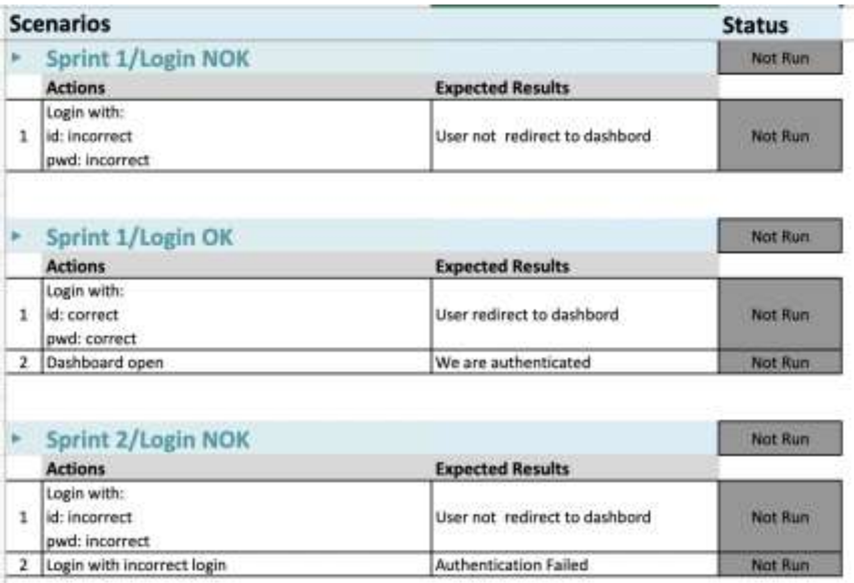
This page shows all the traffic on-going pattern. It can also show the details for the TCP, UDP, and ICMP traffic.

Figure 7: Traffic pattern analysis

4.2.2 TAAS

One of the main functionalities that need to be tested is the authentication process and restriction access. The authentication is done through a REST API using credentials (username & password). As there are different types of user (normal user, admin, public…), there will be customized access rights such as read only, update, deletion. TaaS will be used as quick and secure authentication tool. It will increase security confidence of PowerVAS, contributing to better overall security of our pilot.

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 8: Test scenarios publication

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”.
- User trying to login with correct identifier and password redirect the dashboard with a status result set as “We are authenticated”.

The next steps are to go further in the tests scenarios implementation requiring the long-term license to be provided by EGM, and to deploy these scenarios with all the details related to IP/domain names of servers, different types of credentials to the test platform.

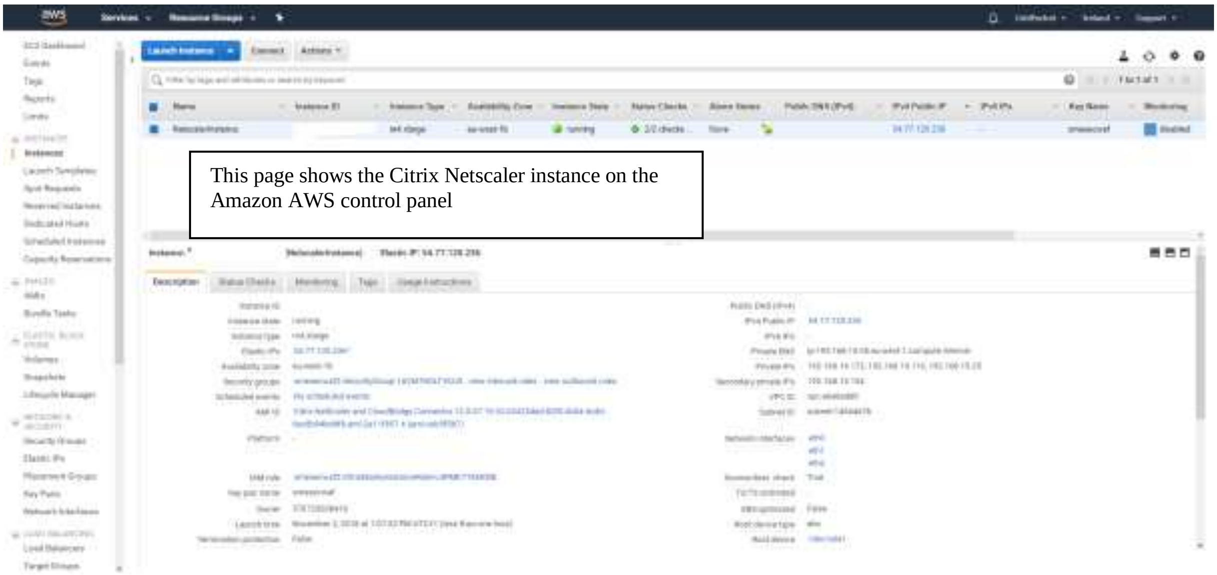
As already mentioned in 4.2.1, GridPocket is still waiting for implementation of EGM TaaS tool, due to delay on the side of EGM.

4.2.3 Netscaler WAF

WAF stands for Web Application Firewall. Netscaler will prevent any suspicious traffic from accessing the PowerVAS. It will significantly increase the security level of our pilot, by filtering out most of potential threats. Including this tool will also improve the credibility of our 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.

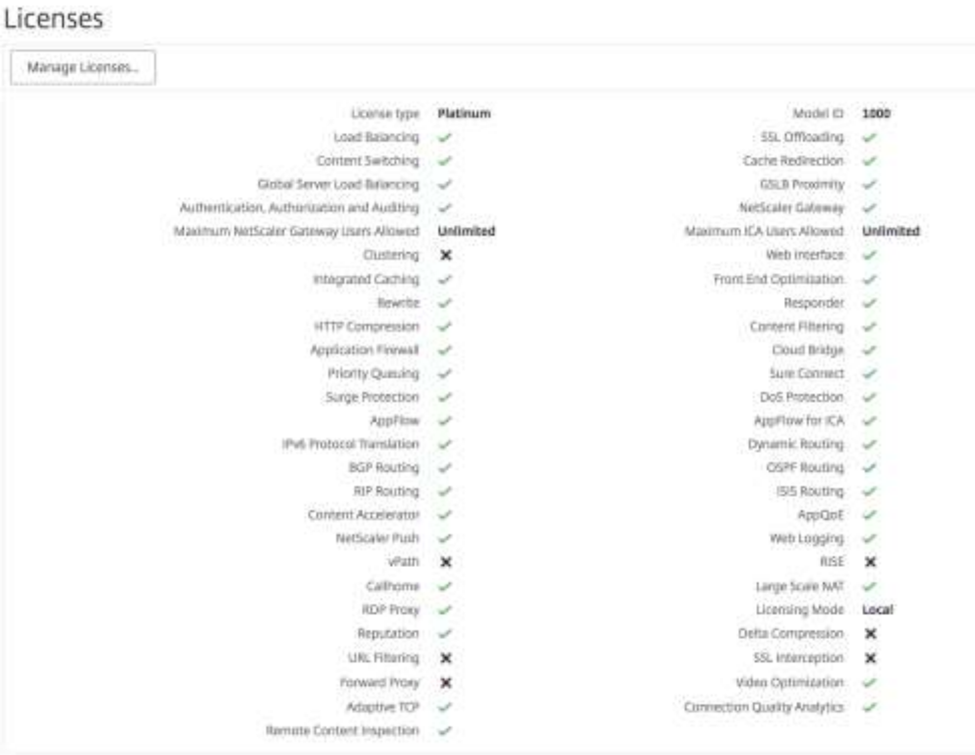
The deployment overview can be seen here:



This page shows the Citrix Netscaler instance on the Amazon AWS control panel

Figure 9: 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:



Licenses

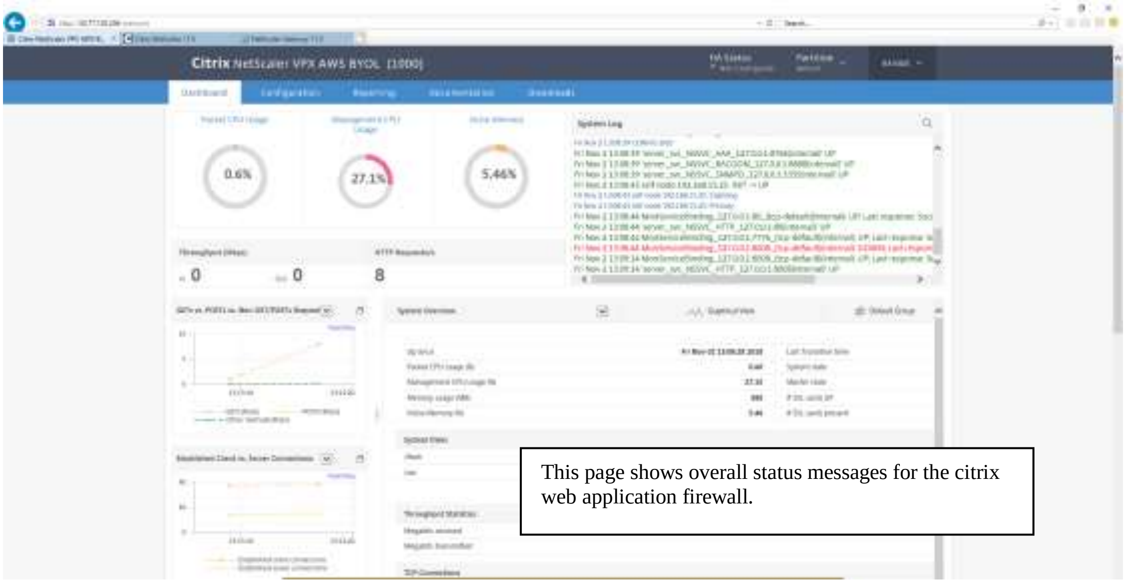
Manage Licenses...

License type	Platinum	Model ID	1000
Load Balancing	✓	SSL Offloading	✓
Content Switching	✓	Cache Redirection	✓
Global Server Load Balancing	✓	GSLB Proximity	✓
Authentication, Authorization and Auditing	✓	NetScaler Gateway	✓
Maximum NetScaler Gateway Users Allowed	Unlimited	Maximum ICA Users Allowed	Unlimited
Clustering	✗	Web Interface	✓
Integrated Caching	✓	Front End Optimization	✓
Rewrite	✓	Responder	✓
HTTP Compression	✓	Content Filtering	✓
Application Firewall	✓	Cloud Bridge	✓
Priority Queuing	✓	Sure Connect	✓
Surge Protection	✓	DoS Protection	✓
AppFlow	✓	AppFlow for ICA	✓
IPv6 Protocol Translation	✓	Dynamic Routing	✓
BGP Routing	✓	OSPF Routing	✓
RIP Routing	✓	ISIS Routing	✓
Content Accelerator	✓	AppQoE	✓
NetScaler Push	✓	Web Logging	✓
vPath	✗	RISE	✗
Callhome	✓	Large Scale NAT	✓
RDP Proxy	✓	Licensing Mode	Local
Reputation	✓	Delta Compression	✗
URL Filtering	✗	SSL Interception	✗
Forward Proxy	✗	Video Optimization	✓
Adaptive TCP	✓	Connection Quality Analytics	✓
Remote Content Inspection	✓		

Figure 10: 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.

The final overview of the WAF can be seen here:



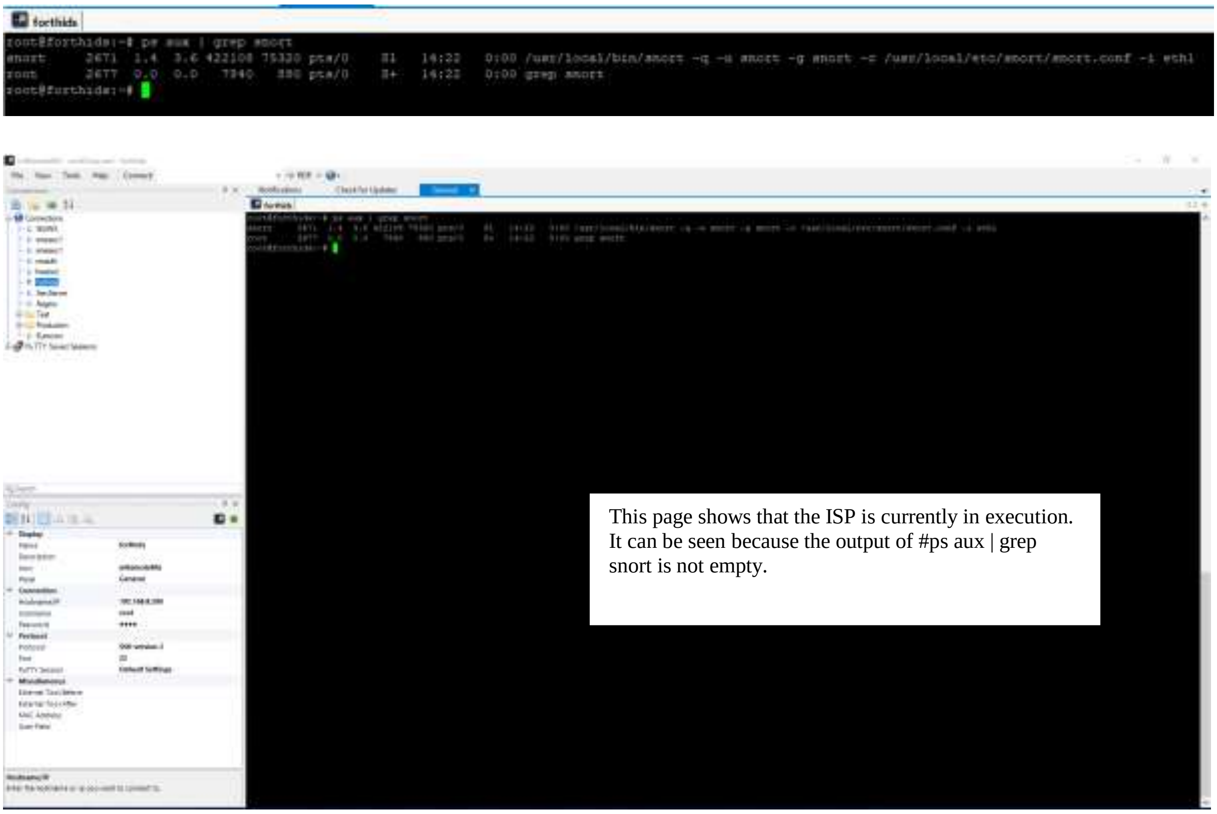
This page shows overall status messages for the citrix web application firewall.

Figure 11: Citrix WAF final overview

4.2.4 IDS

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

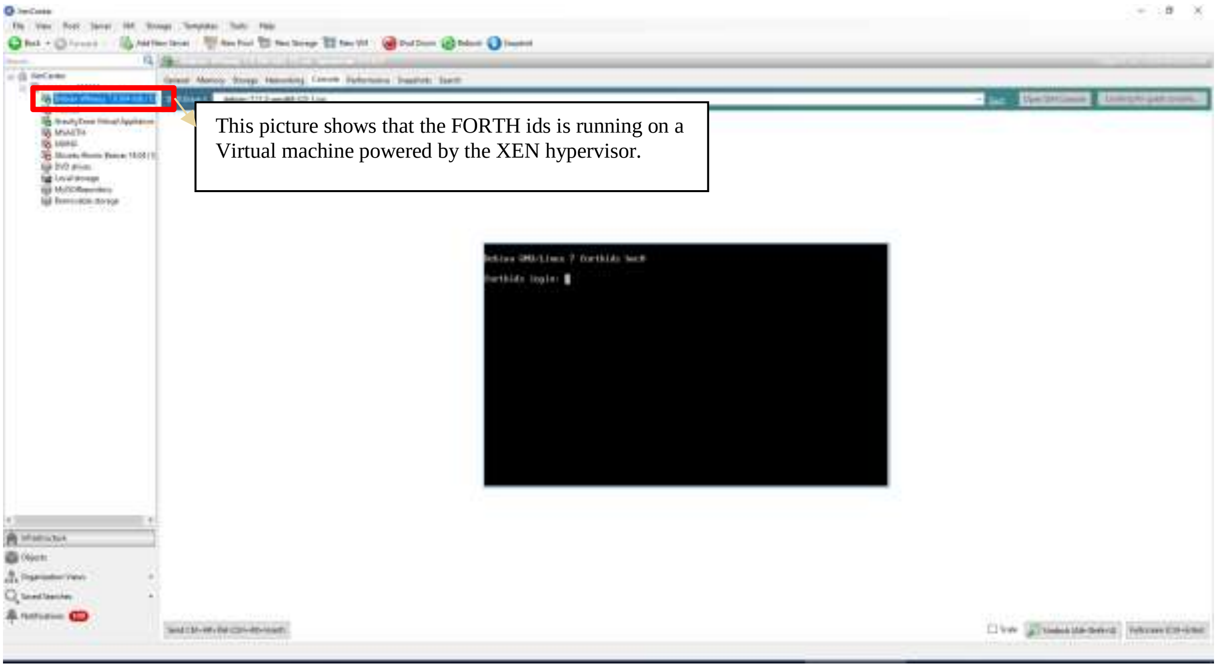
After getting installation instructions from Forth, the first attempt of installation failed because of missing resources (libraries, urls etc). Therefore, a mail thread was started with FORTH in order to get more up to date instructions, which lead to an installation success. The IDS can be seen up and running in the picture below:



```
root@forthids:~# ps aux | grep snort
snort     2671  1.4  3.6 422108 75320 pts/0    Sl   14:22   0:00 /usr/local/bin/snort -q -u snort -g snort -c /usr/local/etc/snort/snort.conf -i eth1
root      2677  0.0  0.0   7840   880 pts/0    S+   14:22   0:00 grep snort
root@forthids:~#
```

This page shows that the ISP is currently in execution. It can be seen because the output of #ps aux | grep snort is not empty.

Figure 12: Forth IDS running



This picture shows that the FORTH ids is running on a Virtual machine powered by the XEN hypervisor.

```
Debian GNU/Linux 7 forthids hvc0

forthids login:
```

Figure 13: Forth IDS running on XEN VM

4.3 Testing

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

- 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.
- EGM TaaS: In its current status, the only way of testing the TaaS is to check if the results of the scenarios implemented (login OK, login NOK) in the Yest software. Further tests will occur once the TaaS implementation is done
- Forth IDS: The IDS aim 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.
- 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 will be held once GridPocket have DNS entry created

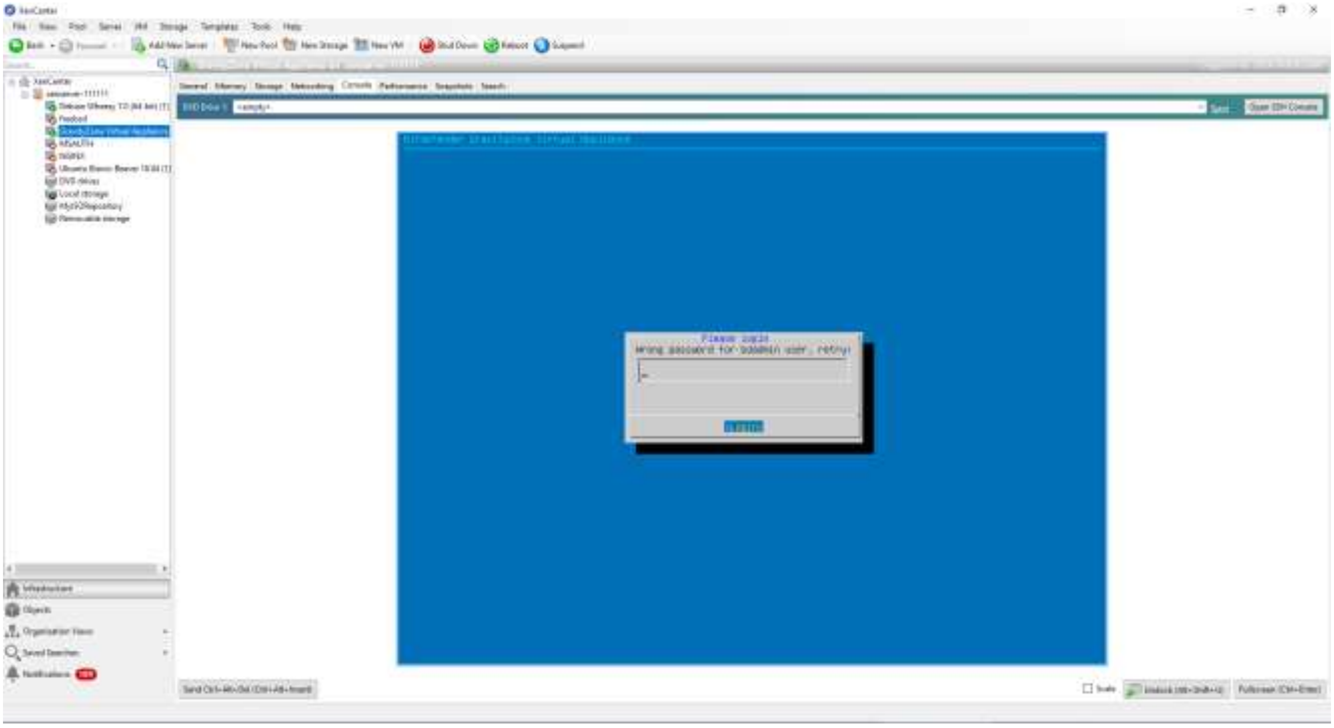
5 Next steps

In the near future GridPocket plans to further improve the security of its pilot. In order to achieve that, we need to finish the implementation of all tools already partially integrated. This task requires further cooperation with our partners, what we are doing right now.

In order to add more security layers to PowerVAS, GridPocket is planning to extend list of SMESEC tools used in Smart Grid pilot by Gravity Zone Antivirus from Bitdefender and Honeypots from FORTH. Moreover, we plan to carry out more internal security trainings to raise cyberthreats awareness among our employees. In the next phase of implementation of SMESEC into our architecture, we will also conduct more overall tests to make sure that all the tools are working as expected.

As described in the upgraded architecture, an antivirus is required but isn't integrated yet. So, the next steps will be to carry on the installation of the Gravity Zone which has already started.

The current status of the integration can be observed here:


XenCenter
File View Pool Server VM Storage Templates Tools Help
Back Forward Add New Server New Pool New Storage New VM Shut Down Reboot Suspend
General Memory Storage Networking Console Performance Snapshots Search
DVD Drive 1: <empty>
Infrastructure
Objects
Organization Views
Saved Searches
Notifications
Send Ctrl+Alt+Del (Ctrl+Alt+Insert)
Scale
Undock (Ctrl+Shift+U)
Fullscreen (Ctrl+Enter)

Bitdefender GravityZone Virtual Appliance

Please login

Wrong password for bdadmin user, retry!

Figure 14: Bitdefender current installation status

To better upgrade the security level of the architecture, it was considered appropriate to integrate a new component: FORTH honeypots. This will enable GridPocket to gather more information about hackers' identity, understand their techniques, and then use these details to better protect its platform.

Individual testing will continue to be performed in parallel to the integration of the different tools in order to make sure each integrated tool provides the expected results. When the whole integration will be completed, scenarios of general testing will be defined and run to validate the overall architecture.

5.1 Integration of business in the SMESEC Framework

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.

So, 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…).

Although integration of SMESEC doesn't change the functionality of PowerVAS for the end users, it will have great impact on our position on the market, as it will increase our status among other companies in our sector, by adding solid security layer to our product. Implementation of SMESEC will potentially elevate Gridpocket above competitors in the market and create more business opportunities for the company.

5.2 Training and awareness plan

As mentioned above, some trainings will need to be held for employees. Different types of training are required as the level of implication in the technical development and integration is different for developers, architects and project managers. Basically, there will be two types of training:

- **Basic**: one for the whole team. It will be mostly about awareness. To let each one knows about the threats and the required good practices. This part of training should focus on avoiding common mistakes that can lead to decreasing the overall security of company products, such as introducing vulnerabilities for cross site scripting and SQL injections into application. Exact training plans are still being discussed.

- **Advanced**: This training is dedicated to the team that will handle the integration of the SMESEC framework into PowerVAS and make sure all the technical requirements are met. Exact design of advanced tests depends on final architecture of SMESEC framework and requirements needed for its implementation

In addition, the Security Manager of GridPocket will make daily use of the dashboard to assess current status. He will also have the task of training other employees and developing training plans.

5.3 Initial testing and validation plan

Tool	Testing Strategy
Forth IDS	These three components will be tested jointly with the same strategy: a penetration test will be conducted on the main endpoint, and it is expected that:
Citrix WAF	
Forth HoneyPots	

	1. The IDS detects the attack 2. The WAF stops the attack 3. The attacker is lured away from the real target by an easy prey which turns out to be the honeypot.
EGM TaaS	This component will be used to test the new authentication micro-service deployed in GridPocket called MS_AUTH. A set of test cases covering user login, logout and general user will be prepared for both normal and privileged user.
Bitdefender Gravity Zone	Test virus signature will be deployed, to check whether it is detected.
ATOS XL-SIEM	The SIEM will provide alerts, which will be correlated with the penetration test activities.

Table 2: Testing strategy

6 Conclusions

6.1 Experience of the initial integration

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. Windows is required.
- **Citrix 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. More documentation from Citrix would be helpful.
- **FORTH IDS**: The main difficulty was the missing of some resources and libraries. After few clarifications and discussions with Forth, the installation could be completed.

From all the SMESEC tools, only ATOS XL-SIEM is fully integrated, while Citrix WAF, Forth IDS and EGM TaaS are almost fully integrated. Gravity Zone and Forth Honeypot implementation started already, but the tools are not functional yet.

6.2 Fulfilling of objectives

Initially, GridPocket planned to make a full integration of the Citrix WAF, the XL-SIEM and the EGM TaaS in the short term. The other components would be integrated in a medium and long term. But, as mentioned in chapter 5 and 6.1, only the XL-SIEM was fully integrated. All the others with the FORTH IDS in addition are partially integrated. The missing part for the Citrix WAF and the Forth IDS is the link between these components and the XL-SIEM make cybersecurity events sharing and gathering possible. Also, as the TaaS tool is not working at the time of writing this document, GridPocket is waiting for EGM to renew the license and implement more test cases for PowerVAS pilot. Currently we are actively working with partners on implementation of all the tools that still are not fully implemented. Delay in implementation of all the tools was caused by problems with installation specific components as well as by personnel changes inside the GridPocket. Currently company is working towards fulfilling all of the objectives.

So, even if the objectives were not fully fulfilled, a good progress was done. GridPocket is looking forward to completing the initial plan and also the implementation of the additional components already started.

6.3 Use in SME environment

As the framework is not yet packaged as a single component, installation process was needed for each tool. In general, the installation of the XL-SIEM was the most obvious one. The other tools required some clarifications, discussions or training from these tools providers. So, managing the components in their current status requires at some points good technical level.

6.4 Improvements for the scenario

GridPocket looks forward to completing the integration of the components described in chapter 5 (Next steps) and welcome new partners to the consortium with new tools which could be integrated and of interest for the Smart Grid pilot. Some of our thoughts after implementing the pilot are:

- In general tools could have better documentation. Implementation of some of them required asking for assistance from creators (e.g. Netscaller), or installing additional libraries (e.g. IDS)
- Tools implementation and using could be simplified and not require any additional training to implement (e.g. TaaS).
- Full integration of all components into single framework will be helpful, as their separate implementation is time consuming. This point will probably lose its importance after SMESEC integration phase.
- Compatibility both with Windows and Unix-based platforms is very important, as SMEs (including GridPocket) often use mixed type of software.

References

[1] **Deliverable:** SMESEC D2.1 – SME security characteristics description, security and market analysis report. Oikonomou George. 2017

[2] **Deliverable:** SMESEC D2.2 – SMESEC security products unification report. Ciprian OPRISA. 2017