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

D2.1 SMESEC security characteristics description, security and market analysis report

Document Identification			
Status	Final	**Due Date**	30/11/2017
Version	1.1	**Submission Date**	15/12/2017

Related WP	WP2	**Document Reference**	D2.1
Related Deliverable(s)	D2.2. D2.3	**Dissemination Level (*)**	PU
Lead Organization	CITRIX	**Lead Author**	George Oikonomou
Contributors	ATOS, BD, EGM, FHNW, FORTH, GRIDP, IBM, SCYTL, UOP, WOS	**Reviewers**	Francisco Hernandez, WOS
			Jose Francisco Ruiz, ATOS

This document is issued within the frame and for the purpose of the SMESEC project. This project has received funding from the European Union’s Horizon2020 Framework Programme H2020-DS-SC7-2016 under Grant Agreement No. 740787 and supported by Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 17.00067. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the European Commission.

This document and its content are the property of the SMESEC Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the SMESEC Consortium or the Partners detriment and are not to be disclosed externally without prior written consent from the SMESEC Partners.

Each SMESEC Partner may use this document in conformity with the SMESEC Consortium Grant Agreement provisions.

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

Keywords:

security, market, survey, WP2, requirements, capabilities, use case, protection, endpoint, IoT, sensors, incidents, threats, smart city, smart grid, e-voting, firewall, SIEM, anti-virus, testing, compliance, maturity model, honeypots, patching, antiROP

Document Information

List of Contributors	
Name	Partner
Jose Francisco Ruiz	ATOS
Susana Gonzalez Zarzosa	ATOS
Ovidiu Costel Mihaila	BD
Ciprian Oprisa	BD
George Oikonomou	CITRIX
George Tsolis	CITRIX
Philippe Cousin	EGM
Jordan Martin	EGM
Samuel Fricker	FHNW
Martin Gwerder	FHNW
Alireza Shojaifar	FHNW
Sotiris Ioannidis	FORTH
Christos Papachristos	FORTH
Filip Gluszak	GRIDP
Fady Copty	IBM
Sharon Keidar-Barner	IBM
Jordi Cucurull	SCYTL
Pau Julia	SCYTL
Jordi Puiggali	SCYTL
Adria Rodriguez	SCYTL
Kostas Lampropoulos	UOP
Apostolos Fournaris	UOP
Andrea Bartoli	WOS
Francisco Hernandez	WOS

Document History			
Version	Date	Change editors	Changes
0.3	26/09/2017	Christos Papachristos FORTH	Integration of requirements provided from all use cases-pilots
0.4	02/10/2017	Christos Papachristos FORTH	General Security Requirements
0.5	5/10/2017	George Oikonomou	Added market research results
0.6	10/10/2017	Christos Papachristos FORTH	Introduction added
0.7	15/10/2017	George Oikonomou CITRIX	Market research complete, adding requirements/capabilities
0.8	26/10/2017	George Oikonomou CITRIX	FORTH contribution in use case requirements complete. Product extensions, and requirements vs. capabilities
0.9	31/10/2017	George Oikonomou CITRIX	Changing to final submission template, completing extensions sections. FHNW contribution for risk assessment
0.10	10/11/2017	George Oikonomou CITRIX	Finalizing all section text, correcting spelling errors, adding section conclusions, fixing cross-references. Report ready for internal review.
0.11	22/11/2017	George Oikonomou CITRIX	Addressing first reviewer's comments.
0.12	30/11/2017	Jose Francisco Ruiz, ATOS, Christos Papachristos, FORTH	Added extra feedback from partners, adding second review comments.
0.13	04/12/2017	George Oikonomou, CITRIX	Addressing second reviewer's comments.
0.14	05/12/2017	Samuel Fricker, FHNW, Francisco Hernandez, WOS	Addressed second reviewer's comments.
0.15	11/12/2017	George Oikonomou, CITRIX	Preparing final version.
1.0	15/12/2017	George Oikonomou, CITRIX	Final deliverable version ready.
1.1	15/12/2017	ATOS	Quality review, submission to EC.

Table of Contents

List of Tables

List of Figures

List of Acronyms

Abbreviation / acronym	Description
ACL	Access Control List
API	Application Programming Interface
AST	Application Security Testing
CASB	Cloud Access Security Broker
CSRF	Cross-Site Request Forgery
CYSFAM	Cyber Security Focus Area Maturity
DDoS	Distributed Denial-of-Service
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
EDR	Endpoint Detection and Response
EPP	Endpoint Protection Platform
FW	Firewall
GRC	Governance, Risk Management and Compliance
GW	Gateway
IAM	Identity and Access Management
IDS	Intrusion Detection System
IoT	Internet of Things
IPS	Intrusion Prevention System
ISFAM	Information Security Focus Area Maturity
IT	Information Technologies
MiTM	Man-in-the-Middle
NIC	Network Interface Controller
NSM	Network Security Monitoring
OT	Operational Technologies
OWASP	Open Web Application Security Project
RPO	Recovery Point Objective
RTO	Recovery Time Objective

Abbreviation / acronym	Description
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SME	Small and Medium-sized Enterprise
SNAT	Source Network Address Translation
SSH	Secure Shell
SWG	Secure Web Gateway
UEBA	User Entity Behaviour Analytics
USG	Unified Service Gateway
UTM	Unified Threat Management
VDS	Virtual Distributed Switch
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network
WAF	Web Application Firewall
XSS	Cross-Site scripting

Executive Summary

This document presents the initial analysis of the SMESEC contributed products and their capabilities to cover the pilot use cases security needs. Furthermore, it contains a thorough technical survey of the security market today, positions the SMESEC framework into the existing market, and presents potential SMESEC product improvements.

Although this document is delivered at the same time as the other deliverables of WP2 the work done here was used as basis for the other parallel activities, which are covered in the other two deliverables of this WP (D2.2 [1] and D2.3 [2]). Additionally, the work presented here is (and will be used) by activities of other WPs such as designing and developing of the SMESEC framework architecture, project innovation, validation of the use cases, dissemination activities, etc.

The four SMESEC use cases have been analysed in technical terms, focusing on their security-related issues and concerns. The analysis discusses all desired features that the particular SMEs have identified, but also attempts to extend in the general SME context. An initial risk assessment has been also conducted on the four pilot use cases with the proposed SMESEC methodologies.

The SMESEC contributed products have been then analysed in terms of technical requirements and capabilities in the security field. These products cover a wide range of the security field and the key interconnection points are identified and described in detail in Deliverable 2.2 [1]. The goal was to understand how these products match the pilot use cases requirements.

Finally, an extensive technical survey of the security market has been conducted for identifying the major market segments, the key players in each segment and their products. Having knowledge of the security market details will help positioning SMESEC framework offering and relate it with other products. Apart from identifying the strengths of a unified solution, this survey has assisted in understanding what other in-market solutions can fit in SMESEC and what are the possible technical and innovative extensions in existing SMESEC products that could cover these gaps.

The key outcomes of this report are that SMESEC products can currently satisfy a large deal of security requirements in many different market segments in the context of SMEs. Having the pilot use cases as a guide, the project addresses some security issues that SMEs face in their everyday operation. Furthermore, the product extensions proposed will help to extend the coverage of SMESEC framework within the security market: the integration of multiple features under a single framework will give an added value both to the products and the framework itself in regard to the competition.

1 Introduction

1.1 Purpose of the document

This is the first deliverable of WP2 “Adaptation of SMESEC security components to SMEs requirements”. The role of this WP in the SMESEC project is to provide the basis where other Work Packages will rely to define the architecture (WP3), the validation of the use cases (WP4), the innovation (WP5) and position in the security market (WP6).

Specifically, D2.1 provides a detailed description of the use cases and the contributed products of the partners of the project. On the one hand, the part of the SMESEC use cases describes in-depth the scenario of the use cases, requirements and needs (focusing in a wide range of SME security requirements), expected functionality with SMESEC, etc. On the other hand, the section of the contributed products analyses all tools of SMESEC and presents, after the breakdown of the functionality of each product, the way they work, planned extensions, and the range of capabilities in the security market they cover. The current state versus the desired one to achieve at the end of the project is finally described.

Therefore, the purpose of this document is to identify how the products will respond to the SME security needs, though the detailed examination of the SMESEC pilot use cases and the thorough technical view on the contributed products.

1.2 Relation to other project work

As described previously, this document covers the needs of the SMESEC use cases as well as the contributed product capabilities. This is the ground where other deliverables and Work Packages will be based, and more specifically:

- D2.2 will describe the interfaces between the SMESEC products, based on the initial survey covered in Section 5.
- D2.3 will elaborate on the initial pilot risk assessment as covered in Section 3.
- WP4 will describe integration and validation in the use cases using as basis the requirements and needs provided here by the partners
- WP5 takes into account the product extensions in Section to discuss about Innovation.
- WP6 uses parts of the market research in Section 4 to analyse from a business perspective, whereas D2.1 covers the technical characteristics of the market segments.

1.3 Structure of the document

This document is structured in six major chapters.

Chapter 2 introduces the SMESEC use cases and, after a high-level description of the security needs, explains in thorough detail the technical aspects of each of the four use cases: e-voting (SCYTL), smart city (University of Patras), IIoT sensors (WorldSensing) and power grid (GridPocket). For each of those the top ranked threats and security needs are provided, as identified by the partners.

Chapter 3 presents an initial risk assessment of the use cases. The CYSFAM maturity model method has been applied to both analyse risks and build an automatic risk assessment for checking the fulfilment of KPIs in the project.

Chapter 4 provides a thorough survey of the security market segments for SMEs today and identifies emerging markets that are greenfield for innovation. For each of these segments, the key players and their products are presented in summary.

Chapter 5 covers the technical characteristics of the partners' tools and identifies the capabilities and the value that they bring into SMESEC. An analysis of the technical characteristics helps also to identify possible links among them.

Chapter 6 analyses the use case requirements (as set in Section 2) and the SMESEC product capabilities (as analysed in Chapter 5) in order to match them in a way that will assist the SMESEC framework architecture.

Chapter 7 provides details for potential extensions to the SMESEC products identified by the partners (owners) linked to the results of the market analysis (Section 5) and the potential matches to the use case requirements and needs (Section 6).

Chapter 8 finally presents the conclusions of this report, and links the results to the other WP2 deliverables.

2 Security Requirements Analysis

Small and Medium-sized Enterprises (SMEs) are an important driver for innovation and growth in the EU [3]. Taking into account cyber-security, SMEs do not always understand all the risks and business consequences for the development of technologies without the adequate level of protection against cybercrime. The level of SMEs information security and privacy standards adoption is relatively low [4].

The increasing pressures from external and internal threats demands for the SMEs to have a consistent and iterative approach for identifying, assessing and managing cybersecurity risks. All enterprises, despite their size, heavily relay on new technologies, communication, and the interconnectivity of information technology and operational control systems. This adaptation and reliance on IT and OT systems, and networks has changed and expanded the potential vulnerabilities and increased potential risk to enterprise operations [5].

These potential risks and vulnerabilities may expose the privacy of the end-user or of the SME's service. Compromising the identity of the end-user can have catastrophic results to the SME's reliability and trust with direct impact to its work cycle [6]. Moreover, there are certain types of services that require the transactions between the user and the services to be completely private with the end-user, in order to be able to confirm that her transaction was successful. Thus, it is essential to have a strong framework that protects the privacy of the end-users and the SME's information.

To manage cybersecurity risks, a clear understanding of the SME's business models and security considerations specific to its use of information technologies and control systems is required. Because each SME's risks are unique, along with its use of information technology and operational control systems, thus a variety of tools and methods need to be used in a unified manner to fulfil the required features.

2.1 SMEs Common Systems and Services that need to be protected

In order to identify the common security requirements, it was needed first to identify what are the common services or type of services running in all the pilots. The following list summarizes these commons services running and the assets of each one, that the SMESEC framework needs to protect:

- **Web servers** *(front-end, application and presentation servers)*: Most IT-enabled SMEs, use at least one type of web server in order to serve their content, run their applications or present analysis and results of their system. Thus, a basic requirement is to provide tools that protect web servers of all kinds and flavors.
- **Database servers:** The use case SMEs use databases to collect data from the sensors, to retain user information, save the state of the application and more. A framework aiming to protect SMEs is essential to provide mechanisms securing databases along with policies enhancing user privacy.

- **Network interconnectivity:** The network connection, either to the private network or the internet, is essential for the undisturbed activity of the enterprise. A DDoS attack for example, could cripple the network connection of the SME making it unreachable for the users.
- **Cloud:** The cloud and virtualization technologies are becoming more and more a part of enterprise solutions as well as the main platform for web based application servers. Thus, there is an increasing need to secure the cloud-based services of SMEs
- **End-node, sensors, data-loggers:** The use case SMEs utilize end-nodes hardware or software that send and receive data to / from the SMEs' core. These end-nodes are generally considered unreliable, sensitive and untrustworthy. The proposed framework should be able to secure the connection of these end-nodes to the core and improve their reliability. Finally, it should provide privacy enhancing and anonymity features.
- **Gateways:** End-nodes like sensors, data-loggers or IoT devices, usually communicate with the core network of the SME through software or hardware gateways. If an adversary could take control or incapacitate these gateways, the whole SME service would be handicapped.
- **Virtual Machines:** More and more SMEs rely on virtualization technologies such as Cloud, Virtual Machine Instances, etc. to run multiple and concurrent services for the public. The SMESEC framework should offer security features for protecting applications running inside a virtual machine as well as the one virtual machine instance from attacking the other.

2.1.1 Internal Threats

Numerous internal threats have been identified that are common among SMESEC use case SMEs. Internal threats could be proved catastrophic for the SME as the malicious insider has closer access to the SME's resources and key points of the infrastructure. As a result, the proposed framework should take into account the possibility on malicious insiders and provide tools and mechanisms that detect and mitigate the effect of an inside attack incidents. The common internal threats identified by SMESEC pilots are the following:

- **Users' privacy compromise:** The data, of the users, that are kept by the system can be compromised and their privacy exposed.
- **Alteration or deletion of sensitive data and/or software**: Malicious insiders could alter or delete sensitive data and software that would render the system incapable of operating. More over user's data could be altered or deleted.
- **Unauthorized manipulation of data and/or software:** The system could be manipulated by an unauthorized malicious insider in improper ways to attack other systems or gain access to data that, otherwise, would be infeasible.
- **Inside attack to the system (DoS, code injection):** Direct attack to the system resources by using the system's own infrastructure.
- **Sabotage:** A malicious insider could sabotage the system by a number of malicious and improper acts that could hinder the system's operability or reliability.
- **Data leakage:** This internal threat is crucial to all SMEs and other infrastructures, as information is a key part of any system and leaking inside information can have catastrophic consequences to the SME or the infrastructure.
- **Unprotected SSH keys – unauthorized access:** Unauthorized access to the system by users without the proper credential could expose the system to greater threats as mentioned before.

2.1.2 External Threats

The four use cases have identified the external threats that their system may face and have grave consequences to their infrastructure. External adversaries could vary from enterprise espionage and malicious competitors up to hackivists. Malicious competitors aim to attack the reliability and the proper operation of an enterprise, in order to create margins to gain a larger part of the market. Hackivists, on the other hand, could attack a specific SME if they consider its serves proposes they oppose to or for some unidentified reason. All those groups of attackers pose the following list of potential external threats:

- **Unauthorized use of the system:** Users of the system should be authorized and granted access based on the privilege group they belong to. Unauthorized access could lead to more serious threats that are mentioned below.
- **Impersonation, Repudiation, MiTM attacks:** A large number of threats have to do with the incorrect identification of the user and thus the possibility of adversaries impersonating legit users, reusing credential or altering legit requires for malicious purposes.
- **Privacy compromising:** Exposing private data of the SME system or the users, by compromising key databases or other data centers is a serious threat to consider for all SMEs.
- **Alteration or deletion of data:** Accessing, altering or deleting sensitive data of the SME from a remote location is a real threat that all SMEs face. The proposed SMESEC framework needs to provide solutions that protect SMEs' data from external unauthorized modification.
- **Distributed Denial of Services:** DDoS attacks are the most common attacks against infrastructures and SMEs, as they are difficult to mitigate and can cause heavy hindrance to the proper operation of the system. The use of amplification attacks has risen as they are easy to perform and difficult to counter by the security systems.
- **Physical attack to key system locations:** A physical attack to a specific sensitive location of the SME infrastructure hosting system servers, gateways or other physical assets of the SME is always a threat.
- **Targeted attacks to datacenters, gateways and other key points of the infrastructure:** Software or denial of service targeted attacks to specific key points of the system infrastructure can be extremely destructive for the SME and render it useless.

2.2 General Security Requirements

In this section, the security features and requirements that are shared among the pilot SMEs and the small and medium enterprises in general are explored. With these features and requirements in mind, a more concrete and general solution can be provided through the SMESEC project that will be applied to all SMEs and not just SMESEC Pilots.

2.2.1 Physical Protection

Each of the use case SMEs use plethora of physical assets. Whether IoT Sensors for the industrial IoT pilot are considered, or Voting Ballots for the online voting pilot, Network Gateways for the SmartCity pilot, reverse proxies for the SmartGrid pilot, SME data centers or even high-value PCs spread across different locations need to be protected. The physical protection of these assets is a de-facto high priority security requirement, as all assets are vulnerable to a variety of physical attacks.

More information about the assets that each use case SME holds can be found in the sections 2.3-2.6 where each use case SME is presented.

Although, the cost and disturbance that a physical attack can cause to a number of high-value assets are taken into account, it is not a specific goal of the SMESEC framework to explore. In the context of the SMESEC project the focus is on network, cyber, software and hardware attacks, that can be performed against SME's core IT or OT systems.

2.2.2 General Security System Requirements

Small and Medium Enterprises security characteristics may differ significantly from one SME category to another. Every enterprise contains different critical assets, implements different technologies and tools, and needs different protection methods in order to mitigate specific attacks targeting its assets or protocols.

With that said, there are common security requirements and features that were extracted after receiving extensive input from our four use case SMEs. Although the use case SMEs are active to distinctively different market areas, a number of common security requirements has been identified that do appear to be crucial in our use case SMEs but in most small and medium enterprises, as well, and will be further explored in the following sections.

2.2.2.1 High level Security System Requirements

All pilots have identified the following high-level requirements as crucial for their SME to operate unhindered and efficiently. These high-level requirements need to be covered by the proposed security framework.

- **Availability:** All pilots have identified the need for their systems and services to be available to their end-users. SMESEC framework needs to provide tools and methods that will enhance systems' availability
- **Usability:** The proposed security framework should be easy to use by the SMEs' system administrators with no to little training
- **Privacy:** It is of high importance that the SMESEC framework protects and enhances the privacy of SMEs' information and end-users.
- **Cost:** As SMESEC aims to protect small and medium-sized enterprises the cost of deploying and maintaining the proposed framework has to be small.
- **Alerting:** All SMEs require a complete and configurable alerting mechanism that will produce alerts and logs based on the incidents that are taking place in their systems and networks in real time.
- **Ease of Control and Administration:** The whole security framework must be configurable and easy to use by the SMEs' administrator.
- **System Integrity:** SME systems need to be resilient against cyberattacks, thus the system's integrity should be conserved at all times or specific response and recovery protocols should be in place.
- **Confidentiality:** All information used by the system and/or provided by its end-users should be kept private following the SME guidelines and needs.

- **Non-repudiation:** There is a strong need among the SMEs that each asset/service of the system will be accessed by the authorized user/admin.
- **Authentication:** A strong authentication scheme must be in place in all SMEs in order to deter unauthorized access to valuable assets and services. Furthermore, privilege escalation should be prevented by all costs.
- **Scalability:** The security framework proposed should provide scalability being able to cover the growing needs of an SME with multiple nodes, users and accesses being added daily.

2.2.2.2 Cyber Security Requirements

Apart from the common high-level security requirements that all SMEs share there are common cyber-security and network-security specific requirements that need to be fulfilled by the proposed framework. As all small and medium enterprises take advantage of the information technologies and information networks providing services that require interconnectivity, cloud-based operations, web services, web applications and remote/local database access, the need of cybercrime specific countermeasures is more than apparent.

Taking into account all the assets that need to be protected as well as the requirements clearly stated by the use case SMEs, we have extracted the following common cyber security and host protection requirements:

- **Protection against code injection** that can happen via URL Misinterpretation, Input Validation problems or Buffer Overflow attacks. All these attacks are common against web servers and web services. Also, session hijacking is another common attack against web applications and need to be addressed by the proposed framework.
- **Protection against Denial of Service (DoS) attacks** that target the network, OT or IT, of the SME by sending large volumes of date **(**aka volume attacks) or DoS attacks that target the application protocol (aka application layer attacks). These kinds of attacks gain more and more fame between the adversaries as they can render a whole infrastructure useless with limited resources. This can be achieved by using existing infrastructures and protocols such as DNS and NTP to create amplification Denial of Services Attacks. DDoS attacks can be mounted against all assets of the SME system that are connected to the internet or even between VMs hosted in the same physical machine.
- **Malware protection**. Whether one thinks of host-based malware, infected removable drives or malicious insiders that want to infect the SME infrastructure and servers, the need of malware protection is of grave importance. The proposed framework needs to provide security features for the core and its end-nodes in order to protect them from the installation and execution of code (or executables) no matter what its origin is, internal or external.
- **Protection of database servers**. Attacks like SQL injection, password cracking and unauthorized access should be detected and prevented by the proposed framework. A strict policy of keeping all systems up-to-date and fully patched should be in place along with clearly distinct roles and access rights for the database servers.
- **Cloud-based and virtualization security** tools are needed to protect the main applications running in the cloud or in Virtual Machines. These tools include detection and prevention of inter- and intra- VM attacks, either DDoS attacks, network attacks, code injection via known or 0-day vulnerabilities.

- Basic **Network Protection tools** that include ACLs, Firewalls, IPSs are needed to deter unauthorized access to the SMEs' assets connected to the OT or IT network.
- **Strong Authorization** and more specifically secure SSH access is essential for all use case SMEs. Remote access for development and administration is mandatory for all enterprises. Thus, strong SSH keys and password need to be in place and attacks against the SSH service need to be detected and logged.
- Most of the use case SMEs may face potential **MiTM** and **repudiation attacks**. These types of attacks need to be addressed and provide counter measures by the proposed framework.

Finally, another common requirement is the protection of Wi-Fi network of the SME. Unauthorized access, password cracking, session hijacking as well as DoS attacks need to be deterred and mitigated

2.3 E-voting Pilot

2.3.1 Scytl Secure Electronic Voting system

Scytl's Online Voting product is a secure solution that enables voters to securely and easily cast their votes from any location and on any device with a stable Internet connection. This solution enfranchises all voters, including remotely located voters, while ensuring privacy and integrity of the results integrity.

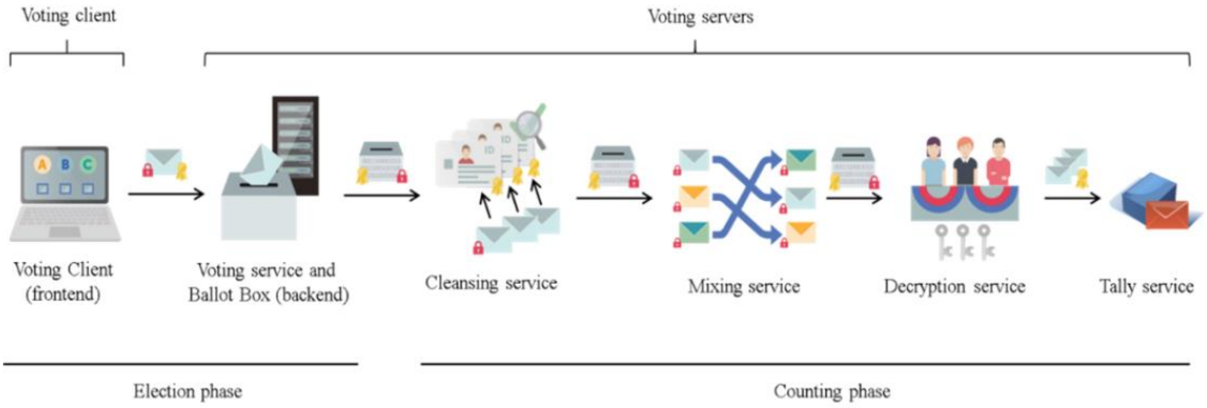


Figure 1. SCYTL pilot: e-Voting architecture

The voting solution also provides the following remarkable features:

- End-to-end encryption: In order to protect the voter privacy also in front of the election servers, the votes are encrypted client-side. Thus, when the vote is received it is already encrypted and the server cannot know the content of the votes. The contents of the votes are not decrypted until the end of the election.
- Mixnet and decryption: In addition to being encrypted in the device of the voters, votes cannot be decrypted until they are anonymized. To do so, a mixing process is used for shuffling and making it impossible to link the mixed vote to the identity of the voter who has cast it. Only when votes are mixed can they be decrypted. To ensure this, the decryption process requires the participation of several members of the electoral board. At the beginning of the election,

the election key that allows the decryption of the votes is divided in shares and stored in smartcards (one for each member). In cryptography, this method is called “secret sharing. Thanks to this, only by gathering together a minimum threshold of the board is it possible to decrypt the individual votes.

- Key roaming: Since voters usually do not have cryptographic keys in their computers or in card identities (or they do not know how to use them), a mechanism called key roaming is implemented. This mechanism provides the voter with a keystore that contains personalized keys to be used to sign the votes. These keystores are protected with a derivation of the voters' credentials.
- Immutable logs: The voting back-office generates immutable logs for all critical operations, i.e. logs that are cryptographically protected against manipulation.

The online voting solution incorporates several modules in order to fulfil all the electoral administrator's and voters' needs, such as the Voting Back-Office web interface and the Voting Portal, the Credential Generation module, the Credential Delivery Back-office web interface and Credential Delivery Portal, and the Receipts Back-Office web interface and Receipts Portal.

2.3.2 List of Requirements

2.3.2.1 Systems and Components Used

The following systems must be protected:

- **Web application servers:** These servers are used to run the server-side voting components. It is important to protect them from several attacks, e.g. Denial of Service (DoS), which would prevent voters from voting in the election; stealing of sensitive information (such as already cast votes or voter keystores, although they are encrypted); or altering the correct functioning of the system (such as disallowing certain voters from voting, disabling secure logs, etc.)
- **Web servers:** These are the servers used to connect the web application servers with the voters. In this case the most common type of attack would be a DoS.
- **Database servers:** These are the servers that maintain the database that contains the information used and generated by the voting system, for example the ballot box or the list of voters. Common attacks could be stealing, destruction or manipulation of the data it contains.
- **Network:** This is the network that is used to communicate the different components of the voting system and the voting system with the voters. Typical attacks could be eavesdropping/sniffing of information and unauthorized access to the system servers through the network.

2.3.2.2 Classification of criticalness

Considering four levels of criticalness, the elements to be protected can be classified as shown here:

- Critical: Web application servers, Database servers
- Severe: Network
- Medium: Web servers

2.3.3 E-voting Pilot Potential Attackers and Threats

Potential internal threats

1) **Ballot stuffing**: an attacker can try to add in the ballot box votes from voters that did not participate in the voting process. The voting channel and the system storing the ballots must prevent the acceptance of votes that have not been cast by their intended voters.
2) **Voter privacy compromise**: an attacker could break voter privacy by linking the voter with his/her voting options and, thereby, breaking vote secrecy. The voting system must ensure that the intent of the voter remains secret during the voting and counting phases.
3) **Vote modification**: vote contents could be modified to change the election results. The voting system must detect any manipulation of valid cast votes.
4) **Vote deletion**: an attacker could try to delete valid votes from the ballot box. The ballot box must be protected against unauthorized changes.
5) **Publication of non-authorized intermediate results**: the intermediate results could be disclosed before the election is closed, influencing those voters that have not yet exercised their right to vote. The voting system has to preserve the secrecy of the cast votes until the tally process to prevent any partial results disclosures.
6) **Inaccurate auditability**: not enough election traceability or easy to tamper with audit data may allow attackers to hide any unauthorized behaviour. The voting channel should provide means to implement an accurate audit process and to detect any manipulation of the audit data.
7) **Unauthorized manipulation of software or data.** An internal or external attacker accessing the servers could be able to manipulate the software which is running the election, or modify directly the data containing the software configuration, electoral roll, the ballot box... The voting servers should guarantee the integrity of their software and stored data, in a way that any manipulation should be detected and alerted.

Potential external threats

1) **Unauthorized voters casting votes**: non-eligible voters could try to cast a vote for a specific election. The voting channel must provide a robust way to remotely identify voters.
2) **Voter impersonation**: a voter or an attacker could try to cast a vote on behalf of another person. The voting channel must provide a robust way to detect any impersonation attempt.
3) **Ballot stuffing**: an attacker could try to add in the ballot box votes from voters that did not participate in the voting process. The voting channel and the environment storing the ballots must prevent the acceptance of votes that have not been cast by their intended voters.
4) **Voter privacy compromise**: an attacker could break voter privacy, linking the voter with his/her voting options and, thereby, breaking vote secrecy. The voting system must ensure that the voter’s intent remains secret during the voting and counting phases.
5) **Vote modification**: vote contents could be modified to change the election results. The voting system must detect any manipulation of valid cast votes.
6) **Vote deletion**: an attacker could try to delete valid votes from the ballot box. The ballot box must be protected against unauthorized changes.
7) **Publication of non-authorized intermediate results**: the intermediate results could be disclosed before the election is closed, influencing those voters that have not yet exercised their right to vote. The voting system has to preserve the secrecy of the cast votes until the tally process to prevent any partial results disclosures.

8) **Voter distrust**: a voter does not have any means for verifying the correct reception and count of his/her vote. Therefore, the voter could have a negative feeling about the voting process. The voting platform must allow the voter to check if the vote has been correctly received at its destination, and if it has been present in the tallying process.

9) **Election boycott/denial of service**: an attacker could disrupt the availability of the voting channel by performing a denial of service attack. The voting platform must detect the eventual congestion of the election services in order to react against them as soon as possible, e.g. by using contingency channels.

10) **Inaccurate auditability**: not enough election traceability or easy to tamper with audit data may allow attackers to hide any unauthorized behaviour. The voting channel should provide means to implement an accurate audit process and to detect any manipulation of the audit data.

11) **Unauthorized manipulation of the voting servers.** An attacker could hack the systems and gain unauthorized access to the servers, compromising their security and being able to manipulate its content. The voting servers should block any hacking attempt, and alert in case of any incident occurs.

12) **Unauthorized manipulation of software or data.** An internal or external attacker accessing the servers could be able to manipulate the software which is running the election, or modify directly the data containing the software configuration, electoral roll, the ballot box... The voting servers should guarantee the integrity of their software and stored data, in a way that any manipulation should be detected and alerted.

13) **Physical unavailability of technological components**. A serious incident against the datacenter containing the servers and network components supporting the infrastructure of the election could make the voting service unavailable. The voting platform should be prepared against unauthorized accesses and vandalism, fire, water-flooding, natural disaster.

Threats and vulnerabilities due to human factor (end-users)

1) **Voter coercion and vote buying**: one person or organization could buy or force a voter to vote for specific voting options. The voting channel must prevent a voter from proving to a third party in an irrefutable way his/her voting intent.

2) **Voter distrust**: a voter does not have any means for verifying the correct reception and count of his/her vote. Therefore, the voter could have a negative feeling about the voting process. The voting platform must allow the voter to check if the vote has been correctly received at its destination, and if it has been present in the tallying process.

Potential attack locations

The following list shows the possible origin locations of attacks:

- Anywhere with an internet connection
- The datacenter where the system is hosted
- The administration network

2.3.4 System Functionality and Resources

Normal behaviour of the current system

Considering a system with the following infrastructure:

- 6 servers
  - FE (Front End) - Apache
  - 2 ME (Middle End) - Tomcat
  - 2 DB (Database) - Oracle
- FW (Firewall)
- Load Balancer
- IDS (Intrusion Detection System)
- Backup system

The system has the following resource usage:

- ME: For each Tomcat 25 MB RAM are needed for concurrent user and a core for each 500 threads (125 users at 4 threads/user)
- FE: 2 MB of RAM for each thread (4 threads/user): 200 users -> 800 thread max -> 1.6 GB -> two servers with 2 cores and 2 GB
- DB: Oracle 11g with 300 DB connections (a portal or *backoffice* (BO) uses use 20 connections maximum by default)

Description of the abnormal behaviour of the system

The size of an election, number of voters and the voting period can highly determine what can be considered a normal or abnormal behavior. However, if there are number of incoming connections to the voting server higher than the number of voters, this could be considered an abnormal behavior. Also, a large number of repeated failed authentication requests could also be mapped to attacks to try to brute force voter credentials.

Software utilities used or needed in the use case

- **Traffic filtering:** To prevent access escalation from vulnerable host to its neighbours, network traffic must be strongly monitored and filtered with ACLs (access control list) for ensuring the internal networks are only accessible from and to trusted connections (source IP, destination IP and port).
- **Network Traffic Monitoring:** All the network traffic events are monitored. All the noticeable logs are sent to the monitoring server for auditing and analysis purposes.
- **VLAN isolation:** To enforce encapsulation of the network traffic, a set of networks is implemented on both environments. Every network is assigned a dedicated and unique IP subnet and VLAN ID.
- **Securing the public access:** To secure the public access towards environments, end users in the public network are only granted connectivity to the Front-End web servers laid in the DMZ (demilitarized zone).
- **SSH access:** UNIX-based command interface and protocol for securely getting access to a remote server/computer**)**
- **Linux system** with capabilities such as, disable root access, SELinux (secure Linux module) etc.
- **OpenScap:** internal system audit tool
- **Zabbix:** open source monitoring solution for network monitoring and application monitoring
- **Splunk:** SIEM, event and log correlator

Hardware components and procedural solutions used in the use case

The electronic voting backoffice can use smartcards to store shares of the election key, thus when the election is finished a number of card holders have to introduce their card to decrypt the votes.

However, this is not an infrastructure level protection. Apart from this, no other specific hardware components are required.

Trust models used in the use case

Password Aging	A minimum of 7 days and maximum of 90 is defined to avoid changes inside the voting periods. Every password change is logged and detected by OSSEC.
Previous password restriction	Any new password has to be the different to the last three passwords that the user had.
Locked user account	Before a user is locked, three failed attempts are allowed

User Account types

- **Infrastructure users**
    - Developers team: every developer user is in the tomcat group and is granted rights to start/stop services and modify tomcat configuration files. They also have access to the database to execute scripts and SQL queries.
    - IT team: users are granted rights to become SuperUsers/administrator user.
- **Administrative users:** All users of the system follow the best practices for strong password policy according to the standards set by the NIST. Every administrator user is nominal.
- **Monitoring users:** To access the monitoring systems (both Splunk's and both Zabbix's), nominal users and personal certificates are required. There are three types of users:
    - Viewer: With read permissions over dashboards and maps
    - Security: Read permissions and creation of alerts and triggers
    - Systems: Read/write permissions.
    - **Database users:** There are the following database users
    - SysDBA users: Administration users with super admin rights
    - Creation Table User: For each application, a different user is created with table creation and deletion capabilities.
    - Application Users: Application user have read/write privileges to the tables inside a schema
    - Read Only Users: Access to the database outside the application is allowed only for read purpose.
    - **Voting back-office users:** Different type of administrators can access the voting back-office at application level using one of the following roles, no end users (voters) can reach it:
    - Superadministrator: The Superadministrator can perform any action on the Online Voting platform management environment and create or edit any type of administration user.
    - Institution administrator: The Institution administrator manages all the Election Events related to the Institution they are assigned to. This user can also create other administrators for his institution, except from Superadministrators and Institution administrators. Note that the Institution administrator cannot restore any Election Events. This action should be performed by a Superadministrator.

- Institution Roll Administrator: The Institution Roll Administrator is responsible for importing and managing the Institution roll before the voting period starts. This administrator can be also responsible for managing activations and authorizations of voters if necessary.
    - Institution Statistics Administrator: The Institution Statistics Administrator can display the participation rate of all Election Events under the Institution assigned.
    - Election Event Roll Administrator: The Election Event Roll Administrator is responsible for importing and managing the Election Event roll, both before and during the voting period. This administrator can be also responsible for managing the authorization of the voters if necessary.
    - Election Event Roll Supervisor: The Election Event Roll Supervisor can take a look at the roll authorized to the Election Event (i.e. look up for a voter to see if he is authorized or has voted), however he cannot make any changes.
    - Election Event Statistics Administrator: The Election Event Statistics Administrator can display the participation rates of all Elections that belong to the Election event assigned.
    - Election Roll Administrator: The Election Roll Administrator can manage the roll of the assigned Election. This user can search through the roll and authorize and de-authorize voters.
    - Web Services Administrator: The Web Services Administrator cannot access the management environment, but can perform the same tasks as the Superadministrator by means of web services.
    - Board member: This user is created when a member of the administration board is willing to perform the Shares Creation and Mixing and Tally ceremonies. It allows the user to follow only the steps of generating the private key and split it into the Electoral Board members, check the configuration of the election and publish it and then after the end of the voting period it also allows of performing the mixing and tally processes.

- **Voting Portal users:** The Voting Portal can be accessed by all the voters using the credentials delivered to them. These users are created off-line by the Credential Generator (the system where the end-user credentials are generated.)

2.3.5 Security Related Systems Used in the Use Case

To prevent access escalation from vulnerable host to its neighbors, network traffic is strongly monitored and filtered with ACLs that ensure the internal networks are only accessible to lawful flows (source IP, destination IP and port).

The following picture depicts the ACL enforcing points within a virtualization farm.

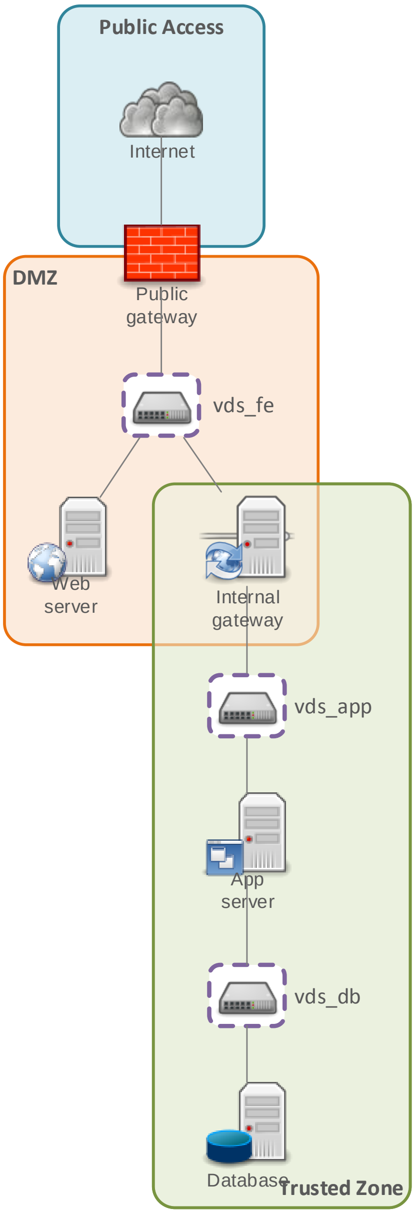


Figure 2. SCYTL pilot: ACL enforcing points

As described in Figure 2, the solution comprises three types of ACL enforcing elements:

- Public gateways: The public gateway exposes 4 downlink interfaces for:
    - The end user public access to the Front-End web servers.
    - The Scytl Offices tunnel towards the Bastion Host.

  Every access implements a dedicated whitelist ACL allowing access to the specific hosts and ports.
- Virtual Distributed Switches (vDS): This is an abstraction exposed by the ESXi farm that allows virtual guests to be logically interconnected to each other, while having the interfaces

associated to one vDS isolated from the others. At this level, it is also possible to define ACLs, so only whitelisted flows are allowed on a per vDS basis.

- Host firewall (FW): Every virtual guest implements its own firewall on the ingress interfaces so only the authorized sources would be allowed to access its local services.
- Physical Switches: As in the virtual distributed switches, ACLs are added in the physical switches to define which flows are allowed.

Security monitoring systems used

- OSSEC [7] or other Intrusion Detection Systems.
- AIDE[8] .
- Linux Audit Daemon.
- Splunk.

Security systems used

- ModSecurity.
- Network firewall.
- Anti-Distributed Denial of Service emergency services (e.g. Incapsula, Akamai, CloudFlare…)

Type of security related information collected

- Application level logs.
- HTTP server logs.
- OSSEC logs.
- Linux Audit Daemon logs.

Emergency protocols used

- **Preparation:** This phase consists on the preparation to be able to handle an incident as soon as it happens. It’s a very important phase because it determines how the incident response team will respond. It is necessary to implement several elements:
    - Policy – Set of principles, rules or practices within the organization. Provides guidance as to whether an incident has occurred in an organization.
    - Response Plan/Strategy – Plan/strategy to handle incidents.
    - Communication – Define whom to contact, when and why.
    - Documentation – Every action taken by the Computer Incidence Response Team (CIRT) should be documented.
    - Team – Made up of several people that consist of different disciplines to handle the various problems that could arise during or from an incident.
    - Access Control – The CIRT must have the permissions necessary to perform their job.
    - Tools – Have available any software or hardware necessary when handling an incident.
    - Training – Essential to be prepared to properly handle incidents.
- **Identification:** This phase consists on the detection of an incident; it requires that events are gathered from the sources available such as SIEM, NSM, alerts, and other resources to determine if an incident has occurred.
    - The CIRT team should be notified and begin to determine the scope of the event and document the evidence found.

- **Containment:** This phase consists on limiting the damage and preventing further damage from happening. The essential steps are:
  - Limit the damage as soon as possible (with short-term actions if necessary).
  - Take a forensic image if a system has been affected
  - Limit further escalation of the incident while allowing normal business operations to continue.
- **Eradication:** This phase consists on removing and restoring the affected systems; taking the necessary steps to remove malicious and other illicit content off of the affected systems. Also, after learning what caused the incident, defences should be improved to ensure that the system cannot be compromised again.
- **Recovery:** This phase consists on bringing affected systems back into the production environment carefully; systems must be tested, monitored and validated before going back to production.
- **Lessons learned:** This phase consists on completing incident documentation which can be also useful for future incidents and as training for new team members. The overall goal is to learn from the incidents that occurred within an organization to improve the team's performance and provide reference materials in the event of a similar incident.

Information exchanged

Described above under section "**Type of security related information collected**".

2.3.6 Security Incidents Handling and Recovery

Categorization

Due to the large variety of possible incidents and their particularities, it is necessary to categorize them. This allows the Incident Response Team to better understand what systems and technologies were involved in generating security events, reporting anomalies or attacks. Also, it is necessary to define specific procedures for most incidents to manage them the best possible way.

Category	Description
Denial of service	Service or information availability affected
Internal Hacking	Hacking attempt from internal sources
External Hacking	Hacking attempt from external sources
Compromised Asset	Known compromise of asset
Abuse of Privileges	Obvious abuse of privileges
Asset Integrity Change	Integrity of service or information
Vulnerability Notification	External notification about vulnerability
Policy Violations	Violations of established policy

Practices used

Depending on the category of the incident a different response practice is used.

Denial of Service

The Denial of Service incidents include situations where a malicious user attempts to make a machine or network resource unavailable to its intended users.

Denial of Service attack on data centre connection

It is produced when the connection of a data centre holding Scytl services is flooded to prevent normal usage or make it unavailable.

Name	Denial of Service attack on data centre connection
Category	Denial of Service
Type	External
Technical indicator	Unusual increase in inbound traffic Unusual increase in HTTP errors
Detection mechanism	NSM alerts and indicators Internal Splunk alerts and indicators OSSEC alerts Notification from data centre technicians
General procedure	1- [IT] Contact with data centre provider and inform about incident 2- [IT] Collect information about the IPs that are carrying out the attack (DoS or DDoS, Origin, Throughput, …) 3- [IT/Data Centre] Secure logs and other evidence 4- [Data Centre] Expand bandwidth to handle peak traffic 5- [Data Centre] Filter attacking IP(s)
Responsible	IT Department
Automated	Partly

Internal Hacking

The Internal Hacking incidents include situations where an attacker is conducting the reconnaissance phase of an attack from inside the internal network.

- **Internal port or service scan detected**

It is produced when multiple services or ports are tested from the internal network to discover all the entry points to a server/host.

Name	Internal port or service scan detected
Category	Internal Hacking
Type	Internal
Technical indicator	Multiple connection attempts from one host or against one host
Detection mechanism	NSM alerts and indicators Internal Splunk alerts and indicators
General procedure	1- [IT] Collect information about the IPs that are carrying out the scan (Origin hosts, Destination hosts, Destination ports, …) 2- [IT] Escalate to Security Director / HR 3- [IT] Monitor activity from the origin hosts detected and block connectivity if attacks begin to take place
Responsible	IT Department
Automated	Partly

- **Internal vulnerability scan / exploitation attempt detected**

It is produced when multiple services or ports are tested from the internal network to discover if they are affected by known vulnerabilities or exploits.

Name	Internal vulnerability scan / exploitation attempt detected
Category	Internal Hacking
Type	Internal
Technical indicator	Multiple malicious attempts from one host or against one host
Detection mechanism	NSM alerts and indicators Internal Splunk alerts and indicators OSSEC alerts
General procedure	1- [IT] Collect information about the IPs that are carrying out the vulnerability scan / exploitation attempt (Origin hosts, Destination hosts, Vulnerabilities, …) 2- [IT] Escalate to Security Director / HR 3- [IT] Block connectivity from Origin hosts 4- [IT] Secure logs and other evidence 5- [IT] Determine the impact of the vulnerability scan / exploitation attempt 6- [IT] Patch all vulnerabilities exposed/detected by the scan
Responsible	IT Department
Automated	Partly

- **Internal Password Brute force attack detected**

It is produced when multiple login attempts are detected in a service or across several services. These attempts can be from one or several internal IPs, against one or several service accounts.

Name	Internal Password Brute force attack detected
Category	Internal Hacking
Type	Internal
Technical indicator	Multiple login attempts on authentication logs The indicators can be found on mail logs, internal services logs, …
Detection mechanism	NSM alerts and indicators Internal Splunk alerts and indicators
General procedure	1- [IT] Collect information about the IPs that are carrying out the brute force attack (Origin IPs, Destination hosts, Services, Users, …) 2- [IT] Escalate to Security Director / HR 3- [IT] Secure logs and other evidence 4- [IT] Include the Origin IPs in the monitoring list for at least the next 24h 5- [IT] Determine the impact of the brute force attack if there are any successful attempts 6- [IT] Change all the passwords that have been successfully brute forced 7- [IT] Correlate the internal IP with other events to detect other attacks made from the same origin 8- [IT] Contact any user whose password has been changed due to the attack
Responsible	IT Department
Automated	Partly

External Hacking

The External Hacking incidents include situations where an attacker is conducting the reconnaissance phase of an attack from outside the internal network.

- **External port or service scan detected**

It is produced when multiple services or ports are tested to discover all the entry points to a server/host. In the external scan the origin of such requests is outside the internal network.

Name	External port or service scan detected
Category	External Hacking
Type	External
Technical indicator	Multiple connection attempts from one host or against one host
Detection	NSM alerts and indicators

mechanism	Internal Splunk alerts and indicators
General procedure	1- [IT] Collect information about the IPs that are carrying out the scan (Origin IPs, Destination hosts, Destination ports, …) 2- [IT] Monitor activity from the origin hosts detected and block connectivity if attacks begin to take place 3- [IT] Include the Origin IPs in the monitoring list for at least the next 24h 4- [IT] Correlate the Origin IPs with other events to detect all attempts made
Responsible	IT Department
Automated	Partly

- **External vulnerability scan / exploitation attempt detected**

It is produced when multiple services or ports are tested from outside the internal network to discover if they are affected by known vulnerabilities or exploits.

Name	External vulnerability scan / exploitation attempt detected
Category	External Hacking
Type	External
Technical indicator	Multiple malicious attempts from one host or against one host
Detection mechanism	NSM alerts and indicators Internal Splunk alerts and indicators OSSEC alerts
General procedure	1- [IT] Filter attacking IP(s) 2- [IT] Collect information about the IPs that are carrying out the vulnerability scan / exploitation attempt (Origin IPs, Destination hosts, Vulnerabilities, …) 3- [IT] Include the Origin IPs in the monitoring list for at least the next 24h 4- [IT] Secure logs and other evidence 5- [IT] Determine the impact of the vulnerability scan / exploitation attempt 6- [IT] Patch all vulnerabilities exposed/detected by the scan 7- [IT] Correlate the Origin IPs with other events to detect all attempts made
Responsible	IT Department
Automated	Partly

- **External Password Brute force attack detected**

It is produced when multiple login attempts are detected in a service or across several services. These attempts can be from one or several external IPs, against one or several service accounts.

Name	External Password Brute force attack detected

Category	External Hacking
Type	External
Technical indicator	Multiple login attempts on authentication logs The indicators can be found on mail logs, external services logs, …
Detection mechanism	NSM alerts and indicators Internal Splunk alerts and indicators
General procedure	1- [IT] Filter attacking IP(s) 2- [IT] Collect information about the IPs that are carrying out the brute force attack (Origin IPs, Destination hosts, Services, Users, …) 3- [IT] Include the Origin IPs in the monitoring list for at least the next 24h 4- [IT] Secure logs and other evidence 5- [IT] Determine the impact of the brute force attack if there are any successful attempts 6- [IT] Change all the passwords that have been successfully brute forced 7- [IT] Correlate the Origin IPs with other events to detect other attacks made from the same origin 8- [IT] Contact any user whose password has been changed due to the attack
Responsible	IT Department
Automated	Partly

Compromised Asset

The Compromised Asset incidents include situations where a company asset becomes endangered due to an attack, a security breach, etc. Once it has been confirmed, all connections and activity from that asset must be considered suspicious and analyzed in depth.

- **Command execution detected**

It is produced when unauthorized or malicious commands are executed on a monitored server.

Name	Command execution detected
Category	Compromised Asset
Type	Internal
Technical indicator	Unauthorized command executed Unusual/Malicious command detected
Detection mechanism	NSM alerts and indicators Internal Splunk alerts and indicators OSSEC alerts
General procedure	1- [IT] Collect information about the commands executed from the affected host before and after the alert

	2- [IT] Monitor activity from the origin host and block connectivity if attacks or pivoting actions begin to take place 3- [IT] Perform memory dump 4- [IT] Check active processes, inbound and outbound connections and user activity 5- [IT] Secure logs and other evidence 6- [IT] Determine if the actions were done by an external attacker or an employee 7- [IT] Determine point of origin 8- [IT] Correlate the origin with other events to detect all attempts made
Responsible	IT Department
Automated	Partly

- **Infrastructure compromised**

It is produced when a company asset is jeopardized by an external attacker or a malicious user.

Name	Infrastructure compromised
Category	Compromised Asset
Type	Internal
Technical indicator	Connections to malicious IPs Unusual increase in outbound traffic Unauthorized configuration modification Unusual connection attempts against other internal servers Unauthorized command executed Privileged actions from an unauthorized user Suspicious actions from a privileged user Unusual increase in outbound traffic
Detection mechanism	NSM alerts and indicators Internal Splunk alerts and indicators OSSEC alerts Employee/Contributor contacts Security Department
General procedure	1- [IT] Isolate machine to dedicated quarantine network 2- [IT] Perform memory dump 3- [IT] Check processes, network connections, new files created, user activity … 4- [IT] Drill-down first occurrence and scope of the incident checking system, firewall, IPS and network logs 5- [IT] Perform computer forensic process to recover data or evidence deleted by the attacker 6- [IT] Correlate with other events to detect all actions made 7- [IT] Determine the impact on the infrastructure and all the assets affected 8- [IT] Secure logs and other evidence 9- [IT] Determine the impact on the server's service and inform users if necessary

	10- [IT] Restore a backup prior to the asset being compromised 11- [IT] Apply patches and/or implement necessary measures to avoid another breach 12- [IT] Return asset to its appropriate network
Responsible	IT Department
Automated	Partly

- **Suspicious outbound traffic from server**

It is produced when unauthorized or suspicious connections are opened on a monitored server.

Name	Suspicious outbound traffic from server
Category	Compromised Asset
Type	Internal
Technical indicator	Connections to malicious IPs Unusual increase in outbound traffic
Detection mechanism	NSM alerts and indicators Internal Splunk alerts and indicators
General procedure	1- [IT] Capture the traffic from the affected host (full packet capture) 2- [IT] Isolate machine to dedicated quarantine network 3- [IT] Perform memory dump 4- [IT] Check processes, network connections, new files created, user activity … 5- [IT] Drill-down first occurrence and scope of the incident checking system, firewall, IPS and network logs 6- [IT] Secure logs and other evidence 7a- [IT] If the analysis clearly shows a compromised asset apply procedure **Infrastructure compromised** from step 5 7b- [IT] If not, determine the impact on the server’s service and inform users if necessary 8- [IT] Correlate with other events to detect all actions made 9- [IT] Apply patches and/or implement necessary measures to avoid malicious traffic 10- [IT] Return server to its appropriate network
Responsible	IT Department
Automated	Partly

- **Suspicious outbound traffic from workstation**

It is produced when unauthorized or suspicious connections are opened on a workstation.

Name	Suspicious outbound traffic from workstation
Category	Compromised Asset
Type	Internal

Technical indicator	Connections to malicious IPs Unusual increase in outbound traffic
Detection mechanism	NSM alerts and indicators Internal Splunk alerts and indicators
General procedure	1- [IT] Capture the traffic from the affected host (full packet capture) 2- [IT] Isolate machine to dedicated quarantine network 3- [IT] Perform memory dump 4- [IT] Identify and notify workstation owner 5- [IT] Check processes, network connections, new files created, user activity … 6- [IT] Drill-down first occurrence and scope of the incident checking system, firewall, IPS and network logs 7- [IT] Secure logs and other evidence 8a- [IT] If the analysis shows a relation with known malware apply procedure **Infected workstation** 8b- [IT] If the analysis clearly shows a compromised asset apply procedure **Infrastructure compromised** from step 5 8c- [IT] If not, determine the impact on the server's service and inform users if necessary 9- [IT] Correlate with other events to detect all actions made 10- [IT] Apply patches and/or implement necessary measures to avoid malicious traffic 11- [IT] Return workstation to its appropriate network
Responsible	IT Department
Automated	Partly

Abuse of Privileges

The Abuse of Privileges incidents include situations where an employee misuses his account permissions with malicious intent.

- **Massive internal data harvesting - source code / files**

It is produced when an employee tries to gather as much company information/data/knowledge as possible with malicious intent and/or illegally.

Name	Massive internal data harvesting - source code / files
Category	Abuse of Privileges
Type	Internal
Technical indicator	Unusual high amount of connections to a service/repository Unusual throughput of network traffic detected on a device
Detection mechanism	NSM alerts and indicators Internal Splunk alerts and indicators

General procedure	1- [IT] Capture the traffic from the affected host (full packet capture) 2- [IT] Collect information about the connections from the host that is carrying out the harvesting (Origin, Destination hosts, Services, Users, Resources, …) 3- [IT] Secure logs and other evidence 4- [IT] Escalate to Security Director, HR and his direct supervisor 5- [IT] Include the origin IPs in the monitoring list for at least the next 24h 6- [IT] Impound the device used for the information gathering 7- [IT] Isolate machine to dedicated quarantine network 8- [IT] Determine the data harvested and remove it from the impounded machine 9- [IT] Determine if any data has already been sent outside Scytl premises 10- [IT] Correlate the internal IP with other events to detect other actions done from the same origin
Responsible	IT Department
Automated	Partly

- **Escalation of privileges attempted by user / abuse of Admin account**

It is produced when an unauthorized escalation of privileges is attempted by a non-privileged user, or when a user with an admin account misuses it.

Name	Escalation of privileges attempted by user / abuse of Admin account
Category	Abuse of Privileges
Type	Internal
Technical indicator	Privileged actions from an unauthorized user Suspicious actions from a privileged user
Detection mechanism	Internal Splunk alerts and indicators OSSEC alerts
General procedure	1- [IT] Capture the traffic from the affected host (full packet capture) 2- [IT] Collect information/activity of the service account which has been abused 3- [IT] Secure logs and other evidence 4- [IT] Escalate to Security Director, HR and his direct supervisor 5a- [IT] If there has been a successful escalation of privileges, in case of a vulnerability/breach fix it, and in case of password guessing change the password for a more robust one 5b- [IT] If there has been an abuse of an admin account, revoke privileges in case of nominal account, or change password in case of shared account 6- [IT] Determine impact of the abuse 7- [IT] Restore service to a prior backup if there have been configuration changes produced by the malicious user
Responsible	IT Department

Automated	Partly

Asset Integrity Change

The Asset Integrity Change incidents include situations where uncontrolled changes are produced either in services or files.

- **Unexpected integrity change detected**

It is produced when a network configuration change, which is not controlled, is produced.

Name	Unexpected integrity change detected
Category	Asset Integrity Change
Type	Internal
Technical indicator	Detection of integrity change
Detection mechanism	OSSEC alerts
General procedure	1- [IT] Verify if it was a controlled change 2- [IT] Understand impact of change 3- [IT] Understand source of change 4- [IT] Drill-down data from other sources (NSM, Splunk, logs) 5a- [IT] If the server has been compromised apply procedure **Infrastructure compromised** 5b- [IT] Analyze if more changes were made in the server 6- [IT] Restore the modified files from a backup 7- [IT] Secure logs and other evidence 8- [IT] Notify Security Director
Responsible	IT Department
Automated	Partly

Vulnerability Notification

The Vulnerability Notification incidents include situations where people outside the company discover and notify existing vulnerabilities in our services.

- **External notification about vulnerability in system**

It is produced when an external user contacts the company about a vulnerability they have discovered in our systems, an unavailable service, a defaced web page...

Name	External notification about vulnerability in system
Category	Vulnerability notification

Type	Internal
Technical indicator	External source (e.g. researcher, customer)
Detection mechanism	Contributors or customers contact Security Department Contributors or customers contact Scytl employee and they forward the notification to Security Department
General procedure	1- [IT] Thank the external source for the notification 2- [IT] Verify the vulnerability notified 3- [IT] Patch the vulnerability and/or implement necessary measures to avoid exploitation from a malicious user 4- [IT] Analyze when the vulnerability was introduced and drill-down to determine if it was exploited at any point; checking system, firewall, IPS and network logs 5a- [IT] If any server has been compromised apply procedure **Infrastructure compromised** 5b- [IT] Analyze if other services are affected by the same vulnerability 6- [IT] Patch the vulnerability and/or implement necessary measures in all affected servers 7- [IT] Thank again the external source for the notification, explaining that the vulnerability has been fixed 8- [IT] Secure logs and other evidence 9- [IT] Determine the impact on the server's service and inform users if necessary 10- [IT] Notify Security Director
Responsible	IT Department
Automated	Partly

Policy Violations

The Policy Violation incidents include situations where employees don't follow the Security policies defined and that pose a high risk to corporate data.

- **Weak password detected on device**

It is produced when the Password Policy regarding password strength is not followed on a device. This device can be, among others, a workstation, a server, or a network device; and the password can be deemed weak by the factors described in the policy.

Name	Weak password detected on device
Category	Policy Violations
Type	Internal/External
Technical indicator	Default password

	Password in dictionary list Password in most common passwords list
Detection mechanism	Periodic passwords scans Internal documentation
General procedure	1- [Security] Verify with account owner 2- [Security] Change password 3- [Security] Check access level of account (impact) 4- [Security] In case of high impact check for unusual authentications either in Splunk or, if it has not been integrated, in the affected device logs. 5- [IT] If unusual authentications are detected apply procedure **Successful unauthorized or suspicious access to account** 6- [Security] Send employee reminder mail about Security Policies
Responsible	Security and IT Department
Automated	Yes

- **Password storage/sharing detected**

It is produced when the Password Policy [Name of document] regarding password storage/sharing is not followed; for example, by storing/sharing passwords in plaintext, by using HTTP Basic authentication, by leaving passwords in documentation...

Name	Password storage/sharing detected
Category	Policy Violations
Type	Internal/External
Technical indicator	Corporate passwords published in internal services Plaintext passwords in services
Detection mechanism	Periodic searches in internal services Internal documentation Visual detection NSM alerts and indicators Internal Splunk alerts and indicators
General procedure	1- [Security] Verify with account owner 2- [Security] Check with owner if password is valid or not 3- [IT] Change password 4- [Security] Check Access level of account (impact) 5- [Security] In case of high impact check for unusual authentications either in Splunk or if it has not been integrated in the affected device logs. 6- [IT] If unusual authentications are detected apply procedure **Successful unauthorized or suspicious access to account**

	7- [Security] Send employee reminder mail about Security Policies
Splunk alert procedure	1- [Security] Gather in Splunk all the user/password tuples detected due to appearance of passwords in application log files, as GET parameters, in error messages, ... 2- [Security] Drill-down first occurrence of the incident 3- [Security] Apply General procedure 4- [IT] Modify the application affected so that passwords don't appear in logs, parameters, errors, …
NSM alert procedure	1- [Security] Gather in NSM all the user/password tuples detected due to appearance of passwords in Basic authentication, as GET parameters, in error messages, ... 2- [Security] Drill-down first occurrence of the incident 3- [Security] Apply **General procedure** 4- [IT] Modify the application affected so that passwords don't appear in logs, parameters, errors, …
Responsible	Security and IT Department
Automated	Not yet. The periodic searches in internal services and the Splunk alerts have to be defined.

- **Destruction of corporate data**

It is produced when the Data Security Policy [Name of document] regarding protection of corporate data is not followed; for example, by destroying corporate data without authorization.

Name	Destruction of corporate data
Category	Policy Violations
Type	Internal
Technical indicator	Disappearance of monitored files Detection of delete method requests Unauthorized deletion/decommission of a server
Detection mechanism	NSM alerts and indicators Internal Splunk alerts and indicators OSSEC alerts Employee contacts Security Department
General procedure	1- [Security] Perform analysis and determine scope of the destruction 2- [Security] Escalate to Security Director 3- [IT] Stop/Pause destruction process 4- [IT] Isolate device 5- [Security] Communicate with owner of information 6- [Security] Try to determine if the destruction was involuntary, intentional or the device was compromised 7- [Security] If the device has been compromised apply procedure **Infrastructure**

	compromised 8- [IT] Restore information from backup 9- [IT] Return workstation to its appropriate network 10- [Security] Send employee reminder mail about Security Policies
Splunk alert procedure	1- [Security] Gather in Splunk all the files being deleted either by delete requests, disappearance of files monitored with OSSEC or auditd logs showing formatting events 2- [Security] Drill-down first occurrence of the incident and scope of the destruction 3- [Security] Apply **General procedure from step 2**
NSM alert procedure	1- [Security] Gather in NSM all the files being deleted by delete requests 2- [Security] Drill-down first occurrence of the incident and scope of the destruction 3- [Security] Apply **General procedure from step 2**
Responsible	Security and IT Department
Automated	Not yet. The Splunk alerts have to be defined.

Other security guidelines used

N/A

Recovery processes

The correct assessment of a critical situation is the first and most crucial stage of the disaster recovery process, and will lead to a decision whether a disaster situation has occurred or not. If so, a recovery strategy will be invoked. In summary, the identification and assessment processes will involve the following stages (which are described in more detail in the following subsections):

- **Identify** a potential disaster situation.
- **Conduct** an initial assessment of the situation to determine if it should be considered a major incident or a disaster situation.
- **Handle** the major incident.
- **Escalate** the disaster situation.
- **Mobilize** a disaster recovery team.
- **Conduct** full assessment.

Although the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) are dependent on the project and Service Level Agreement (SLA), an example of possible parameters is:

- Recovery Point Objective: Less than five minutes
- Recovery Time Objective Less than one hour

2.3.7 Data Protection and Recovery

Type of data kept

The following data is kept by the electronic voting system in the database:

- Ballot box: contains all the votes cast

- Electoral roll: list of voters that are authorized to vote for a given election

Data storage solutions used

A database is used to maintain the information.

- **Oracle RAC database servers**

Number of devices	Model	CPU	RAM	HD	Ethernet
2	HP DL360 G9	1x8 cores	64GB	2x300GB SAS 10k	2xDual Quad Ports 1Gbps

- **Virtualization Farm**

Number of devices	Model	CPU	RAM	HD	Ethernet
3	HP DL360 G9	2x8 cores	64GB	2x300GB SAS 10k	2xDual Quad Ports 1Gbps

- **Storage Array**

Number of devices	Model	HD	Ethernet
1	NetApp FAS2650HA	12x900GB SAS 10k	1/10 Gbps Ethernet Ports

Data Replication features (Snapshot and Snapmirror)

Storage disaster and recovery practices

Described in Section 2.3.6 (Security Incidents Handling and Recovery)

2.4 Smart City Pilot

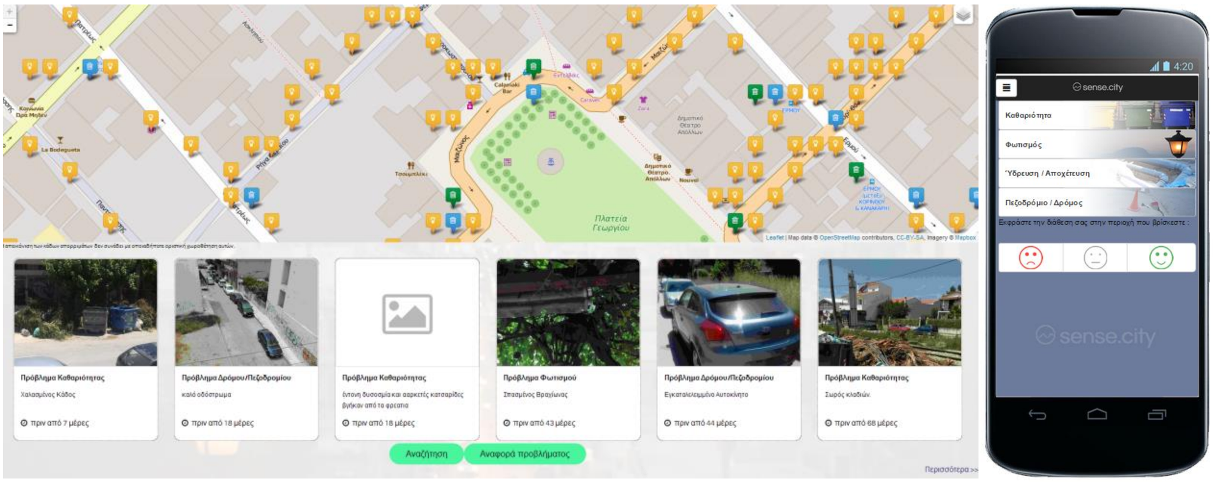
2.4.1 Sense.City Platform

The Sense.City platform (http://sense.city) provides tools to citizens to activate their creativity, design and communication. It also engages them into becoming more active towards a participatory society and democracy while it facilitates interactions and synergies with city authorities and public services. By using the Sense.City platform, citizens become the city sensors and the actual voice of the city itself! With their own communication devices (mobile phones) or via the Sense.City web application, citizens can post in real time issues and problems for something that happens in their city, inform their fellow citizens and the municipality for problems and incidents that occur every moment. The main features of Sense.City are:

- **What is happening in the city:** Citizens are the city sensors! Using own communication devices, through the Sense.City mobile application they update their fellow citizens and the municipality of problems and incidents that occur every moment.
- **Urban participation:** Actively participate in the processes and solve problems concerning your life in the city. Help in urban development and better relationship between citizens and administration services of the city.

- **Co-creativity:** The Sense.City platform provides the tools to enable citizens, and calls for collective thinking and actions both citizens and administration services.

The service is offered through a mobile application and a web application. In a nutshell, the mobile app is mainly used to report errors to a public administration, while the web app can be used for reporting problems, for overviewing information over one or more cities, and finally for accessing the administrator’s page where public servants can see, and address reported issues for their municipality (issue management backend). Figure 3 depicts the mobile and web application of Sense.City.



Πρόβλημα Καθαριότητας
Χαλασμένος Κάδος
πριν από 7 μέρες

Πρόβλημα Δρόμου/Πεζοδρομίου
καλό οδόστρωμα
πριν από 18 μέρες

Πρόβλημα Καθαριότητας
έντονη δυσοσμία και αρκετές κατσαρίδες βγήκαν από τα φρεατια
πριν από 18 μέρες

Πρόβλημα Φωτισμού
Σπασμένος Βραχίωνας
πριν από 43 μέρες

Πρόβλημα Δρόμου/Πεζοδρομίου
Εγκαταλελειμμένο Αυτοκίνητο
πριν από 44 μέρες

Πρόβλημα Καθαριότητας
Σωρός κλαδιών.
πριν από 68 μέρες

Εκφράστε την διάθεση σας στην περιοχή που βρίσκεστε :

Figure 3. Sense.City web and mobile applications

Sense.City overall architecture and interconnection of services.

Figure 4 displays the Sense.City overall architecture and connected services. Sense.City API is implemented in Node.js and the persistence is accomplished by a MongoDB server. The issue management is supported by Bugzilla [10], a well-known open source issue management system. Citizens and public authorities are notified of issues by emails and short messages to their mobile phones. Sense.City analytics are supported by an ElasticSearch [11] cluster. All services are virtualized and hosted in an OpenStack private cloud installation.

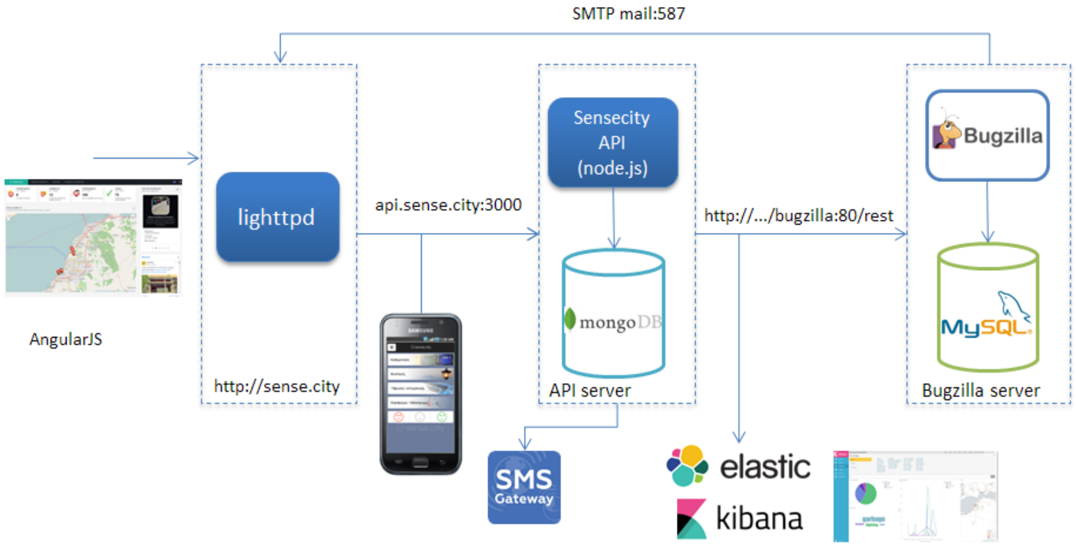


Figure 4. Sense.City Architecture

The platform is scalable and can be easily adopted by other cities. Multiple cities are supported under different domains: e.g. *http://patras.Sense.City*, *http://zakynthos.Sense.City*, etc. City geo-fencing allows us to propagate the issue to the backend management, for the equivalent city and public service. Fixed data location (i.e. lightning posts, garbage bins locations) allows us to approximately identify where the problem is and help the public services.

The platform covers and tracks the full lifecycle of an issue. That is, from the moment it was first reported, keep track of all city assignments as well as any reactions/responses from/to authorities and citizens. For this, the platform has also a backend system for public authorities to monitor and manage issues reported in the city, as well as search, respond to citizens and analyze them.

The web server of the application is running on lighttpd web server on a public IP. The services being used by the application except for the SMS service, which is a third-party service, are running on the virtual infrastructure created by OpenStack. At the compute nodes (Figure 5) two virtual machines have been deployed: one for hosting the Sense.City API service and a mongodb database and one for hosting the Bugzilla application. Both VMs have Public IPs attached. Sense.City API accepts https requests from a) the web server application, b) the Sense.City mobile application and c) other 3rd parties. This API communicates with bugzilla and mongodb in order to return the response to each request. It is also connected with an SMS third party service which is running on the endpoint (*https://api.theansr.com/v1/sms*). Sense.City API and SMS service are based on RESTFUL API logic. Finally, in terms of resources being used by the virtual machines, the virtual machine of Sense.City API is currently using 2 vCPUs, 40GB of disk space and 4GB of RAM. On the other hand, Bugzilla virtual machine is using 2 vCPUs, 40GB of disk space and 8GB of RAM.

Sense.City Private Cloud

The infrastructure where OpenStack and some parts of Sense.City are running on are depicted in Figure 5:

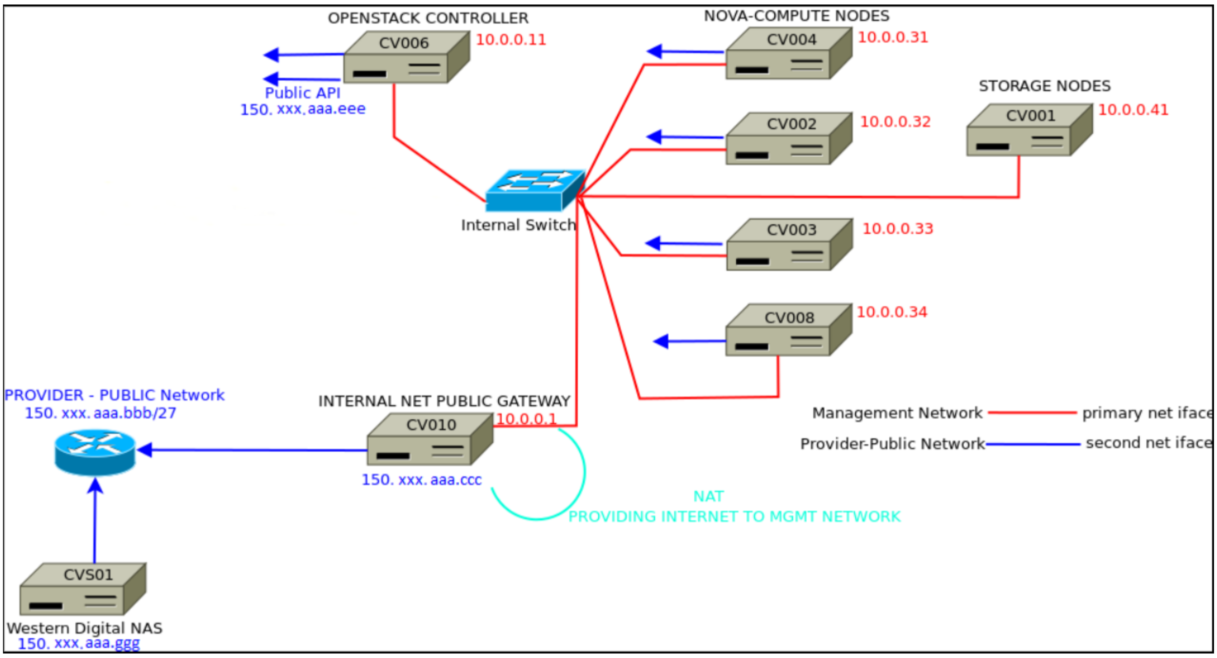


Figure 5. Sense.City network components

The OpenStack controller where the orchestration of the virtual infrastructure and networking is taking place, through the backend services provided by OpenStack software, is residing on the physical node CV006. The two main backend services of the controller are the nova-api and the neutron-api. Nova-api is responsible for the virtual infrastructure of OpenStack. On the other hand, neutron-api handles networking of the virtual infrastructure by using an L3 agent, a DHCP agent and finally an L2 agent.

The virtual infrastructure of OpenStack is running on physical nodes CV002, CV003, CV004 and CV008. Those nodes are called compute nodes in OpenStack terminology. Each one of those nodes has two network interfaces: one for the internal communication of the machines and the vxlan implementation, and one for the floating IPs. Floating IPs are public IPs assigned by the OpenStack controller to virtual machines so that they can be publicly accessible through the provider network 150.xxx.aaa.bbb/27[1]. The default gateway of the network is 150.xxx.aaa.ccc. Finally, floating IPs are based on SNAT. Similar with OpenStack controller node, all compute nodes are running two main services: nova and neutron agents. Those services are communicating with OpenStack controller nova-api and neutron-api services in order to implement the overlay network. Nova-api service moves around the virtual machines on the physical infrastructure depending on their resources needs.

Regarding the storage resources, Sense.City infrastructure utilizes the cinder service of OpenStack. Cinder service is a way to create volumes and attach them to the virtual machines running dynamically on the compute nodes. In order to backup Sense.City data, a NAS device is used on CVS01. In the future, it is planned to use the storage node of OpenStack infrastructure which is the machine CV001 to store the data as objects through the swift service of OpenStack.

Sense.City current OpenStack version is Newton (14.0.1). The controller and the nova compute nodes are running on Ubuntu 16.04.2 LTS. Moreover, each virtual machine hosting Sense.City services is

[1] Addresses obfuscated for protection.

running on ubuntu server 16.04 image which uses QCOW2 format and the container format of that image is bare. Finally, its size is 310 MB. It is important to mention that the web server (lighttpd [9]) of Sense.City application is running on a separate machine 150.xxx.aaa.ddd which is not shown up on Figure 5.

2.4.2 List of Requirements

2.4.2.1 Systems and Components Used

Alias	**Description**
OSCONTROLLER (Figure 5, CV006)	Sense.City OpenStack infrastructure is open to the public internet. That is, the OpenStack Controller is accessible since one NIC is connected to the University of Patras core network.
OSNODE (Figure 5, CV002-4, CV008)	Each node is accessible since one NIC is connected to the University of Patras core network.
NAMHOST (Figure 4)	The Web Server (bare metal) which hosts Sense.City frontend
LIGHTTPD (Figure 4)	The lighttpd server (located at NAMHOST) which hosts other websites along with the Sense.City frontend
SCWEB (Figure 4)	The front-end web application
NAMMS (Figure 4)	The mail server (NAMMS) hosted together with the Sense.City Web Server (NAMHOST)
SCAPIHOST (Figure 4)	The Sense.City API server (Virtual Machine)
SCAPI (Figure 4)	The Sense.City API service
SCAPIMDB	The API service MongoDB

(Figure 4)	
BUGZILLAHOST (Figure 4)	The server that hosts the Bugzilla service (Virtual Machine)
BUGZILLA (Figure 4)	The bugzilla service hosted on Apache
BUGZILLADB (Figure 4)	The MySQL server hosted at BUGZILLAHOST

Table 1. Sense.City systems and services

2.4.2.2 Classification of Criticalness

Alias	Criticality	Description
OSCONTROLLER	HIGH	All infrastructure is managed through this.
OSNODE	HIGH	Many VMs are hosted on top of this.
NAMHOST	HIGH	It hosts the main frontend website.
LIGHTTPD	HIGH	It hosts the main frontend website but also hosts other websites.
SCWEB	HIGH	This is the main front end component of the system where all users also login to the system.
NAMMS	MEDIUM	If this component is compromised an attacker can send spam emails or block our email service.
SCAPIHOST	HIGH	This component is critical since it hosts the main API service.
SCAPI	HIGH	This component is critical since it services the main API.
SCAPIMDB	LOW	The main DB of Sense.City. We consider the risk low, since this component is not directly exposed to the

		public.
BUGZILLAHOST	MEDIUM	It hosts the main Bugzilla service.
BUGZILLA	MEDIUM	It provides the Bugzilla features.
BUGZILLADB	LOW	This is the main DB for reported issues management and tracking. We consider the risk low, since this component is not directly exposed to the public.

Table 2. Criticality classification of the components of Sense.City

2.4.3 Smart City Pilot Potential Attackers, Threats

Potential internal threats

- The shared host of web applications can be an issue. If another web application on the same server is compromised, then also Sense.City SCWEB service can be compromised.
- The NAMMS accepts only connection from localhost. However, if another hosted website is compromised, then it can use this server for sending spam, also making the service unable to send emails and notifications to Sense.City users.
- Although all services are hosted on a private cloud Sense.City may encounter attacks from other machines in the network (lab network and university network).
- Emails and mobile phones of end-users are stored unencrypted in the database.
- Unauthorized manipulation of running services or data and any manipulation should be detected and alerted**.** An internal or external attacker accessing the servers could be able to manipulate the services or modify directly the data containing the software configuration. All servers should guarantee the integrity of installed services and stored data.

Potential external threats

- Generic DoS attacks to all services
- Attacks to SCAPI to break the service.
- Attacks to SCAPI to get user personal data (emails, passwords mobile phones).
- Unauthorized users start reporting issues to SPAM the service and cause the city operations to be loaded with garbage data.
- Unauthorized users getting access by acting as city authorities starting manipulation city issue data in malicious ways.
- Incidents against the datacenter and network services.

Threats and vulnerabilities due to human factor (end-users)

- Fake but authorized users start to post false issues.
- User from the city authorities gets access to citizen data (emails, mobile phones).

- Malicious insider (e.g. developer) manipulating or destroying data.
- Malicious insider (e.g. developer) attacking (even involuntarily) the system.

Potential attack locations

- Sense.City physical infrastructure (private cloud) via internet.
- Sense.City service and listening ports via internet.

2.4.4 System Functionality and Resources

What is the system normal behavior

- Currently there are around 50 -100 visitors per day, and 5-10 city issues per day.
- CPU usage is below 10% for all services, memory for API is less than 500Mb and for Bugzilla is less that 1Gb

What is the system abnormal behavior

- More than 10 issues reported per minute for a certain city is considered to be an abnormal behavior.

Software utilities used or need to be used in the use case

- Prometheus is used to monitor the infrastructure, the services, and receive alerts for high CPU and network usage.
- It would be desirable to use services that monitor the infrastructure for DDoS attacks or unauthorized data manipulation.

Hardware components and procedural solutions used or need to be used in the use case

- There are no hardware components installed.
- All servers are accessible only via SSH.
- Web access and APIs are under HTTPS.

Trust models used or need to be used in the use case

The following list depicts the access rights that the different Sense.City actors have on the service components.

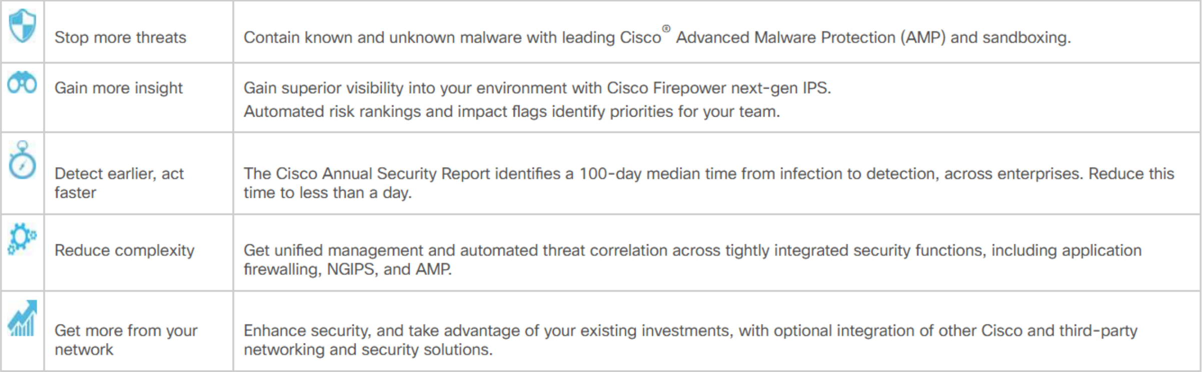
- The development team has access to the private cloud Sense.City project and can manage the Sense.City infrastructure.
- Developer has access to NAMHOST web server to update the SCWEB service.
- Developer has access to SCAPIHOST to update the SCAPI service.
- Developer has access to BUGZILLAHOST to update the BUGZILLA service.
- Subscribed citizens have access to view their issues.
- Subscribed user from city authorities can admin city issues.

The only defined trust model for user access is:

Locked user account	Before a user is locked, three failed attempts are allowed

2.4.5 Security Related Systems Used or In Need in the Use Case

In general, the service is behind the University of Patras firewall. This firewall is Cisco Firepower 4100 Series, a fully integrated next-generation firewall (NGFW) appliance. Its main features are depicted in the following Figure 6



Stop more threats	Contain known and unknown malware with leading Cisco® Advanced Malware Protection (AMP) and sandboxing.
Gain more insight	Gain superior visibility into your environment with Cisco Firepower next-gen IPS. Automated risk rankings and impact flags identify priorities for your team.
Detect earlier, act faster	The Cisco Annual Security Report identifies a 100-day median time from infection to detection, across enterprises. Reduce this time to less than a day.
Reduce complexity	Get unified management and automated threat correlation across tightly integrated security functions, including application firewalling, NGIPS, and AMP.
Get more from your network	Enhance security, and take advantage of your existing investments, with optional integration of other Cisco and third-party networking and security solutions.

Figure 6. Cisco Firepower® NGFW (next-generation firewall)

Security monitoring systems used

Sense.city is using use three monitoring services for the physical infrastructure: Graphana, Prometheus and Alert Manager. Each of them listening to end-points of the system. More specifically:

- Graphana is used to monitor the usage of the node resources on the physical infrastructure.
- Prometheus is being used to set alert rules, which inform the administrators of the infrastructure in case of some thresholds of infrastructure nodes resources have been exceeded. In order to check those resources, the *node_exporter* script runs on all the infrastructure nodes that are of interest. This script exposes software and hardware metrics to the Prometheus server running on the <internal_gateway> (Figure 5) machine to check if some of the current rules being set is broken.
- The Alert Manager handles the events created by Prometheus by sending an email to the administrators.

Security systems used

- The University firewall blocks attacks to known ports (e.g. port 80).
- Fail2Ban [12] installed to detect failed login attempts.

Type of security related information collected

Fail2Ban gathers blocked IP addresses with at least 3 failed login attempts.

Emergency protocols used

There are no emergency protocols used.

Information exchanged

N/A

2.4.6 Security Incidents Handling and Recovery

The following issues are so far in scope:

- Unauthorized usage.
- Failed SSH login attempts to any system.
- High traffic or High CPU usage.

Security Related Practices used

- Capture the traffic or CPU usage from the affected host.
- Collect information about the connections.
- Capture logs and other evidence.
- Escalate to direct supervisor.
- Always update critical software to latest version.

Other security guidelines used

N/A

Recovery processes

- Attempt to shut down malicious processes and connections
- Spin up a new clean VM in pace of the old service and recover data from last backup

2.4.7 Data Protection and Recovery

Data storage solutions used

- Databases used: MongoDB and MySQL.
- Configuration files.

Data storage technologies used

- OpenStack Swift [13] for storage.
- We use a NAS in the datacenter.

Storage disaster and recovery practices

- All servers of Sense.City datacenter are configured with RAID 5.
- There is a weekly backup for every critical service in a NAS.
- There is a daily backup of the BugzillaDB in a NAS.
- Aim for RTO is 3 hours.

2.5 Industrial Services Pilot

2.5.1 WorldSensing Industrial Monitoring System

Worldsensing as industrial IoT pilot partner in the SMESEC project will provide the best use case to test, in a real and practical scenario, the benefits of protecting an IoT environment from cyber attacks at all levels. This is why Worldsensing brings a complete solution composed by sensors, dataloggers, gateways and a software platform based on cloud that represent a real scenario with a great variety of devices and software that add complexity and diversity of threats. Finally, the scenario will demonstrate how SMESEC can help in supporting a SME and its users by protecting and increasing awareness of cybersecurity for users, systems and citizens of the smart cities.

Use Case and details

The use case that WorldSensing (WOS) is proposing within SMESEC project is a **smart infrastructure monitoring** for smart cities with emergency management for construction site using LoadSensing product.

Loadsensing is a wireless data acquisition and monitoring system which combines state-of-the-art wireless monitoring and advanced software tools. It is widely recognized as the leading solution for connecting and monitoring infrastructures in remote locations.

Loadsensing devices are battery-powered and are equipped with long-range, low-power wide area network (LPWA) radio communications and are compatible with the majority of the geotechnical sensors commonly used. The software suite is web-based and facilitates real-time data capture and analytics. It is also possible to set automatic alarms to make operations safer.

Mining and construction companies and operators of bridges, tunnels, dams, railways and many other inaccessible assets can now work with reliable data. Having remote access to this information and real-time insights enables operators to anticipate needs, manage their workforce, diminish risks and even prevent disasters.

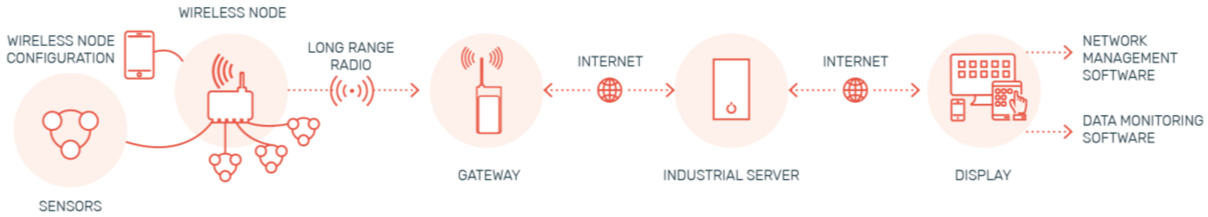


Figure 7. Worldsensing overview architecture

Loadsensing LS-G6 [14], from Worldsensing, is a network system of dataloggers (nodes) that takes sensor readings and connect them to internet. The nodes are energetically autonomous, they power the sensors and collect the data readouts at a sampling rate previously set on the configuration of the device (e.g. once a day, once an hour, etc.). Loadsensing is specifically designed to monitor structural parameters such as vibration and angles of inclination (tilt) in buildings and civil works. The nodes are easily configured on site by using only a cell phone and the app developed by Worldsensing (Dlog [15]). Among other features, the configuration of the Dlog defines the radio network to which is going to be connected (gateway) and the frequency of readings. Each datalogger can hold up to 5 different sensors, depending on the model (i.e. 5 Channel Vibrating Wire Datalogger).

Dataloggers send the data wirelessly, through a long-range radio system to the gateway. The gateway acts as a concentrator, uploading all the sensor inputs coming from the nodes wirelessly to internet.

Sensor readouts are as a rule stored in the client's servers (on-premises cloud) or third-parties cloud providers. Then, the network management software developed by Worldsensing allows the user to access remotely to all the data from the sensors, as well as manage the entire network remotely. Some of the management tools the software provides are: manage sampling rate for each of the dataloggers connected, Internet connectivity options, system status, map view of datalogger location and radio coverage, customize files of selected data, automatically push files to another server, etc.

Loadsensing includes different designs of dataloggers to cover and obtain data from the majority of types of sensors commonly used in civil and geotechnical engineering. Loadsensing dataloggers are then compatible with sensors from analogue, digital to vibrating wire output signals. As a result, one client can have a wide range of sensor types all together connected to the same network and data acquisition system.

Robustness and weather proof design of Loadsensing dataloggers make them suitable for almost any environmental conditions.

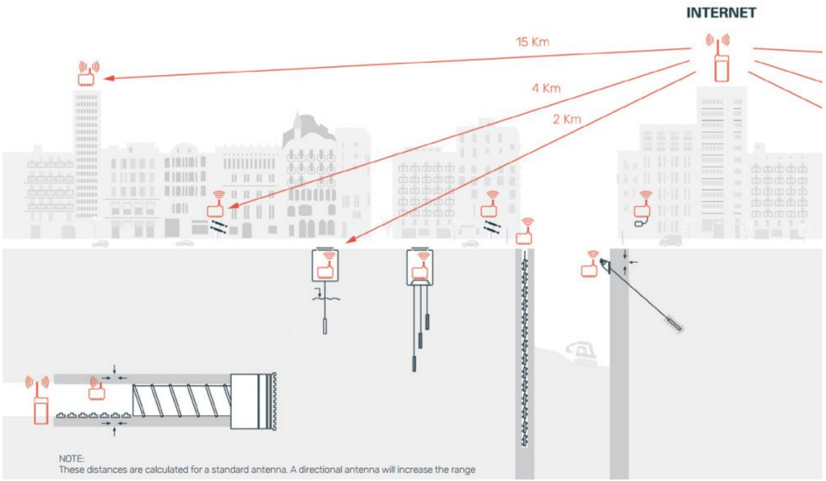

INTERNET
15 Km
4 Km
2 Km
NOTE:
These distances are calculated for a standard antenna. A directional antenna will increase the range

Figure 8. WorldSensing: General scheme set-up of a LoadSensing deployment in a city

The radio network coverage can be influenced by a wide range of external factors including the presence of buildings or infrastructures causing interferences, other radio signal interferences or the way itself in which the Loadsensing devices are installed on the field (height, covering elements, manholes, etc.)

Loadsensing provides estimation of the radio range as the results from tests performed at the conditions where Loadsensing is more likely to be used. Dataloggers can send data to a gateway placed up to 15 km distance on an open field, or 2 km when the datalogger is placed inside a manhole in a highly dense area of urbanisation.

Loadsensing dataloggers have an internal memory where all the readings of the data is stored. This ensures that if any unexpected problem arises to the radio communication with the gateway, the data will be safely stored and accessible from the datalogger.

Measuring inclinations with tiltmeters is essential for the success of many projects: from controlling building response during a tunneling project, over analyzing settlements, to tracking changes in the inclination of structures such as bridge piers or historical monuments and dams, to monitoring landslides including berms in open pits.

The Loadsensing Tiltmeter is a low-power long-range Wireless datalogger and inclinometer in a single, compact box. It measures tilt in two (biaxial) axes in the plane of its base. It combines a highly precise MEMS sensor plus the radio transmission network of Loadsensing system. Its ability to provide accurate measures with long-range wireless communication and extended battery life sets this inclinometer apart from other comparable products in the market.

Thanks to the long-range technology of the radio system used, the gateway-datalogger relative position is not a determining aspect in the installation. This result in many advantages of Loadsensing unique system:

- No signal repeaters needed (Star topology network).
- Gateway can be installed close to power source and Internet/3G/GPRS coverage.

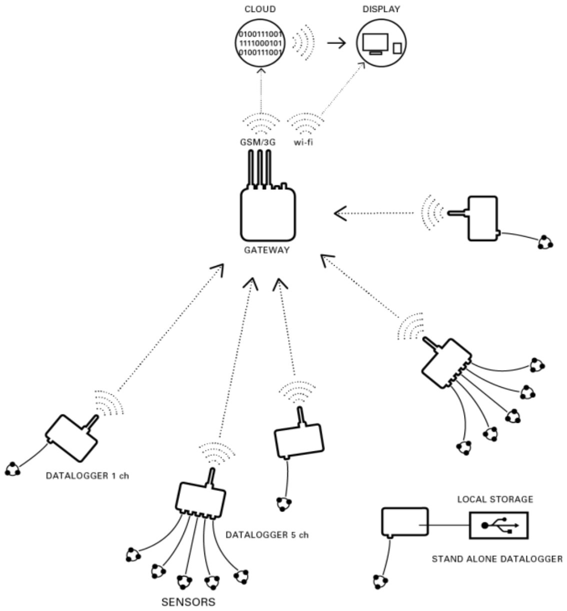


Figure 9. WorldSensing: Detailed LoadSensing architecture with the flow information flow

The different elements that compose the solution are described next:

1-**IoT devices (dataloggers)** are smart low-power devices equipped with sensors. The values measured (sensor readouts) are communicated wirelessly to the concentrator (gateway).

2-**Gateway**, which transfers the sensors' inputs to the cloud so that they can be visualized and analyzed therein.

3-**Cloud,** SW tools used to analyze the collected data from the deployed technologies.

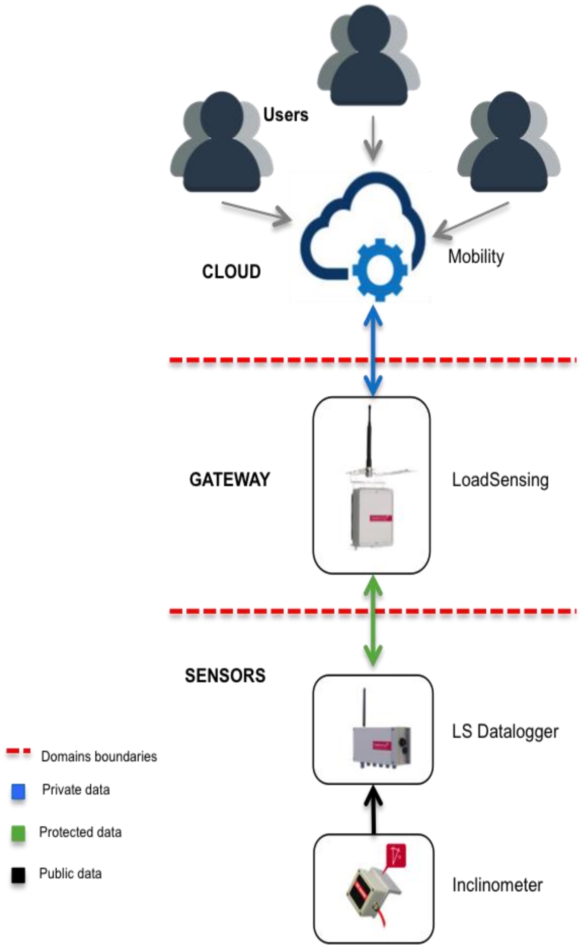


Figure 10. Worldsensing: Domains at a LoadSensing installation with the type of data flow

Service - Smart Infrastructure Monitoring

The service provided by WOS consists of IoT devices able to monitor the correct stability of the infrastructure. Such service is particularly interesting in several cases, notably: understand and plan the maintenance cycle of infrastructure, detect if problems occur during the construction process, etc.

Considering the necessity of protecting industrial IoT environments, the selected use case for SMESEC project is the Emergency Situation Management in Smart City during a construction process.

With more detail, whenever a new structure is being built, other buildings nearby may become unstable by the procedure, causing cracks or falls. LoadSensing's inclinometer allows engineers to monitor this in real time by observing the software dashboards. In addition, if a sensor reports a value higher than an alarm threshold, the alarm manager will broadcast an alert to prevent accidents.

Figure 11. Worldsensing: General view of elements in a Smart City

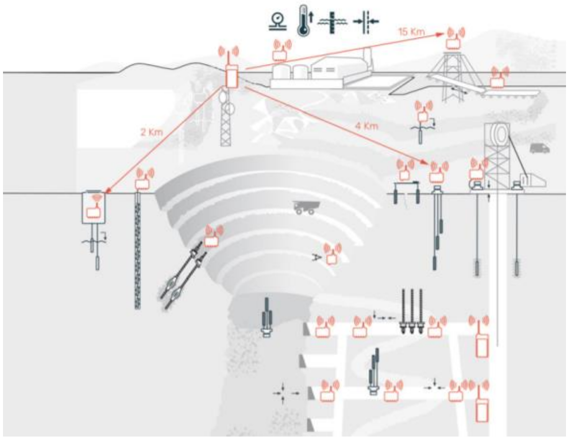


Figure 12. Worldsensing: General view of Loadsensing in an open-cast mine

Characteristics

- Industrial IoT
- LoRa wireless connectivity
- Physical elements
- SaaS
- Low power devices

Data flow and security classification

The data flow on the WOS solution is:

IoT device to Gateway to Cloud (Figure 13): The **IoT device** gets inclinometer information and sends it to the **Gateway** (wireless), which stores and forwards it to the **Cloud**. It is also possible (but not frequent) that the **Gateway** sends configuration messages (wireless) to the **IoT device** to set the desired characteristics. This is a periodical data flow.

Data have been classified and labeled in 3 different blocks:

1. **Public (Black)**: Information with a basic level of protection
2. **Protected (Green)**: Information with a high level of protection
3. **Private (Blue)**: Information with the maximum level of protection

The following scenarios illustrate the data flow and interaction among different elements.

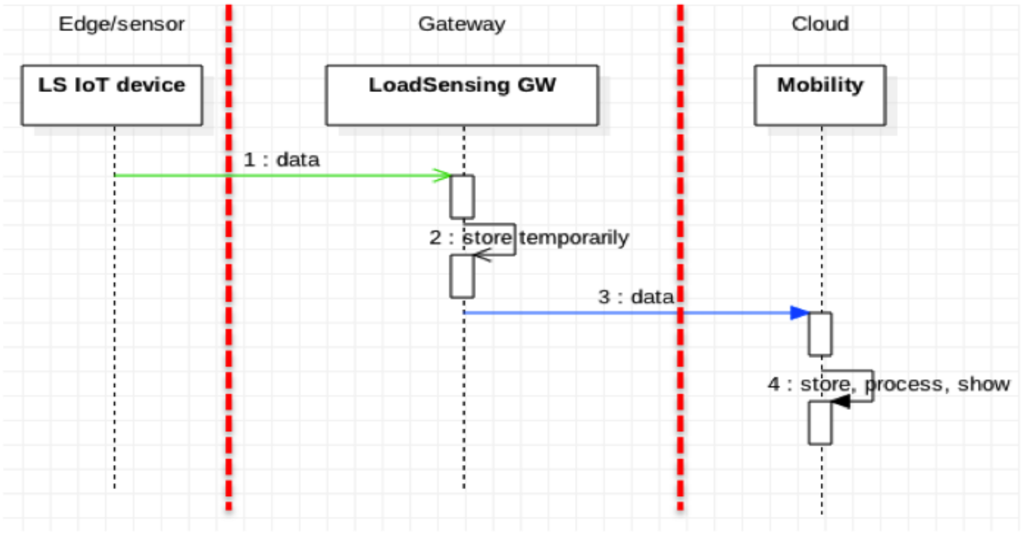


Figure 13. Worldsensing: Typical data flow in LoadSensing

2.5.2 List of Requirements

2.5.2.1 Systems and Components Used

The description of elements and their main characteristics are presented considering the domain classification outlined in Figure 8.

1) Sensor Domain: Sensors and Dataloggers

Worldsensing's LS-G6 dataloggers are low power, easy to use and field-friendly, and they are used for data acquisition from a great range of sensors in the market. Moreover, radio models can be used for long range communications, up to 15 km in open-field scenarios, and 4 km in urban scenarios.

LS-G6 dataloggers are battery powered, and easily configured through the Android Configuration App. The dataloggers and the gateway are robust (IP68 dataloggers, IP67 gateway) and do not need re-casing.

LS-G6 dataloggers are used in a wide range of professional sectors, such as civil engineering, mining, environmental or industrial monitoring, among others.

As far as the inclinometer sensors are concerned, the SCA121T Series contain 3D-MEMS-based dual axis inclinometer modules that provide instrumentation grade performance for leveling applications in harsh environment. The measuring axes of the sensing elements are parallel to the mounting plane and orthogonal to each other. Low temperature dependency, high resolution and low noise, together a with robust sensing element design, make the SCA121T the ideal choice for leveling instruments. The Murata inclinometers are insensitive to vibration, due to their over damped sensing elements, and can withstand mechanical shocks of up to 20000 g [16]. Vibrating wire sensors can be interfaced to the LS-G6-VW: the datalogger is supplied with cable glands (one for each channel), for the adjustment to different cable diameters.

After each terminal block is connected, taking a sensor reading is recommended to ensure that the connections have been done correctly. This reading should be compared with the reading of the sensor on installation with a portable readout unit, before connecting to the LS datalogger.

Features

- Dual axis inclination measurement (X and Y)
- Measuring ranges ±30° and ± 90°
- 0.0025° resolution (10 Hz BW, analog output)
- Sensing element controlled over damped frequency response (-3dB 18Hz)
- Robust design, high shock durability (20000g)
- High stability over temperature and time
- Single +5 V supply and unregulated 7…35V supply
- RoHS compliant

Data storage

The internal node memory size is 4 MB. The 5-channel datalogger connected to 5 sensors stores up to 73.500 readings. The 1-channel datalogger stores up to 200.000 readings. Times of data storage for LS datalogger 1 ch and LS datalogger 5 ch are indicated in Table 3. Here, channel (ch) is defined as the total number of sensors that a datalogger can control and operate. Memory mode is a circular buffer. When memory is full, logging continues by overwriting earliest readings. Besides the data from the sensor, health data is collected hourly, which indicates the battery voltage, the internal temperature of the node and the node uptime.

Number of sensors	Sampling rate		
	60 minutes	30 minutes	10 minutes
1	more than 10 years	more than 20 years	3.5 years
5	8 years	4 years	17 months

Table 3: Times of data storage (without overwriting) for LS VW-datalogger 1 ch and LS VW- datalogger 5 ch.

2) Gateway Domain: LoadSensing Gateway

a. Summary

- 868 MHz ISM band LongRange™ bidirectional communications capabilities
- Embedded, remote and open low power communication station
- Open development framework based on standard Linux OS
- WAN connectivity over GPRS/EDGE/3G or Ethernet

b. System

CPU:

- Based on ARM 926EJS core processor
- Up to 230 MIPS
- Real-time clock saved by battery
- Hardware watchdog
- Optimised power consumption management

Volatile memory:

- Low power DDRAM 128 MB
- 10 MB used for system firmware

Non-volatile memory:

- 128 MB NAND flash (40MB used for system firmware and auto-recovery mechanism)
- 8 GB eMMC

USB host interface allowing:

- Local software upgrade with simple USB key
- USB/NET local configuration/maintenance access

Power

- PowerOverEthernet supply: 48V class 0 (Max : 15Watts, Nominal : 3Watts (Lora Rx mode with GSM network attachment)
- DC power supply (ex: solar panel use) : 11 to 30Volts
- Power control: ignition detection, software OFF switching
- Back-up battery (up to about 1 minute allowing safe power down)

c. Communication

LongRange:

- Incorporate Lora™ bidirectional communications technology (RX : 863-873MHz , TX : 864-873MHz)
- Sensitivity: up to -141 dBm
- Tx conducted power from 0dBm to +28dBm
- 49 LoRa Demodulators over 9 channels
- More than 15km range in sub-urban situation

WWAN:

- HSDPA/UMTS (900/2100MHz): DL 3.6 Mbps / UL 384 Kbps (HSDPA), UL/DL 384Kbps (UMTS)
- GPRS/EDGE (850/900/1800/1900MHz): UL/DL 85.6Kbps (GPRS), UL/DL 236.8Kbps (EDGE)
- IMEI inside
- Internal antenna

Ethernet:

- PowerOverEthernet IEEE 802.3af alternative B 10/100 Base T compliant

GPS:

- Integrated GNSS high sensitivity GPS module
- NMEA 2.0 compliant

  - Internal antenna

d. Software

Operating System:

  - Standard Long-Term Support Linux version 3.10
  - File system YAFFS2 (NAND) and EXT4 (eMMC)
  - Support of all GNU/Linux tools (cross-compiled for ARM)
  - POSIX1 file system
  - TCP/IP BSD4.4 socket on network bearer

Software packages included:

  - PYTHON
  - SQLITE

Networking:

  - DHCP client and server
  - FTP server
  - SSH server
  - NFS client
  - Firewalling (iptables) and IP routing (layer 3)
  - HTTP server
  - TFTP server
  - L2TP tunnelling

3) Cloud Domain:

The cloud software to be used in the use-case proposed by Worldsensing relies on the Mobility platform [17] developed for the management of Smart Cities. This tool provides Operational Intelligence functionalities to city operators, and it has the particular feature of ingesting heterogeneous data from different sources. Here, the software will be used to geoposition the sensor deployment and perform the data analysis. The main technical characteristics of “Mobility” are summarized below:

Docker Images:

- Core
  - Mbmapsapi:2.0.1 - Ubuntu
  - Mbsqlapi:2.0.1 - Ubuntu
  - Mbredis:1.0.0 - Debian
- Utilities
  - mbrabbitmq: rabbitmq:3 - Debian
  - mbkong: kong:0.9.9 - CentOS
- Server
  - Mbhttpd:2.1.2 + Mbwebapp:1.5.6 + Mbadminpanel:1.1.0 - Debian
- Database
  - Mbpostgres:1.2.2 - Debian
- Services
  - Mbcustomobjects_service:1.4.0 - Alpine Linux

  - ○ Mbaction_service:1.2.0 - Alpine Linux
  - ○ Mbaction_log: 1.0.2 - Alpine Linux

--- Configurable

- Datafeeds
  - ○ Mbdatafeed_lstilt - Debian
- Objects
  - ○ Mbobject_lsinclinometer - Alpine Linux

--- Customisable

- Connectors
  - ○ Mbobject_loadsensing: Debian

2.5.2.2 Classification of Criticalness

The industrial monitoring sensors use case belongs mostly to the IoT domain, in contrast with the previous two use cases that fall under the Enterprise domain, and as such, different criticalness domains apply. Based on the use case analysis, the following levels of criticalness have been identified:

SENSORS DOMAIN: *Noncritical*

GATEWAY DOMAIN*:* *Critical*

CLOUD DOMAIN: *Highly critical*

2.5.3 Industrial Services Pilot Potential Attackers Threats

Potential internal threats

- Software misuse
- Access abuse
- Unauthorised Backend access
- Unprotected SSH keys
- Sabotage
- Data leakage

Internal threats basically compromise the operation of the LoadSensing deployments, and primarily the integrity and confidentiality of the stored data in the servers.

Potential external threats

- Physical access to the IoT devices and gateway
- Cyberattack to the gateway
- Cyberattack to the software platform (Mobility)
- MiTM attacks
- Brute force attacks to the web application
- DDos attacks

- 0day attacks
- Code injection

External threats apart from the same risks listed above for the internal threats, may trigger false alarms and cause irreparable damage to the sensors. It should be pointed out that false events in Mobility could lead to states of alert with a direct impact on citizens (i.e. infrastructure evacuation) and economic losses.

Threats and vulnerabilities due to human factor(end-users)

- Misuse of the software platform
- Stolen passwords
- Code injection

The misuse of the system due to the human factor may lead to the same consequences listed above for both internal and external threats.

Potential attack locations

Loadsensing deployments are generally in public places. For this reason, the cyber- and physical security of the nodes is subject to manifold and difficult to control risks that can jeopardize their integrity at any time (i.e. vandalism, nodes manipulation, etc.). Besides, the internet connection of the gateway opens the door to remote attacks. The same applies to the cloud infrastructure of the use-case. For all these reasons, it is not a straightforward task to enumerate the potential attacks locations, since the three domains are subject to many unrestrained potential risks.

2.5.4 System functionality and resources

What is the system normal behavior

IoT device sensors provide structure inclination periodically to the software platform through the gateway. This can be monitored real time using **Monitoring Software (Mobility)**.

What is the system abnormal behavior

- Services don’t work at the cloud side.
- Mobility software doesn’t receive inclination data from the gateway.
- The gateway doesn’t receive information from the dataloggers

Software utilities used or need to be used in the use case

N/A

Trust models used or need to be used in the use case

Two different roles are defined for the access to mobility software, internal team (developers, operations, quality) via SSH and web and external users (clients) only via web.

2.5.5 Security Related System Used or In Need in the Use Case

Security monitoring systems used
Nothing used as of yet

Security systems used
IPtables as firewall and ACLs: feeding a list of machines which interact with LoadSensing infrastructure is considered a basic security measure. Those with "write" and "configuration" permissions are crucial to guarantee the functioning of the system and the integrity of the acquired data.

Type of security related information collected
Access logs of internal and external users and API users: following the same approach than in the previous point, not only the machines interacting with LoadSensing are monitored, the adequate permissions are also granted to the physical users and their logs in the system controlled. The same applies to those users getting data through APIs.

Emergency protocols used
Nothing used as of yet

Information exchanged
Nothing used as of yet

2.5.6 Security Incidents Handling and Recovery

No incidents have happened yet, but if there appear, should be handled through the Cloud Service Provider.

Practices used
Nothing used as of yet

Other security guidelines used
Nothing used as of yet

Recovery processes
In the event of a cloud platform disaster or malfunction, the docker-based architecture of the solution allows checking the last backup and restore it in a simple way.

2.5.7 Data Protection and Recovery

Type of data kept
Public information (noncritical and critical) and personal information (highly critical) is kept.

Data storage solutions use
Docker with PosgreSQL

Data storage technologies used
Cloud

Storage disaster and recovery practices
Not following standards and best practices as of now.

Backups of dockers are made, including data in the Cloud

2.6 Smart Grids Pilot

2.6.1 GridPocket SAS

The PowerVAS [16] platform is initially based on the global oneM2M [19] and ETSI M2M [20] standards. This is the first solution to combine high performance large scale data analysis, machine events handling and behavioral science to enable electricity, gas and water utility value-added services with unprecedented levels of applicative flexibility, consumer commitment, and usage insights.

In the architecture of PowerVAS separate modules are integrated together to assure the secure energy data collection, structured and unstructured data storage and treatment, horizontal scaling, user interaction and programmable control. PowerVAS, as a dynamic platform, offers diverse and personalized functional solutions.

This core platform is extended by GridPocket and thirty party applications for data analysis, demand-response management, open data services, electric vehicle charging, renewable energy production and the award winning GridPocket's EcoTroks [21] consumer engagement application (award of EDF Innovation in 2012, award of Green Innovation France in 2011). These applications are fully customizable and distributed via partnerships with leading energy distributors, equipment manufacturers and utilities worldwide. GridPocket proposes a software development kit to enable independent vendors to create and commercialize new energy-related applications.

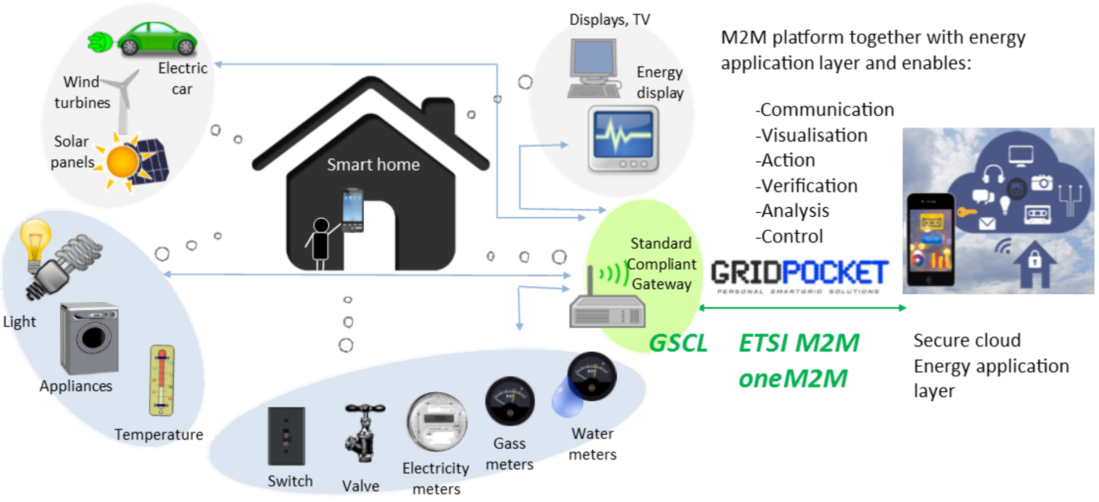


Figure 14. GridPocket use case description – connection between GridPocket cloud platform and smart grid components

2.6.2 List of requirements

A specific care needs to be taken of all components of the cloud applicative environment. There is at least one instance of the production environment and one instance of the pre-production environment put in place for every utility customer.

2.6.2.1 Systems and Components Used

Alias	Description
Cloud platform	All systems are based in public cloud (OVH, Amazon…) or private clouds of business customers [20]
User Interface VM	Virtual Machine that keeps functionality of web application.
API Layer VM	API is security layer that takes care of improved security on database
DB VMs	Data base cluster with MongoDB technology (Architecture based on customer requirements).
RP VM	Nginx Reverse Proxy [23] to provide improved security for whole system.
Live Monitoring System	Zabbix Server [24] that live monitor all VMs. One monitoring system for all customers is used.

2.6.2.2 Classification of criticalness

Based on any risk assessment of each system provide a classification based on criticalness

Alias		Description
Cloud platform	HIGH	The security of the cloud platform provider is essential for the security of the system
User Interface VM	HIGH	The UI VM are front end of the system
API Layer VM	HIGH	API manages accesses to the system

DB VMs	HIGH	Energy data involves personal and sensitive information
RP VM	HIGH	Reverse proxy is part of the system security
Live Monitoring System	MEDIUM	The monitoring system assures communication with administrators in case of problems. It has access to major components of the platform.

2.6.3 Smart grids pilot potential attackers and threats

Potential internal threats

- DoS and DDoS on all system components – this attack will block end-users from accessing the platform, it can also impact other subsystems communication with GridPocket's platform (e.g. metering data management platform) from functioning correctly
- DB Injection –the modification of data in DB would result is several impacts including users' equipment functioning, billing information
- Man in the middle – Men analyzing and manipulating JavaScript in server to EndUser communication

Potential external threats

- DoS and DDoS attacks on all systems and services accessible from Internet (VPN, Logging to the PowerVAS System)
- MiTM – Men analyzing and manipulating JavaScript in server communication

Threats and vulnerabilities due to human factor (end-users)

- Compromising Credentials – loss of credential exposes personal data of end-users, as well as logical and physical system connected to his account

Potential attack locations

- All locations with Internet Access (Only PowerVAS and VPN) – the front end of PowerVAS is exposed to public internet, anyone with IP access to access this platform
- GridPockets Internal network – this network is available to employee of the company, a limited access might be available to visitors or sub-contractors
- Network of the Hosting Company – the hosting companies are public cloud infrastructure providers or internal IT departments of utility companies
- Network of building that GridPocket has office in – this case applicable for some subsidiaries of GridPocket that are connected to a campus network
- Network of GridPocket ISP (Can spoof an IP) – the ISP are large telecom companies

2.6.4 System Functionality and Resources

The platform instances are built based on the performance requirements of specific business customers (utilities). The architecture choices might depend on the number of end users, volume of data, third party systems connected, local security requirements, integration with other legacy solutions, service-level agreements. To run basic environment, the following are needed:

- Reverse Proxy (Nginx) – It can run load balancing and security improvements due to isolating application server. Amount of resources based on load
- Application server (minimum one) – NodeJS Application Server 2 CPU, 2 GB of RAM
- API Layer Server (minimum one) – NodeJS Application that improves security isolating DB from User Interface Server
- DB Cluster Minimum one server or more depends on load and data security requirements
- Monitoring (Zabbix) – One instance for all environment.

What is the system normal behavior

- System Monitor (Zabbix) doesn't alert.
- After putting correct address to browser, one can see login page.
- After putting correct credentials, one can login to the system

What is the system abnormal behavior

- Zabbix sends alerts (via email of to the internal instant messaging system that GridPocket uses)
- No login screen after putting correct address to browser
- No possibility to login even if someone can see login page (DB Failure)
- Slow response time
- Modified service data

Software utilities used or need to be used in the use case

N/A

Hardware components and procedural solutions used or need to be used in the use case

No use of hardware security devices

Trust models used or need to be used in the use case

Several different roles are defined for the access to the software: internal team (developers, operations, quality) via SSH and web, utility administrator (via WEB), end-users (clients) only via web with different level of features and permissions (building manager, occupant, visitor…)

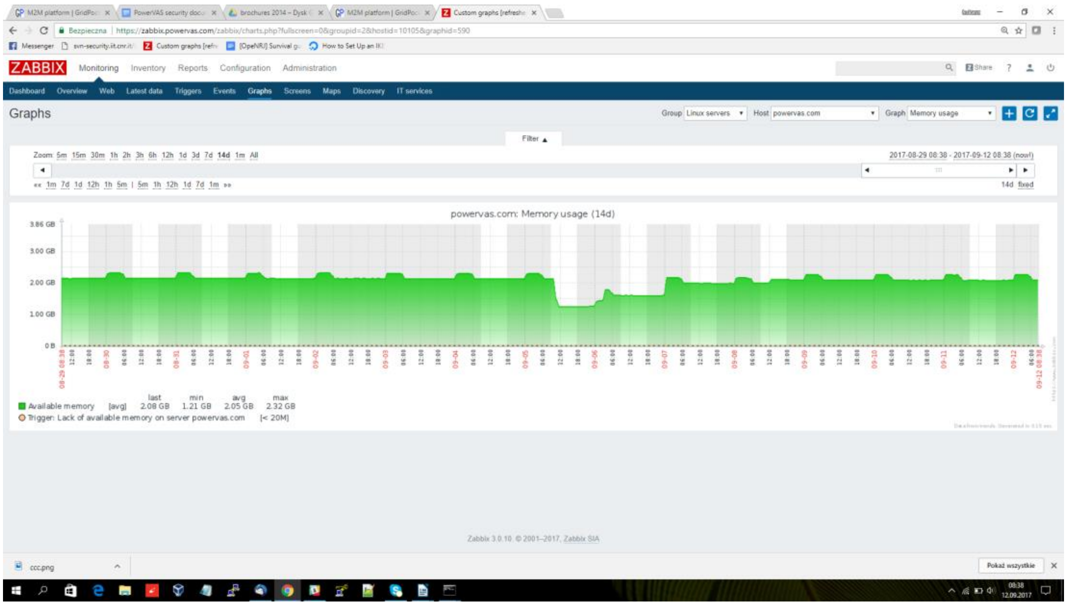


Figure 15. GridPocket example of Zabbix monitoring

2.6.5 Security Related System Used or In Need in the Use Case

Security monitoring systems used

- **Zabbix** – Open Source system that uses its own agent, SNMP and other collecting methods. It can alert if configured trigger is raised. It collects data from all systems components like User Interfaces, App servers, mDbs, Zabbix can show data on graphs for easy data analysis.
-

Security systems used

- **IPTABLES** – This is solution is put in place as part of the main firewall on reverse proxy (the only one machine with external IP)
- **Fail2Ban** – This tool is configured in a way that kit can monitor log files looking for different type of attacks and act in case of suspicion use.
- **UFW** – Firewall solution used on the internal machines to restrict unwanted network traffic in environment Local Area Network
- **Zabbix –** central monitoring platform ensuring control of the entire system

Type of security related information collected

All system components logs are collected and analyzed, like:

- NGINX log that keeps all login attempts to the system. This log is analyzed with Fail2ban and eventually Fail2Ban automatically blocks "bad traffic"
- VPN StrongSwan [25] log. his log is analyzed with Fail2ban and eventually Fail2Ban automatically blocks "bad traffic"
- NodeJS logs
- MongoDB logs

Emergency protocols used

None at the moment

Information exchanged

No inputs/outputs

2.6.6 Security incidents handling and recovery

Practices used

None yet

Other security guidelines used

None yet

Recovery processes

None yet

2.6.7 Data Protection and Recovery

Type of data kept

For proper working of the system all personal data involving the end users need to be collected, stored, and retrieved. Additionally, all measurement data like, water, energy or gas consumption is also collected, stored and retrieved. On top of consumption data, there are some analyzing tools.

Data storage solutions used

Mongo DB Cluster Storage – storage of personal data (identification, parameters), energy data (metering data logs) and other data (weather data logs, connected devices logs)

Data storage technologies used

NAS, and RAIDs – the storage clusters are put in place according to requirements of each platform instance. This includes RAID disk solutions and NAS subsystem.

Storage disaster and recovery practices

None yet

3 Risk/Vulnerability Assessment

3.1 Prioritized Cybersecurity Threats

Cybersecurity should be lightweight and effective for SMEs. We followed a taxonomy-based approach in order to understand the priorities and needs of SMEs for cybersecurity. With a questionnaire, we asked the four SMESEC SME use case partners to study the OWASP **top-10 cybersecurity threats** [26] and select the ones they perceive to be of top relevance for them. The obtained results will be used for the design and development of the SMESEC framework and strategy for the market together with the market analysis and exploitation plan of WP6.

Table 3 gives an overview of the cybersecurity threats that were prioritised by the SMESEC use cases. The table lists the threats according to decreasing median ranking (a threat that was not selected to be of priority was considered to be rank 14).

Threat	OWASP Rank	Rationale	Scytl	GRID	UoP	WOS
T01 Distributed Denial of Service (DDoS)	-	This attack is easy to perform and very difficult to mitigate without an infrastructure made for this purpose.	1	1	5	n/a
T02 Using Known Vulnerable Components	9	An SME needs to quickly identify when someone is trying to exploit a known bug. In some cases, there are vulnerable components that do not have a fix or replacement. Even the SMESEC security framework should be assessed.	2	NP	1	5
T03 Broken Authentication and Session Management	2	Unauthorized users might be messing with submitted problems or the backend.	12	2	4	1
T04 Security Misconfiguration	5	Various components are used for more than one service. If one of them is attacked, then multiple services are vulnerable.	8	3	2	4
T05 Injection	1	-	4	5	NP	2
T06 Cross-Site Scripting (XSS)	3	Linking to known vulnerable components can be used to attack an API.	6	4	3	NP
T07 Sensitive Data Exposure	6	Even with just email and phone number, a user may be identified. The exposure of such information is a risk with a high impact, but measures at the application level may mitigate it. This threat must be re-evaluated with the new GDPR regulations.	5	NP	7	3
T08 Garbage Data	-	Someone spamming garbage data may cause serious issues to a digital service.	n/a	n/a	6	n/a
T09 Internal Threats (Malicious Insiders)	-	Users with elevated access rights can cause damage to various components, code, and databases. Most likely this damage will be involuntary.	3	n/a	8	n/a
T10 Insecure Direct Object References	4	-	7	NP	9	NP
T11 Cross-Site Request Forgery (CSRF)	8	-	9	NP	10	NP
T12 Not Validated	10	-	10	NP	11	NP

Redirects and Forwards						
T13 Missing Function Level Access Control	7	-	11	NP	NP	NP

Table 3: Cybersecurity treats, prioritised by the SMESEC use cases

In Table 3 column "OWASP Rank," the dashed cells are non-OWASP threats added by the SMESEC use case SME partners. NP means non-prioritized.

The threat priorities reflect the **experience of cybersecurity experts** in the SMESEC consortium. According to these experts, SMEs indeed perceive threats like T01 (DDoS), and T02 (the use of vulnerable components) to be critical even though their global OWASP ranking places its criticality lower. The perception is likely to be driven by the available information in the media.

Media reports about T01 (DDoS attacks) have become common. Some reports show that even small consumer devices such as baby phones and webcams can be a threat. A simple firewall is not able to block such an attack as the bandwidth of the firewall can be exhausted even before the firewall. The only means to protect against bandwidth exhausting DDoS attacks is to buy services in professional data centres with large and redundant lines.

The perception of T02 (vulnerable components) is likely to be driven by a combination of time-to-market pressure and the use of complex cybersecurity frameworks that are not understood by the SME. The time-to-market pressure pushes the SME to focus on innovation and down-prioritise quality and security. By using a complex cybersecurity framework, the SME loses control and knowledge over the parts covered by the framework. In this situation, some SME worry that the framework increases the SME's attack exposure. An attack on the framework would not only affect it but all the applications that are using the framework. The use of the framework by a large number of SMEs turns these SMEs into targets that are vulnerable to one single attack, i.e. through the framework. To mitigate this threat, the SMESEC framework will need to be as simple as possible and managed to minimize exposure to such cyber risks.

The rating of the threats T03 (broken authentication), T05 (injection), and T06 (cross-site scripting) is consistent with the OWASP ranking. The consistency could indicate that SMEs are afraid of the liability that comes with the delivery of a vulnerable product or service.

Some of the SMESEC use case SMEs added threats not considered by OWASP: Three added T01 (Scytl, GRID, UoP: DDoS) and two added T09 (Scytl, UoP: the internal threat of malicious insiders). The consulted experts from the SMESEC consortium agreed with that judgment. This threat may have a significant impact on the SME's reputation. One SMESEC use case partner SME added T08 (UoP: garbage data). Their service was particularly exposed to that threat.

Some differences can be observed in the judgments of different SMESEC use case partner SMEs, for example in the judgment of T03 (broken authentication). Depending on the type of business and depending on the awareness and measures installed by an SME, the threat exposure can change. A SME that has invested in the mitigation of such a threat is not so much exposed to the threat anymore, thus judges it to be of lower criticality.

The priorities shown in Table 3 will be used to review the alignment of the SMESEC framework with the needs of the SMESEC use case partner SMEs. At the same time, the obtained threat analysis is preliminary. Threats evolve, and so does the understanding of how they should be addressed. The

SMESEC consortium plans to repeat the threats analysis during the SMESEC trials and plans to include threat monitoring as an important part of the SMESEC offering, thus allowing evolution and self-alignment even when the SMESEC framework is being used.

The four SMESEC use case partner SMEs were also asked to identify the most **important causes that affected their prioritised cybersecurity threats**. They categorised the threats as being internal or external when reasoning about the causes that impact the risks. Some of the threats were agnostic to the location of the potential attacker or problem.

- Internal causes: T02 (vulnerable components), T03 (broken authentication), T04 (security misconfiguration), and T09 (malicious insiders) were judged to be internal risks as they refer to decisions made by employees. T04, for example, was a result of bugs in the digital offering of the SMESEC use case partner SME that affected security.
- External causes: T01 (Distributed Denial of service), T05 (injection), and T06 (cross-site scripting) were considered external. For example, Distributed Denial of Service requires the use of many machines to execute the attack.
- T07 (sensitive data exposure) was considered to be a hybrid because it is affected by decisions made by employees but depend on the customers' end-user behaviour.

Further drivers of cybersecurity threats were past incidents. For example, an attacker had gained access to a web server of one of the four SMESEC use case partner SMEs and spammed e-mails through the e-mail service. Affected by that driver were the threats T02 (vulnerable components), T03 (broken authentication), and T04 (misconfiguration).

Some of the threats were requested to be managed by customers. One use case partner had requirements for ISO/IEC 27.000 compliance. Also, T01, T02, and T05 had to be addressed by one of the use case partners based on customer requests.

The SMESEC use case partner SMEs used multiple approaches for **discovering cybersecurity threats**. Employees identified some of the threats. For example, one of the SMESEC use case partner SME's employees identified T07 (data exposure), T08 (garbage data), and T09 (malicious insiders) to be particularly problematic.

Other threats were identified with changes in regulations. For example, the threat T07 (sensitive data exposure) is perceived to be particularly problematic when the new GDPR regulation come into force.

The SMESEC use case partner SMEs obtained knowledge about how to handle the cybersecurity threats by studying the news, cybersecurity web portals, and cybersecurity social forums. The satisfaction of the SMESEC sue case partner SMEs with these knowledge sources is good.

Our questionnaire encouraged the SMESEC use case partner SMEs to reflect about common cybersecurity risks. This request generated in-depth reflection about the priorities of the risks, the causes for these risks, and possible mitigation strategies – a form of awareness about cyber risks. As a benefit, the SME that answer such a questionnaire develop a readiness for improving cybersecurity capability. SMESEC intends to utilize questionnaires for this purpose as part of the SMESEC framework offering (see the subsection below).

The SMESEC use case partner SMEs addressed some of the threats already before they received and answered our questionnaire. The following approaches and tools were used:

- Continuous updates for all operating systems, software components, and external services were a practice adopted to address T02 (vulnerable components) and T04 (security misconfiguration). The satisfaction was excellent, and no improved tooling is needed.
- Dependency checks were used to address T02 and identify vulnerable components that should not be used. The satisfaction was excellent, and no improved tooling is needed.
- Firewalls were used to isolate the digital service from the environment. The satisfaction with the used firewalls was good.
- Fail2Ban [12] was used to mitigate dictionary attacks in SSH. The satisfaction was good, and Fail2Ban should be used as a benchmark.
- Prometheus [79] was used for high traffic monitoring. The satisfaction was bad, and SMESEC should consider the offering of alternatives.
- MicroFocus Fortify [80] was used to address T03 Broken Authentication and Session Management, T05 (injection), T06 (cross-site scripting), T07 (sensitive data exposure), T10 (insecure direct object references), T11 (cross-site request forgery), and T13 (missing function level access control). The satisfaction was good, and Fortify should be used as a benchmark.
- Incapsula [81] was used to address T01 DDoS. The satisfaction is good, and Incapsula should be used as a benchmark.

3.2 Evaluation of Awareness Capability Improvement Models

Maturity models are being used by organisations to assess and improve their maturity of how they handle cybersecurity. The maturity model allows a company to understand its strengths and weaknesses and therefore companies could create a plan for improvement and fix their identified issues. For example, the company can define new policies and processes (at different levels), plan and perform employee training, and procure tools to build on the strengths and reduce the weaknesses.

In the context of cybersecurity for digital products that are developed and offered by SMEs, University of Utrecht had proposed two alternative maturity models: the Information Security Focus Area Maturity Model (ISFAM [27]) and the Cyber Security Focus Area Maturity Model (CYSFAM [28], in publication). ISFAM is a lightweight incremental model that has been used successfully for improving the cybersecurity practices of a medium-sized company that used information and communication technology to support its business. CYSFAM is a comprehensive maturity model that has been used successfully for improving the cybersecurity practices of a large company, a finance institute with offices in The Netherlands, that offered digital services to customers.

Information and feedback obtained from the four SMESEC use case SMEs indicated a combination of ISFAM and CYSFAM might be appropriate to help to build awareness and capabilities to address the prioritised threats. The SMEs targeted by SMESEC are primarily selling digital products and services and consider themselves only secondarily as being users of ICT. The CYSFAM themes should thus be used to give focus to the cybersecurity practices. The SMEs required a lightweight approach to managing cybersecurity. This concern is reflected in the structure of ISFAM. ISFAM is thus a good starting point for building a modular, incremental framework that allows a SME to manage cybersecurity in a risk-based, value-oriented manner.

An initial architecture of a **cybersecurity awareness and capability model adapted to SMEs**, a SMESEC capability model, could be structured as follows. The architecture is based on a conceptualization of an SME in terms of the products the SME develops, the services the SME offers, the infrastructure the SME uses, and the resources like humans and finances it uses. The conceptualisation allows adaptation to the specifics of the SME, for example, to differentiate between a medium-sized company that develops IoT products and a small company that offers online services.

The SMESEC capabilities should be based on the CYSFAM capability themes. Table 4 shows the CYSFAM themes and the value they may offer to an SME when being adopted. According to the SMESEC experts, the scope of CYSFAM is adequate. The only missing part may be the use of code inspection for fast ramp-up of cybersecurity capabilities and absorption networks for addressing distributed denial-of-service attacks. In Table 4, asterisk (*) stands for these themes not originally in CYSFAM.

CYSFAM Theme	Value	Category
Security Baseline	Definition of SME's cybersecurity practices	Ability to Manage Cybersecurity
Vulnerability Scans	Discovery of threats	Ability to Manage Cybersecurity
SIEM	Security information and event management	Ability to Manage Cybersecurity
Asset Management	Management of threats	Ability to Manage Cybersecurity
Patch Management	Addresses T01 Denial of Service, T02 Vulnerable Components, T03 Broken Authentication, T05 Injection, T06 XSS, T07 Sensitive Data, T10 Object References, T11 CSRF, T12 Redirects and Forwards, and T13 Access Control	Fast Ramp-Up of Capabilities
Access Control and Audit	Addresses T03 Broken Authentication, T09 Malicious Insiders, and T13 Missing Access Control	Fast Ramp-Up of Capabilities
Malware Scans	Reduces threats	Fast Ramp-Up of Capabilities
* Code Inspection	Reduces Denial of Service, DB injection, and identifies security holes.	Fast Ramp-Up of Capabilities
User Training	Establish cybersecurity awareness, knowledge and good behaviour	Fast Ramp-Up of Capabilities
*Absorption Networks	Addresses T01 Distributed Denial of Service	Upon SME Initiative
Network Controls	Reduces threats	Upon SME Initiative
Credential Management	Addresses T04 Security Misconfiguration, T09 Malicious Insiders, and T13 Missing Access Control	Upon SME Initiative
Second Opinion Defence	Mitigates tool-, service-, and method-specific weaknesses	Upon SME Initiative
Security Engineering	Engineering of assets to prevent misuse and malicious behaviour.	Upon SME Initiative
Application Change Management	Management of assets to prevent accidental introduction of vulnerabilities.	Upon SME Initiative
Compliance Audits	Ensures implementation of security baseline	Upon SME Initiative
Automation	Hardens the cybersecurity measures, accelerates, and reduces operational cost	Upon SME Initiative

Standards Compliance	Satisfaction of customer requirements	Upon SME Initiative
CIRT Team and Process	Offers guaranteed response to security-relevant events.	Ability to Manage Cybersecurity (Medium-sized Enterprise)
Budgeting and Funding	Offers capacity to build security and respond to security-relevant events.	Ability to Manage Cybersecurity (Medium-sized Enterprise)
Governance	Establishes autonomy and accountability in the management of cybersecurity.	Ability to Manage Cybersecurity (Medium-sized Enterprise)

Table 4. Analysis of CYSFAM capability themes

SMESEC should provide an SME with the ability to select relevant CYSFAM themes and apply them to the SME's product development, service provision, infrastructure, and resources. To support SMESEC adoption, the themes should be grouped into themes for managing cybersecurity, fast ramp up with a lot of value for little cost, value-creating themes for the specific needs of the SMESEC user, and organisational themes for medium-sized enterprises.

This capability improvement architecture will be used as a basis for designing the cybersecurity awareness and capability improvement plan in the deliverable D2.3 [2].

4 Security Market Analysis

In this section, an analysis of the security market follows. The main goal is to:

1. Identify what are the key market segments
2. Identify emerging markets that will play key roles in the next few years
3. Identify key players and product capabilities
4. Summarize findings and correlate to SMESEC products

A large part of the research in this section has been based on the online resource of [29].

4.1 Security market segments

4.1.1 Encryption

Encryption refers to the process of protecting sensitive data by converting to an encoded form that can be decrypted by means of a protected key. This method ensures that even if security is breached in other levels, data will still be highly protected and will be useless to any malicious user (see online resources [30], [31], [32], [33]).

Key players:

Symantec endpoint encryption	Symantec's encryption portfolio includes endpoint, file and folder and email encryption. Integration with Symantec Data Loss Prevention automatically encrypts sensitive data being moved onto removable media devices or residing in emails and files. Robust management features include individual and group key management, automated policy controls, and out-of-the-box, compliance-based reporting. Heterogeneous management capabilities include support for native OS encryption (FileVault2) and Opal compliant self-encrypting drives. URL: https://www.symantec.com/products/endpoint-encryption
Sophos Safeguard Encryption	Sophos SafeGuard Enterprise Encryption 7 introduces the most complete data protection solution on the market today, protecting data on multiple devices and operating systems. Whether data resides on a laptop, a mobile device, or being collaborated upon via the cloud or other file sharing method, SafeGuard Encryption is built to match organizational workflow and processes without slowing down productivity. URL: https://www.sophos.com/en-us/products/safeguard-encryption.aspx

McAfee Complete Data Protection	McAfee Complete Data Protection secures critical data on endpoints with powerful enterprise-grade drive encryption. This endpoint encryption suite also enables management of native encryption on Macs and Windows systems. URL: https://www.mcafee.com/us/products/complete-data-protection-advanced.aspx
Kaspersky Endpoint Security	Data encryption with highly integrated security policies that can be aligned with application and device controls protects your data if devices or files are lost or stolen. URL: https://www.kaspersky.com/small-to-medium-business-security/endpoint-select

Table 5. Encryption key players and products

Encryption Market affinity to SMESEC

In fact, encryption is one of the first requirements when it comes to protecting sensitive data. Apart from the key players, there is a wide range of open source solutions as well (e.g. VeraCrypt [34], CryptTool [35], DiskCryptor [36], etc.) that cover different aspects like file, filesystem, and network encryption. None of the SMESEC contributed products is now directly related to the encryption market, thus it makes this particular market attractive for adding the specific capabilities to the SMESEC.

4.1.2 Governance, Risk Management and Compliance (GRC)

Governance, Risk Management and Compliance (GRC) is a term often used to describe the organization efficiency to achieve its objectives, address uncertainty and act with integrity. In these three terms, (i) Governance refers to the processes involved to assure that the organization handles information properly across all workflows, (ii) Risk Management stands for predicting and handling possible risks that may slow the organization achieving the goals and (iii) Compliance includes all the processes to adhere with laws and regulations, as well as company policies (such as PCI DSS, HIPAA, HITRUST, EI3PA, SOX, GLBA, FISMA, ISO 27001) (see online resources [34], [38], [39]).

Key players:

EMC-RSA	RSA Archer eGRC Solutions allow you to build an efficient, collaborative enterprise governance, risk and compliance (eGRC) program across IT, finance, operations and legal domains. These solutions include policy, risk, compliance, enterprise, incident, vendor, threat, business continuity and audit management. URL: https://www.rsa.com/en-us/products/governance-risk-and-compliance

IBM	The IBM OpenPages GRC Platform delivers a modular platform for foundational GRC, enabling businesses to deploy scalable solutions for managing enterprise wide risk and compliance. It is designed for increasing overall productivity and efficiency, the OpenPages GRC Platform supports agile implementation for rapid time to value. URL: https://www.ibm.com/analytics/us/en/business/governance-risk-compliance/
MetricStream	MetricStream offers an advanced and comprehensive IT GRC software solution for streamlining IT GRC processes, effectively managing IT risk, and meeting IT regulatory requirements. The MetricStream solution enables companies to implement a formal framework to rigorously measure, mitigate, and monitor IT risks. URL: https://www.metricstream.com
RSAM	Rsam's Enterprise GRC software helps organizations successfully manage risk, compliance, audit, and security needs effectively. The Rsam Platform provides the most intuitive and flexible solutions for GRC, security risk intelligence, vendor/third-party risk management, KPI/KRI metrics, and on-demand applications. URL: http://www.rsam.com
Risk Vision (formerly Agiliance)	RiskVision™ is an integrated, purpose-built risk intelligence platform that offers a flexible, modular approach to managing enterprise risk. RiskVision pre-packages concurrent Integrated Risk Management Solutions (IRMS) and Security Operations, Analytics, and Reporting (SOAR) use cases that integrate three lines of defense of risks. URL: https://www.riskvisioninc.com
Lockpath	Lockpath Keylight Platform consists of a fully integrated suite of management applications designed to manage all facets of compliance and risk programs, including IT Risk Management, Operational Risk Management, Vendor Risk Management, Audit Management, Business Continuity Management and Corporate Compliance. URL: https://www.lockpath.com/platform/

Table 6. Governance, Risk Management and Compliance key players and products

GRC market affinity to SMESEC

This market covers some security aspects that usually SMEs neglect to address, like who has the rights to the data, whether data adhere to company or other legal compliances, and what how to deal with issues that can be foreseen through risk management. This kind of services often comes on top of other first level security solutions, and SMESEC aims to address this space as well.

By collecting traffic, usage, and other data from the underlying infrastructure (firewall, antivirus, etc.) the integrated framework can re-assess the risk periodically, whereas the overall architecture should take into account general governance and compliance constraints. FHNW contributed product will help here, and many of the characteristics of the main products in this market segment can drive the development of extensions.

4.1.3 Data loss prevention

Data loss prevention is the set of security controls for protecting sensitive enterprise data from being disclosed to unauthorized users across all platforms (computers, mobile, etc.) and throughout its life cycle (see online resources [40], [41], [42], [43]).

Key players:

Symantec	Symantec Data Loss Prevention is the most comprehensive and a fully integrated DLP which protects your information wherever it lives: in the cloud, on mobile devices and in your data centers. Security experts at Symantec are leading the innovation in Data leakage prevention (DLP)Technology for the start. URL: https://www.symantec.com/products/data-loss-prevention
Digital Guardian	Digital Guardian Data Loss Prevention (DLP) gives you the deepest visibility, the fine-grained control and the industry's broadest data loss protection coverage to stop sensitive data from getting out of your organization. URL: https://digitalguardian.com/
Forcepoint	The Forcepoint™ DLP Module enables you to discover and protect sensitive data in the Cloud or on-premise. You can secure personal data, intellectual property and meet compliance requirements quickly with custom or out-of-the-box. URL: https://www.forcepoint.com
Intel Security	McAfee Total Protection for Data Loss Prevention (DLP) safeguards intellectual property and ensures compliance by protecting sensitive data wherever it lives: on premises, in the cloud, or at the endpoints. McAfee Total Protection for DLP is delivered through physical or virtual low-maintenance appliances and the McAfee ePolicy Orchestrator platform for streamlined deployment, management, updates, and reports. URL: http://www.intelsecurity.com

Table 7. Data Loss Prevention key players and products

DLP market affinity to SMESEC

Data leakage is a serious concern among all enterprises, and traditionally impose strict rules over the access and exploitation of these data. As there is no contributed product in the DLP market, SEMSEC must take into account all these concerns by examining the main characteristics of the DLP products and provide either some level of DLP protection, or hooks for integration with third-party DLP products.

4.1.4 Unified Threat Management (UTM) / Firewalls

Unified Threat Management is the all-in-one security solution that integrates multiple solutions, such as antivirus, VPN, firewalls, content filtering, etc. often running simultaneously (see online resources [44], [45]).

Key players:

Fortinet	FortiGate UTM solutions are compact, cost-effective, all-in-one security appliances ideal for small businesses, remote, and retail networks. They include high-performance next generation firewall, VPN, IPS, application control, web filtering, antivirus, antispam, data loss prevention, and more—easily managed via a single console. URL: https://www.fortinet.com/products/next-generation-firewall.html
Checkpoint	Check Point has one of the best united threat management, or UTM, approaches, providing solid products -- both for the high and low ends of the market -- with the essential features enterprises look for. URL: https://www.checkpoint.com/products-solutions/all-products/
Sophos	Sophos SG Series firewall: Essential next-gen firewall protection for your network, web, email, applications, and users. Sophos UTM's simple, intuitive user interface (UI) is designed to let you quickly protect your network and users. It offers the latest next-gen firewall protection including mobile, web, endpoint email encryption and DLP. URL: https://www.sophos.com/en-us/products/unified-threat-management.aspx
SonicWALL	Unified threat management (UTM) technology delivers comprehensive protection and simplifies security management, all without slowing your network. Get gateway antivirus, anti-malware, anti-spam, intrusion prevention, content/URL filtering, SSL VPN and application control capabilities in a single package. URL: https://www.sonicwall.com/en-us/home
Cisco Meraki MX	The Meraki dashboard provides deep visibility and control over all of your security appliances from any Internet-accessible device, anytime, anywhere. View networked clients, bandwidth consumption, and application usage across all sites—and push policies to block, shape, or whitelist activity to optimize

	performance and user experience. URL: https://meraki.cisco.com/products/appliances
Barracuda NextGen Firewall (X Series)	The X-series firewall enables small and medium size companies to securely adopt cloud applications, virtualization and mobility within IT constrained environments. Barracuda NextGen Firewalls are a cornerstone of Barracuda's Total Threat Protection framework, which integrates purpose-built, best-of-breed, highly scalable security solutions to protect users, networks, and data centre applications. Components like web and email security, web application security, and secure remote access integrate with the X-series firewall. URL: https://www.barracuda.com/products/nextgenfirewall_x
Juniper UTM offering (SRX series)	Unified Threat Management (UTM) is an optional function for the branch SRX Series that provides an integrated suite of network security features to protect against multiple threat types including spam and phishing attacks, viruses, trojans and spyware infected files, unapproved website access, and unapproved content. URL: https://www.juniper.net/us/en/products-services/security/srx-series/

Table 8. Unified Threat Management key players and products

UTM market affinity to SMESEC

UTM seems like a candidate model for the SMESEC unified framework: UTM solutions basically integrate several different market solutions under a single umbrella, suitable for small organizations that cannot afford multiple, often hard-to-integrate security solutions. The characteristics of the products in this market can be a guide for the overall architecture of SMESEC unified framework.

4.1.5 Security Information and Event Management

Security Information and Event Management (SIEM) is a technology that enables the aggregation of data produced by multiple devices, network infrastructure, systems, and applications. Log data may be the primary source of information but SIEM systems are able to consume from other complex data structures. These characteristics, combined with other sources such as user directories, vulnerabilities, etc., allows SIEM systems to monitor systems and users as well as compliance to policies and standards (see online resources [46], [47]).

Key players:

HPE ArcSight SIEM	A comprehensive Security Information & Event Management (SIEM) solution that enables cost-effective compliance and provides advanced security analytics to identify threats and manage risk, so you can protect your business URL: https://software.microfocus.com/it-it/software/arcsight-

	express-siem-appliance
IBM QRadar	IBM® Security QRadar® SIEM consolidates log source event data from thousands of devices endpoints and applications distributed throughout a network. It performs immediate normalization and correlation activities on raw data to distinguish real threats from false positives. As an option, this software incorporates IBM Security X-Force® Threat Intelligence which supplies a list of potentially malicious IP addresses including malware hosts, spam sources and other threats. IBM Security QRadar SIEM can also correlate system vulnerabilities with event and network data, helping to prioritize security incidents. URL: https://www.ibm.com/ms-en/marketplace/ibm-qradar-siem
Intel Security SIEM (was McAfee Enterprise Security Manager – ESM)	McAfee SIEM solution brings event, threat, and risk data together to provide strong security intelligence, rapid incident response, seamless log management, and compliance reporting—delivering the context required for adaptive security risk management. At the core of the SIEM offering, McAfee Enterprise Security Manager delivers the performance, actionable intelligence, and real-time situational awareness required to identify, understand, and respond to stealthy threats, while the embedded compliance framework simplifies compliance. URL: https://www.mcafee.com/us/products/enterprise-security-manager.aspx
LogRythm	LogRhythm's security intelligence and analytics platform enables organizations to detect, prioritize and neutralize cyber threats that penetrate the perimeter or originate from within. URL: https://logrhythm.com/products/siem/
Splunk	Splunk's Security Intelligence Platform, consisting of Splunk Enterprise and the Splunk App for Enterprise Security, offers a sonar view of the sea of threats to your data. Comes as Splunk Enterprise, Splunk Cloud, or Splunk Light. URL: https://www.splunk.com/en_us/products/splunk-enterprise.html
SolarWinds SIEM	SolarWinds Log & Event Manager (LEM) software is a virtual appliance. SolarWinds positions LEM as an easy-to-deploy and use SIEM for resource-constrained security teams that have no requirements for big data advanced analytics or malware detection integration. LEM has integrations with SolarWinds' other products for operations monitoring to support activities such as change detection and root cause analysis. SolarWinds LEM is a good fit for small or midsize companies that require SIEM technology that is easy to deploy, and for those that use other SolarWinds operations monitoring components. URL: http://www.solarwinds.com/siem-security-information-event-management-software

EMC RSA SIEM	RSA NetWitness Logs and Packets goes beyond baseline SIEM capabilities. Designed for scale and heavy analytic loads, RSA NetWitness Logs and Packets will spot sophisticated attacks and will prioritize alerts. URL: https://www.rsa.com/en-us/products/threat-detection-and-response/rsa-netwitness-logs-packets

Table 9. Security Information and Event Management key players and products

SIEM market affinity to SMESEC

Undoubtedly, SIEM is a key component in a security solution, especially when multiple products are involved. The ability of SIEM products to ingest large amounts of heterogeneous data from several sources, correlate, create and visualize insights, makes it indispensable component in a security architecture. In SMESEC, there is one contributed product (ATOS XL-SIEM) which can assume this role.

4.1.6 Intrusion Detection and Prevention Systems (IDS/IPF)

Intrusion Detection/Prevention Systems implement threat deterrent technologies that monitor live network traffic to detect and prevent vulnerabilities based on a given set of rules (see online resources [48], [49], [50]).

Key players:

Cisco FirePower	The Cisco FirePOWER Next-Generation IPS (NGIPS) solution sets a new standard for advanced threat protection by integrating real-time contextual awareness, intelligent security automation and superior performance with industry-leading network intrusion prevention. URL: https://www.cisco.com/c/en/us/products/security/firesight-management-center/index.html
McAfee Network Security Platform (now IntelSecurity)	McAfee Network Security Platform is a next-generation intrusion prevention system (IPS) that redefines how organizations block advanced threats. Unlike traditional IPS solutions, it extends beyond signature matching with layered signature-less technologies that defend against never before seen threats. Intelligent workflows save time by isolating threat patterns, enabling security administrators to provide fast and accurate responses to network threats and breaches. URL: https://www.mcafee.com/us/products/network-security-platform.aspx
IBM Security Network Intrusion Prevention System	IBM® Security Network Intrusion Prevention System appliances are designed to stop constantly evolving threats before they impact your business. This means providing both high levels of protection and performance, while lowering the overall cost and complexity associated with deploying and managing a large number of point solutions. URL: https://www-01.ibm.com/software/security/products/network-ips/library/

Trend Micro	The TippingPoint Next-Generation Intrusion Prevention System (IPS) offers comprehensive threat protection against advanced and evasive targeted attacks with high accuracy. Using a combination of technologies such as deep packet inspection, threat reputation, and advanced malware analysis. It provides enterprises with a proactive approach to security. URL: https://www.trendmicro.com/en_us/business/products/network/integrated-atp/next-gen-intrusion-prevention-system.html
Huawei	Huawei's NIP6000 series is an advanced intrusion prevention system designed to provide application and service security for enterprises, IDCs, campus networks, and carriers. The NIP6000 series utilizes context, application, and content awareness to defend against unknown threats by implementing accurate detection and optimized management. URL: http://e.huawei.com/en/products/enterprise-networking/security/firewall-gateway/nip6000

Table 10. Intrusion Detection and Prevention System key players and products

IDS/IPS market affinity to SMESEC

As with SIEM, IDS/IPS systems are equally important components in a unified security architecture as they can detect and mitigate attacks in real time. IDS integration with other security systems can also give added-value to the whole security solution. In SMESEC, FORTH EWIS will have this role.

4.1.7 Distributed Denial-of-Service mitigation

Distributed Denial-of-Service (DDoS) refers to attacks from multiple sources to a single target in order to make it unable to provide a service by causing denial of service due to flooding by immense traffic. It directly affects the organization operations by denying access to legitimate users (see online resources [51], [52], [53])

Key players:

Cloudflare	CloudFlare's advanced DDoS protection, provisioned as a service at the network edge, matches the sophistication and scale of DDoS threats, and can be used to mitigate DDoS attacks of all forms and sizes including those that target the UDP and ICMP protocols, as well as SYN/ACK, DNS amplification and Layer 7 attacks. URL: https://www.cloudflare.com/ddos/
Arbor Networks	Arbor Cloud is a DDoS service powered by the world's leading experts in DDoS mitigation, together with the most widely deployed DDoS protection technology. URL: https://www.arbornetworks.com
Verisign	Verisign DDoS Protection Services help organizations reduce the risk of catastrophic DDoS attacks by detecting and filtering malicious traffic aimed at disrupting or disabling their internet-

	based services. Unlike traditional security solutions, Verisign DDoS Protection Services filter harmful traffic upstream of the organizational network or in the cloud. URL: https://www.verisign.com/en_US/security-services/ddos-protection/index.xhtml
Akamai	Kona Site Defender combines automated DDoS mitigation with a highly scalable and accurate WAF to protect websites from a wide range of online threats, including network- and application-layer DDoS, SQL injection and XSS attacks – without compromising the user experience. Kona Site Defender can stop the largest attacks and leverages Akamai's visibility into global web traffic to help organizations respond to the latest threats. URL: https://www.akamai.com/us/en/products/cloud-security/kona-site-defender.jsp
Imperva	The Imperva Incapsula service delivers a multi-faceted approach to DDoS defense, providing blanket protection from all DDoS attacks to shield your critical online assets from these threats. Incapsula DDoS protection services are backed by a 24x7 security team, 99.999% uptime SLA, and a powerful, global network of data centers. URL: https://www.incapsula.com
Level 3	Level 3 provides layers of defense through enhanced network routing, rate limiting and filtering that can be paired with advanced network-based detection and mitigation scrubbing center solutions. Our mitigation approach is informed by threat intelligence derived from visibility across our global infrastructure and data correlation. Tailored for any business and IT/security budget, our flexible managed service can proactively detect and mitigate the threats of today to help ensure business-as-usual for employees, partners and customers. URL: http://www.level3.com/en/products/ddos-mitigation/
F5	F5's DDoS Protection solution protects the fundamental elements of an application (network, DNS, SSL, and HTTP) against distributed denial-of-service attacks. Leveraging the intrinsic security capabilities of intelligent traffic management and application delivery, F5 protects and ensures availability of an organization's network and application infrastructure under the most demanding conditions. URL: https://f5.com/products/deployment-methods/silverline

Table 11. Distributed DoS protection key players and products

DDoS protection market affinity to SMESEC

Denial-of-Service attacks can have devastating effects to the normal flow of a business. Either on network, or on individual systems and services, a DoS attack will cause downtime which translates in financial losses. SMEs are normally less protected against this kind of threats, and sometimes they lack the technical expertise to overcome the results of such attacks. In SMESEC, CITRIX AppFirewall and Secure Web Gateway, and FORTH EWIS can help prevent this type of attacks.

4.1.8 Business Continuity / Disaster recovery

Business Continuity Management plans the crisis management processes though a configurable system to describe the business continuity needs, analyse the risks, create and test business continuity plans and initiate and manage the disaster recovery activities (see online resources [54], [55], [56], [57]).

Key players:

Fusion Framework System	The vendor's implementation size sweet spot is for organizations with 1,000 employees that want a strong customization capability as well as BCM program management. URL: https://www.fusionrm.com/fusion-framework-system
Global AlertLink	The product is offered in the following delivery models: on-premises, hybrid, dedicated hosted solution, and shared multitenant with a dedicated client application instance and dedicated client database instance. URL: http://globalalertlink.com
MetricStream	The product is offered in the following delivery models: on-premises, shared multitenant, dedicated client application instance and dedicated client database instance. A GRC vendor, it has moved into the BCMP space due to customer demand. Its implementation size sweet spot is for organizations with more than 5,000 employees that want a visualization. URL: https://www.metricstream.com
Sungard Availability Services	AssuranceCM is Sungard AS' replacement tool for LDRPS, which it will no longer market; however, it will support existing LDRPS customers as needed. AssuranceCM is offered in the following delivery model: shared multitenant with a dedicated client database instance per more than 300,000 employees and 15,000 recovery plans. This implementation was tied for the most complex implementation. Sungard AS is one of only two vendors that has plans to support IoT implementation size sweet spot is for organizations with more than 1,000 employees that want a BCM planning tool based on the latest technology, and with a brand new and very committed product team. URL: https://www.sungardas.com/en/
Continuity Logic	The product is offered in the following delivery models: hybrid, shared multitenant, dedicated client application instance and dedicated client database instance. Continuity Logic had the second most complex implementation based on the number of employees, implementation size sweet spot is for organizations

	with more than 5,000 employees that want strong BCM program management, C/IM and visualization. URL: http://www.continuitylogic.com
Strategic BCP	The product is offered in the following delivery models: hybrid, dedicated client application instance and dedicated client database instance. Its implementation size sweet spot is for organizations with more than 5,000 employees that want strong BCM planning, BCM program management and C/IM functionality. URL: http://www.strategicbcp.com
EMC	Archer Business Continuity Management: The product is offered in the following delivery models: on-premises and shared multitenant. URL: https://www.rsa.com/en-us/resources/rsa-archer-business-continuity-and-it-disaster-recovery-planning

Table 12. Disaster Recovery key players and products

Disaster Recovery and Business Continuity market affinity to SMESEC

Closely related to GRC, this market offers some formalized solutions that describe the plans of recovering after an attack and keeping business operations as smooth as possible. There is no related product currently in SMESEC, but the principles and key characteristics of the products in this segment can influence the decisions for the unified architecture (as in GRC).

4.1.9 Web Application Firewall

Web Application Firewall differ from the typical firewall as they focus mainly on protecting the web traffic (HTTP protocol) from a variety of attacks, such as Cross-Site Scripting (XSS), SQL injection, etc. WAFs are able to inspect the payload of the HTTP traffic and decide if this is legit, and provide input to other tools like SIEMs (see online resource [58])

Key players:

Imperva	Imperva SecureSphere Web Application Firewall analyzes all user access to your business-critical web applications and protects your applications and data from cyber-attacks. SecureSphere Web Application Firewall dynamically learns your applications' "normal" behavior and correlates this with the threat intelligence crowd-sourced from around the world and updated in real time to deliver superior protection. URL: https://www.imperva.com/Products/WebApplicationFirewall-WAF
DenyAll	It combines ease of configuration – with its workflow engine and management APIs – with a proven ability to secure web applications. It embeds negative and positive security, in-context, user behavior analysis, and soon-to-be added web advanced

	security engines, to efficiently protect your web applications while minimizing false positives. URL: https://www.denyall.com
Citrix	NetScaler AppFirewall prevents inadvertent or intentional disclosure of confidential information and aids in compliance with information security regulations such as PCI-DSS. URL: https://www.citrix.com/products/netscaler-appfirewall/
F5	BIG-IP Application Security Manager: It is an on-premises web application firewall (WAF), deployed in more data centers than any enterprise WAF on the market. With advanced firewall capabilities, it secures applications against layer 7 distributed denial-of-service (DDoS) attacks and application vulnerabilities where other WAFs fail. URL: https://f5.com/products/big-ip/application-security-manager-asm
Trustwave	With a unique combination of positive and negative security, perpetual tuning and dynamic virtual patching, the Trustwave Web Application Firewall delivers continuous protection against today's ever-changing threat landscape. Bi-directional traffic analysis, automated behavioral profiling, and multiple collaborative detection engines help you and your team to quickly identify abnormal behavior, improve threat blocking and prevent outbound data leaks. URL: https://www.trustwave.com/Products/Application-Security/Web-Application-Firewall/
Barracuda Networks	Barracuda Web Application Firewall is the ideal solution for organizations looking to protect web applications from data breaches and defacement. With the Barracuda Web Application Firewall, administrators do not need to wait for clean code or even know how an application works to secure their applications. Organizations can ensure robust security with a Barracuda Web Application Firewall hardware or virtual appliance, deployed either on-premises or in the cloud. URL: https://www.barracuda.com/products/webapplicationfirewall

Table 13. Web Application Firewall key players and products

WAF market affinity to SMESEC

A lot of today's business depends on web applications: web applications today are far more popular due to the platform independency and easy-of-deployment. The evolution of clouds also made much easier the offering of web applications. Web Application Firewalls protect these valuable applications, and alone or in conjunction with other offerings (such as DDoS), prevent attacks that focus the applications themselves, or other dependant assets (e.g. database backends). In SMESEC, CITRIX contributed AppFirewall product can cover this space.

4.1.10 Secure Web Gateways (SWG)

Secure Web Gateways protect company assets while surfing and enforce the policy companies to the network traffic. They may offer a range of capabilities, including URL filtering, antivirus/antimalware protection, SSL traffic inspection, etc. (see online resources [59], [60], [61])

Key players:

Symantec ProxySG (previously Blue Coat)	Blue Coat Secure Web Gateway consolidates a broad feature-set to authenticate users, filter web traffic, identify cloud application usage, provide data loss prevention, deliver threat prevention, and ensure visibility into encrypted traffic. URL: https://www.symantec.com/products/secure-web-gateway-proxy-sg-and-asg
Zscaler Web Security	Zscaler Web Security provides unmatched security, visibility and control, going beyond the basics of web content filtering. Delivered in the cloud, Zscaler includes award-winning web security integrated with our robust network security platform that features advanced threat protection, real-time analytics and forensics. URL: https://www.zscaler.com/solutions/web-security
ForcePoint TRITON AP-WEB	TRITON AP-WEB stops more advanced, non-signature threats to your data than any other solution. Insider threats – such as employee theft and malware that slips into your network– are just as dangerous as external ones. TRITON AP-WEB is built on a unified platform that enables all of our products to work together and provides industry-leading reporting, sandboxing and DLP capabilities. TRITON AP-WEB is the proven leader in preventing data loss, whether deployed in the Cloud, hybrid or on-premises. URL: https://www.forcepoint.com/product/cloud-security/forcepoint-web-security
Cisco Web Security Appliance	Get advanced threat defense, advanced malware protection, application visibility and control, insightful reporting, and secure mobility. The Cisco Web Security Appliance (WSA) combines all of these forms of protection and more in a single solution. URL: https://www.cisco.com/c/en/us/products/security/web-security-appliance/index.html
McAfee Web Gateway	McAfee Web Gateway delivers high-performance web security through an on-premises appliance that can be deployed both as dedicated hardware and a virtual machine. URL: https://www.mcafee.com/us/products/web-gateway.aspx

Table 14. Secure Web Gateway key players and products

SWG market affinity to SMESEC

Secure Web Gateways can offer a wide range of protections for web traffic, covering not only incoming but outgoing traffic as well. Characteristics such as URL filtering or anti-malware protection can help into preventing malicious content and code entering the organization. The ability to inspect secure traffic makes it also attractive as much of the malware can be transported over secure web connections that otherwise pass uninspected. CITRIX SWG integration to SMESEC will be able to provide such capabilities to the unified framework.

4.1.11 Endpoint security (EPS) / Endpoint Protection Platforms (EPP)

Endpoint Protection Services (EPS) is about protecting endpoints (workstations, servers, mobile devices, etc.) from viruses, trojans, spyware, malware, phishing, etc. (see online resources [62], [63], [64]).

Some of the areas that may be covered by an EPP solution are:

- Anti-virus / Anti-malware
- Personal firewall
- Port and device control
- Memory protection
- Application control
- Data protection (encryption)
- Data loss prevention

Key players:

Sophos Endpoint Protection	Sophos Endpoint Protection makes it simple to secure your Windows, Mac, and Linux systems against malware and advanced threats, such as targeted attacks. URL: https://www.sophos.com/en-us/products/endpoint-antivirus.aspx
Trend Micro	Trend Micro endpoint security gives you the threat protection and data security you need to protect your users and your corporate information across every device and application URL: https://www.trendmicro.com/en_ca/business/products/user-protection/sps/endpoint.html
Webroot	Webroot SecureAnywhere Endpoint Protection leverages cloud-based real-time intelligence to protect organizations against ever-evolving threats. URL: https://www.webroot.com/us/en/business/smb/endpoint-protection
BitDefender	GravityZone Endpoint Security: Bitdefender provides the highly scalable endpoint security solution that businesses require to protect against malware and web threats. URL: https://www.bitdefender.com/business/security.html
Symantec	Symantec Endpoint Protection: Proactively detect and block today's most advanced threats with an endpoint protection solution that goes beyond antivirus.

	URL: https://www.symantec.com/products/endpoint-protection
Kaspersky Lab	World-class security for all your endpoints – including laptops, desktops, file servers and mobile devices. Advanced security for workstations & file servers. Multi-layer mobile security and management. Application Control, Device Control & Web Control. Centralized management console for all functions. URL: https://www.kaspersky.com/small-to-medium-business-security/endpoint-windows
Microsoft	Microsoft System Center 2012 Endpoint Protection provides an antimalware and security solution for the Microsoft platform. URL: https://msdn.microsoft.com/en-us/library/hh546785(v=sc.12).aspx
Intel Security	Intel Security enterprise endpoint security solutions are centrally managed and defend against the full threat spectrum from zero-day exploits to advanced targeted attacks, protecting Windows, Macs, and Linux systems. URL: https://www.mcafee.com/us/products/endpoint-protection/index.aspx
F-Secure	Going beyond malware protection, F-Secure provides end-point protection and security management solutions. URL: https://www.f-secure.com/en/web/business_global/products

Table 15. Endpoint Protection key players and products

EPP market affinity to SMESEC

EPP is one of the traditional markets in terms of awareness, as antivirus solutions used to be present in SME environments several years ago. The more complicated nature of viruses and malware today, in general has made this market solutions even more necessary, and the integration with other security products is definitely an advantage when it comes to the prevention from this kind of threats. BD GravityZone product in SMESEC will cover the endpoint protection field.

4.1.12 Application Security Testing

Application Security Testing help developers, administrators, and enterprises identify security vulnerabilities by performing exhausting testing on various aspects of the software [65]. It may be also categorized as:

- Static Application Security Testing (SAST): Essentially white box testing, which allows the source code to be examined for vulnerabilities
- Dynamic Application Security Testing (DAST): Black box testing by running the software under many different environments and inputs without access to source code.
- Run-time Application Security Protection (RASP): Testing by examining the runtime environment of the application (e.g. JVM) using instrumentation.

- Interactive Application Security Testing (IAST): This is a combination of SAST and RASP, allowing users to check various attack scenarios and the effect on the runtime environment.
- Mobile Application Security Testing (Mobile AST): Combination of SAST, DAST and behavioral analysis using static and dynamic techniques to identify

Key players

IBM	IBM Security AppScan Standard helps organizations decrease the likelihood of web application attacks and costly data breaches by automating application security vulnerability testing. IBM Security AppScan Standard can be used to reduce risk by permitting you to test applications prior to deployment and for ongoing risk assessment in production environments. URL: http://www-03.ibm.com/software/products/en/appscan-standard
WhiteHat Security	WhiteHat Sentinel is a Software-as-a-Service (SaaS) platform that enables your business to quickly deploy a scalable application security program across the entire software development lifecycle (SDLC). Combining advanced scanning technology with the world's largest application threat research team, WhiteHat Security accurately identifies the enterprise vulnerabilities and scale to meet any demand. URL: https://www.whitehatsec.com/resources/whitehat-sentinel-product-family-abridged/
Veracode	Veracode product family includes Binary Static Analysis (SAST), Web Application Perimeter Monitoring, Dynamic Analysis (DAST), Mobile Application Security, Vendor Application Security. URL: https://www.veracode.com
HPE	Fortify on Demand is an application security testing and program management solution that enables customers to easily create, supplement and expand a software security assurance program through a managed service dedicated to delivery and customer support. URL: https://www.hpe.com/h20195/V2/getpdf.aspx/4AA4-1164ENW.pdf

Table 16. Application Security Testing key players and products

AST market affinity to SMESEC

Application Security Testing is usually an operation that does not run in the front-line, but a careful testing of a hardware or software applications before deployment can prevent future attacks. Testing can take place even before deployment, but also while a product has been deployed, providing continuously feedback. Another possible benefit will be enriching tests with even more attack scenarios and consuming this information in an automated manner. EGM TaaS product will have a key role in SMESEC position in this market.

4.1.13 Security Awareness and Training

Users are usually the weakest point in security. Either by their online behaviour (e.g. browsing malicious sites, unwittingly disclosing sensitive information, fall prey to social engineering attacks, etc.), or by bringing into the infrastructure infected devices (e.g. laptops, etc.). They impose a serious risk in the organization security plans.

A number of companies are focusing on increasing security awareness and educating employees and users in general on security aspects and best practices for their everyday online habits (see online resource [66])

Key players:

SANS Securing the Human	SANS Securing The Human provides security awareness training and security awareness programs for cybersecurity awareness professionals around the world. Securing The Human offers industry leading security awareness classes, tools and resources so that security awareness officers can easily and effectively manage their human cybersecurity risk. The SANS Securing The Human program includes all the training, tools, guidance and support security awareness officers need to simply and effectively build a best-in-class program. URL: https://securingthehuman.sans.org/security-awareness-training/overview
The Wombat security education platform	The Wombat Security Education Platform is an integrated Saas-based platform that delivers the Wombat products that you select as part of your customized security awareness and training program. From knowledge assessments and mock phishing attacks, to scheduling interactive training, running reports and reviewing dashboards – Wombat Security Education Platform allows the enterprise to easily run and monitor its program all from one place. Access all of the components of Wombat Continuous Training Methodology that has been shown to reduce successful phishing attacks and malware infections up to 90%. URL: https://www.wombatsecurity.com
PhishMe Simulator	PhishMe Simulator uses industry-proven behavioral conditioning methods to better prepare employees to recognize and resist malicious phishing attempts–transforming one of your biggest liabilities into your strongest defense. URL: https://phishme.com
Mediapro Security Awareness	An Adaptive Security Awareness Program continually improves and adapts with you, as your risks and threat vectors change. It provides you a highly flexible architecture to adjustment your awareness program, on a continual basis, to achieve the maximum results possible for the effort and dollars expended. URL: https://www.mediapro.com

Table 17. Security Awareness key players and products

Security Awareness and Training market affinity to SMESEC

Though not a directly technical market, security awareness market is key for defending against the most critical threat which is the human factor. As part of SMESEC, various security awareness activities will take place, so a study on the offerings of the professionals in this market can help identify what is needed for the effective training of SME employees.

4.2 Emerging markets and key players

4.2.1 Introduction

A number of emerging markets has been identified by top analysts. These markets, although already present today, offer a lot of potential (and grow) in the years to come. Some characteristics of these new markets include:

- The introduction of intelligent methods of detecting/mitigating attacks, rather than a rule or signature-based approach
- Behaviour analysis and user profiling
- A centralized way of collecting, correlating and extracting intelligence from multiple endpoints, providing higher level of confidence for the risks than individual indications.

These markets also present a lot of interest for innovative solutions in the SMESEC framework by introducing bleeding-edge features. Some of the key players in these markets and a short description of their products follow in the following sections.

4.2.2 Deception technology

Deception technology is an emerging market segment in cybersecurity. The main goal of deception technology solutions is the deployment of several decoys in parts of the infrastructure that are indistinguishable with the real servers. If an attacker managed to gain access, the decoys are the easiest targets and quickly notify and trigger appropriate actions against the intruder (see online resources [67], [68])

Key players:

Illusive networks	Illusive Networks is a cyber security firm headquartered in Tel Aviv, Israel. Illusive Network's "Deceptions everywhere" lays out a deceptive layer over the enterprise entire network. The decoys can be data, servers, applications, devices and hosts. The moment the attacker steps onto one of the decoys, he/she is seamlessly transferred to a virtual network separate from enterprise network and investigations and forensics follows. URL: https://www.illusivenetworks.com
Attivo networks	Attivo networks, founded in 2011 and headquartered in Fremont, CA, US, offers a deception based threat detection platform. Attivo network "Threat Matrix Platform" checks all the right boxes and is packed of features that a modern-day deception technology

	should have. URL: https://attivonetworks.com
Smokescreen	Smokescreen's IllusionBLACK deception platform detects cyber-attacks like reconnaissance, spear phishing, lateral movement, stolen credentials and data theft. IllusionBLACK features rapid out-of-band deployment, no performance impact, enterprise scalability, and minimal false positives, leading to faster breach detection and improved security and incident response team productivity. URL: https://www.smokescreen.io/IllusionBLACK/
TrapX	TrapX is a cyber security company founded in 2010 and headquartered in California, US. TrapX "Deception grid" platform provides deception based advance threat defense solution. TrapX has a number of out-of-box use cases for detecting zero-day malware, ransomware and attacks through compromised accounts. URL: https://trapx.com/product/
Cymmetria	Cymmetria, founded in 2014 and headquartered in California, US, has a deception platform called "Mazerunner". Mazerunner intercepts the attacker during the reconnaissance phase and carefully lead them to a monitored deception network where they are analyzed for their tactics, techniques and procedures employed for attacking the enterprise. Mazerunner can be deployed as a virtual appliance and require minimal effort in deployment. URL: https://cymmetria.com/product/
Acalvio	Acalvio provides Advanced Threat Defense (ATD) solutions to detect, engage and respond to malicious activity inside the enterprise networks. Acalvio holds patents in deception and data science and have developed their product "Deception2.0" around that. Acalvio is founded in 2015 and headquartered in California, USA. URL: http://www.acalvio.com

Table 18. Deception Technology key players

Deception technology market affinity to SMESEC

The role of deceptive technology will become vital in the years to come. Solutions that can take the threat away from the sensitive assets of an infrastructure and will contain the threat there are needed as networks and systems become more and more complicated, and maintenance comes more of a burden. IBM AntiROP solution will help SMESEC framework protect applications that become often attack targets.

4.2.3 Endpoint Detection and Response (EDR)

Endpoint Detection and Response is the next step in Endpoint Protection Platforms (EPP). Typically, EDR involves the detection and mitigation to a more sophisticated process including detection, analytics and prioritization of incident response (see online resources [69], [70])

Key players:

Carbon Black	Carbon Black Enterprise Response is the most complete endpoint detection and response solution available to security teams who want a single platform for hunting threats, disrupting adversary behaviour and changing the economics of security operations. Only Carbon Black Enterprise Response continuously records all endpoint activity, centralizes and correlates that data with unified intelligence sources, and reveals a complete kill chain that pinpoints attack root cause to power live threat containment, banning and remediation activities. Built entirely on open APIs, Carbon Black Enterprise Response pushes and pulls data through the security infrastructure to automate and enhance adaptive threat response processes, helping to make it the #1 EDR solution among global enterprises and 70+ of the world's leading IR and MSSP firms. URL: https://www.carbonblack.com
Cisco	Cisco Advanced Malware Protection (AMP) is a security solution that addresses the full lifecycle of the advanced malware problem. It can not only prevent breaches, but gives you the visibility and control to rapidly detect, contain, and remediate threats if they evade front-line defences - all cost-effectively and without impacting operational efficiency. URL: https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html
CrowdStrike	CrowdStrike™ is a leading provider of next-generation endpoint protection, threat intelligence, and pre- and post incident response services. CrowdStrike Falcon is the first true Software as a Service (SaaS) based platform for next-generation endpoint protection that detects, prevents, and responds to attacks, at any stage - even malware-free intrusions. Falcon's patented lightweight endpoint sensor can be deployed to over 100,000 endpoints in hours providing visibility into billions of events in real-time. CrowdStrike operates on a highly scalable subscription-based business model that allows customers the flexibility to use CrowdStrike-as-a-Service to multiply their security team's effectiveness and expertise with 24/7 endpoint visibility, monitoring, and response. URL: https://www.crowdstrike.com
FireEye	The FireEye Endpoint Threat Prevention for the FireEye Security Platform — HX Series was developed by Mandiant consultants for use during an incident response or compromise assessment.

	The management system consists of a hardware appliance that is installed in the primary network and an optional appliance that can be installed into the DMZ for managing off network endpoints. URL: https://www.fireeye.com/products/hx-endpoint-security-products.html
Guidance Software	EnCase Endpoint Security: Mitigate Threats, Maximize Productivity Enterprises demand EDR products to offer scalability, strong detection and incident response workflows, and open integrations to operate more efficiently. EnCase Endpoint Security v6 was designed to not only meet these needs, but then exceed them with a beautifully redesigned front-end user interface. The completely redesigned EnCase Endpoint Security v6 delivers improved performance, better usability, and enhanced capabilities. Moving to the newest version of EnCase Endpoint Security has never been easier or more exciting URL: https://www.guidancesoftware.com
RSA	RSA ECAT is a continuous endpoint solution providing contextual visibility beyond a single alert to provide incident responders and security analysts a full attack investigation platform to detect and respond in real-time against advanced attacks, known and unknown as well as malware and non-malware threats. URL: https://www.rsa.com/en-us/products/threat-detection-and-response/endpoint-threat-detection-and-response
Symantec	Symantec™ Advanced Threat Protection: Endpoint is a new solution to uncover, prioritize, and remediate advanced attacks across all of your endpoints, leveraging existing investments in Symantec™ Endpoint Protection. With one click of a button, you can search for, discover, and remediate any attack artifacts across all of your endpoint systems. And, if you have Symantec™ Advanced Threat Protection: Network or Symantec™ Email Security.cloud, Symantec's Synapse™ correlation technology will automatically aggregate events across all Symantec-protected control points to prioritize the most critical threats in your organization. URL: https://www.symantec.com/products/advanced-threat-protection
Tanium	Tanium gives the world's largest enterprises and government organizations the unique power to secure, control and manage millions of endpoints across the enterprise within seconds. Serving as the "central nervous system" for enterprises, Tanium empowers security and IT operations teams to ask questions about the state of every endpoint across the enterprise in plain English, retrieve data on their current state and execute change as necessary, all within seconds. With the unprecedented speed,

	scale and simplicity of Tanium, organizations now have complete and accurate information on the state of endpoints at all times to more effectively protect against modern day threats and realize new levels of cost efficiency in IT operations. URL: https://www.tanium.com

Table 19. Endpoint Detection and Response key players and products

EDR market affinity to SMESEC

EDR comes as an evolution of EPP, and in fact there is some confusion over the exact borders of each market. However, the characteristics of the EDR products can be a driver for extending the capabilities of SMESEC EPP products, either directly, or by product synergies that will eventually provide EDR capabilities.

4.2.4 Cloud Access Security Brokers (CASB)

Cloud Access Security Brokers (CASB) have appeared in an era where cloud applications become more and more an integral part of the organization workflows. Cloud applications still manage corporate data but run on a not-owned infrastructure. CASBs provide the common access policies from any corporate device (computer, mobile, etc.) to any cloud application. The primary focus of CASBs are SaaS back-office services, such as CRM, file sharing, HR, etc. (see online resources [71], [72], [73])

Key features are visibility, compliance, data security and threat protection.

Key players:

Bitglass	Bitglass Standard Edition provides Total Data Protection, enabling enterprises to adopt the cloud apps that their business needs, securing corporate data anywhere it goes—in the cloud, on devices, at the point of access, and on the corporate network. URL: https://www.bitglass.com/
CensorNet	CensorNet is one of the newer entrants into the CASB market, and its CASB offering complements its existing email and web security products. It also recently acquired a two-factor authentication company (SMS Passcode) to complement its product portfolio. Based on its existing SWG platform, CensorNet is already positioned to capture traffic and see the flow of data to and from SaaS applications. Like most SWGs, CensorNet is based on a forward-proxy architecture, using on-premises physical/virtual appliances. It now also has a cloud-delivered option. CensorNet can also support deployments of the technology in the cloud. The initial offering is focused on visibility and SaaS application user and policy control, and has improved in the past year to deliver more capabilities to a larger number of cloud services. URL: https://www.censornet.com/

CipherCloud	It eliminates cloud security issues by delivering a single solution to secure sensitive customer information across all of your cloud applications, while preserving usability, functionality and performance. Available as a service or virtual appliance, CipherCloud delivers a comprehensive set of protection controls including encryption, tokenization, activity monitoring, data loss prevention (DLP) and malware detection that can overcome your cloud security concerns. URL: https://ciphercloud.com/
Cisco CloudLock	CloudLock focuses on the Shadow IT challenge that matters – those cloud and third-party apps that directly connect into your corporate environment. CloudLock gives you control to decide which apps lead to productivity gains and which ones are a security risk to your organizations. URL: https://www.cisco.com/c/en/us/products/security/cloudlock/index.html
FireLayers	The FireLayers Secure Cloud Application Platform delivers full control over homegrown and popular apps like Salesforce, Office 365, SuccessFactors, NetSuite and endless others. Its Secure Cloud Application Platform, which features risk-based authentication, threat detection and prevention, empowers enterprises with new levels of security, visibility and control across their cloud resources. URL: https://www.proofpoint.com/us
Imperva	Imperva Skyfence Cloud Gateway is a cloud access security broker that provides visibility and control over sanctioned and unsanctioned cloud apps. Organizations can use this cloud security service to discover SaaS applications in use and assess related risks. URL: https://www.imperva.com/
Adallom (now Microsoft)	Cloud access security broker Adallom announced that its cloud application security platform is now available as part of the HP Enterprise Security Products and HP Enterprise Services portfolios. As the adoption of applications like Salesforce, Office 365, and Google Apps for Work continues to grow, one of the biggest challenges for IT organizations is how to secure sensitive corporate data that is now in the cloud. URL: https://www.microsoft.com/en-us/cloud-platform/cloud-app-security
NetSkope	The Netskope Active Platform take cloud app analytics to new level and shows you details about how all cloud apps are being used, not just the ones you sanction. Find out specifics like “Who is sharing content outside of the company from any cloud storage app?” and enforce granular policies like “Don’t let anybody upload PCI to any finance cloud app except for our sanctioned one.” URL: https://www.netskope.com/

Palerra LORIC (now Oracle)	Palerra enables organizations to protect business-critical cloud infrastructure and data with LORIC™, the cloud security automation platform. LORIC is delivered as a service and can be deployed in minutes. URL: https://www.oracle.com/cloud/paas/casb-cloud-service.html
Palo Alto Networks	Aperture extends the visibility and granular control of our security platform into SaaS applications themselves – an area traditionally invisible to IT. Aperture solves this problem by looking into SaaS applications directly, providing full visibility into the day-to-day activities of users and data. Granular controls ensure policy is maintained to eliminate data exposure and threat risks. URL: https://www.paloaltonetworks.com/products/secure-the-cloud/aperture
Skyhigh Networks	Skyhigh Cloud Security Manager enables IT to embrace and accelerate the adoption of cloud services while ensuring privacy, security, and compliance. URL: https://www.skyhighnetworks.com/
Blue coat (now Symantec)	The Blue Coat Cloud Data Protection Gateway is a software solution that delivers critical data privacy and security capabilities to users of public cloud applications. URL: https://www.symantec.com/products/cloud-application-security-cloudsoc

Table 20. Cloud Access Security Broker key players and products

CASB market affinity to SMESEC

Currently there is no direct CASB product capability in SMESEC, but given the emerging phase of this market and the move of SMEs towards cloud infrastructure, it becomes apparent that CASB will be a possible unified framework requirement. If cloud is in the mix, minimizing the risk and Internet exposure for on-premises-to-cloud communication, and making the integration seamless can be a great advantage to SMEs.

4.2.5 User Entity Behaviour Analytics (UEBA)

User Entity Behaviour Analytics technology is an evolvement of the SIEM technology. The main differences from SIEM are: (i) use of advanced analytics and machine learning methods, (ii) has more focused inputs (e.g. user directories, other tools outputs, etc.) (iii) they build profiles for every user or entity they monitor and watch for abnormal behavior, and (iv) has a more detailed field of application, i.e. it may not be able to apply to all use cases that SIEM can (see online resources [74], [75], [76]).

Key players:

Exabeam	Exabeam user behaviour intelligence solution helps organizations tackles challenges like external/internal threats and data theft by applying the advancements in data science to cyber-security. The product is built on a big data platform and performs behavioural

	analytics and risk scoring to determine any malicious activity. URL: https://www.symantec.com/products/cloud-application-security-cloudsoc
Gurucul	Gurucul’s user behaviour analytics and identity access intelligence technology uses machine learning and predictive anomaly detection algorithms to reduce the attack surface for accounts, unnecessary access rights and privileges, and identify, predict and prevent breaches. URL: https://gurucul.com/
Fortscale	Fortscale UEBA uses unsupervised machine learning algorithms to provide user and entity profiling and anomaly detection. Fortscale can ingest myriad sources of data and has inbuilt forensics and investigation capabilities. URL: https://fortscale.com/
Redowl	RedOwl uses a mix and match advance and basic analytics, such as, statistical pattern matching, machine learning and content analytics to profile user behaviour, and identify anomalous user activity. RedOwl UBA solution can ingest both structured and unstructured data formats and has multiuse cases out-of-the box. URL: https://redowl.com/
Niara (now HPE Aruba Introspect)	Niara security analytics platform utilizes both supervised and unsupervised machine learning for behavioural profiling of user and entities. It ingests data sources such as network packets, log data from hosts, application and other security products such as SIEM, DLP and WAF. Niara security analytics platform can be deployed on-premise or can be cloud based. URL: https://www.niara.com/

Table 21. User Entity and Behaviour Analytics key players and products

UEBA market affinity to SMESEC

As networks and systems become more complicated, KPIs or other raw information becomes excessive to handle. The need for more advanced techniques that can study the behaviour of systems, applications or users is becoming very important, and profiling the sources of risk can prevent threats much before they take place. No SMESEC product is currently in this area, but the study of the characteristics of some UEBA products can drive the development of the architecture, or provide the necessary hooks for integration with third-party UEBA vendors.

4.2.6 Identity and Access Management

Identity and Access Management (IAM) is the process of managing digital identities, and access rights to enterprise resource and auditing in an automated manner. As organizations integrate with third party software (e.g. CRM, HR, etc.) it becomes vital to ensure that identity authentication is properly handled without posing threats to the overall organization security infrastructure. IAM are centralized management systems that consolidate the processes of authentication and auditing providing a single framework for access (see online resources [77], [78])

Main goals in IAM are:

- Multi-factor authentication schemes
- Integration with directory services (LDAP, Active Directory, etc.)
- Single Sign-On (SSO)
- Credentials management
- Auditing
- Analytics

Key players:

IBM	IBM® Security Identity and Access Manager provides automated and policy-based user lifecycle management and access controls throughout the enterprise. Available as an easy-to-manage virtual appliance, it pairs IBM Security Identity Manager with IBM Security Access Manager Platform for more secure user authentication and authorization to applications and data. Organizations can use IBM Identity and Access Manager to better administer, secure and monitor user access privileges and activities for enterprise and online environments. URL: http://www-03.ibm.com/software/products/sr/identity-access-manager
Oracle	Oracle's complete, integrated next-generation identity management platform provides breakthrough scalability with an industry-leading suite of identity management solutions. Reduce operational costs. Achieve rapid compliance with regulatory mandates. Secure sensitive applications and data—regardless of whether they are hosted on premises or in the cloud. URL: http://www.oracle.com/technetwork/middleware/id-mgmt/overview/index.html
Sailpoint	IdentityIQ® is SailPoint's governance-based identity and access management (IAM) software solution that delivers a unified approach to compliance, password management and provisioning activities for applications running on-premises or from the cloud. IdentityIQ meets the needs of large organizations with complex identity management processes who prefer to tailor their solution to align with unique business needs. URL: https://www.sailpoint.com/identity-management-software-identityiq/
Okta	The Okta identity management service provides directory services, SSO, strong authentication, provisioning, workflow, and reporting, all delivered as a multitenant IDaaS though some components reside on-premise. URL: https://www.okta.com

RSA	RSA offers both RSA Identity Management and Governance (RSA IGA), a full-fledged identity management suite built from separately licensed components, and RSA VIA, an IDaaS suite composed of separately licensed SAAS point solutions. URL: https://www.rsa.com/en-us/products/rsa-securid-suite

Table 22. Identity and Access Management key players and products

IAM market affinity to SMESEC

The core idea of IAM is the existence of some common user authentication service that not only allows access, but also audits the use of assets and reports possible malicious events. It also allows the correlation of events from multiple sources to single users through the common directory service. SMESEC does not have an offering in this field, however the study of the capabilities of IAM offerings can help SMESEC understand what should be needed to effectively handle the identifications of users and the correlation to specific access events.

5 Technology Stack

This section summarizes the basic technical characteristics that the SMESEC products are offering. The main aim is to identify those properties of the products that will help better understand the capabilities they offer with regard to the SMESEC pilot use case requirements.

5.1 Introduction

In this overview, the technical characteristics and system requirements for the products that are contributed by the SMESEC partners are covered:

Partner	Product
ATOS	XL-SIEM
BitDefender	GravityZone
CITRIX	NetScaler AppFirewall, NetScaler Gateway, NetScaler Secure Web Gateway
EGM	Tool-as-a-Service
FHNW	Adherence Monitor & SUPERCEDE framework
FORTH	Early Warning Intrusion Detection System (EWIS) & Cloud IDS
IBM	AngelEye, ExpliSAT, AntiROP

Table 23. SMESEC product list

The analysis is performed on the following criteria:

- Security market: where each product is positioned according to the markets segments of Section 4.
- Hardware and software characteristics: what are the running requirements of each individual product.
- Cloud readiness: whether the product is able to run in a public or private cloud environment
- Inputs and Outputs: what does each program read as input and what output it produces – useful for considering integrating options.
- Endpoint protection: what kind of devices/service are protected by the product.
- Reporting and analytics: what are the reporting capabilities and what insights it provides.
- Risk assessment: whether it helps assessing the risk.

5.2 Security market

Currently, in SMESEC the contributed products cover a wide variety of segments, as they have been covered in the previous section. The "market" to which each tool belongs is described in Section 4.

Product name	Security Areas	Market
ATOS XL-SIEM	Security Information and Event Management	SIEM
BD GravityZone	Anti-virus / Anti-malware	EPP, EDR
CITRIX AppFirewall	Firewall	WAF, DDoS
CITRIX Gateway	VPN	EPP, USG
CITRIX Secure Web Gateway	SSL interception, URL filtering	USG, SWG
EGM Test-as-a-Service (TaaS)	Testing	AST
FHNW Adherence Monitor & SUPERCEDE framework	Security Readiness Evaluation	GRC
FORTH EWIS & Cloud	Intrusion Detection/Prevention Systems	IDS/IPS
IBM Angel-Eye	Virtual patching	AST
IBM ExpliSAT	Software formal verification tool	AST
IBM Anti-ROP	Anti-ROP solution	Deception Technology

Table 24. SMESEC products by market segment

Current SMESEC products cover a good percentage of the security market (12 segments as identified in Section 4) and the security solution provided are expected to fit most of SME needs. It should be noted that as part of the innovation process, some products may touch new market segments.

5.3 Hardware requirements

The hardware requirements of the SMESEC products follow. Table 25 shows the basic hardware characteristics: hardware architecture required RAM and required disk space.

Product name	Architecture	RAM	Disk
ATOS XL-SIEM	x86_64	16GB (recomm. 24GB)	(not specified)

BD GravityZone	Most	(not specified)	(not specified)
CITRIX AppFirewall	Hypervisor	2GB (recomm. 4GB)	Min 16GB
CITRIX Gateway	Hypervisor	2GB (recomm. 4GB)	Min 16GB
CITRIX Secure Web Gateway	Hypervisor	2GB (recomm. 4GB)	Min 16GB
EGM Test-as-a-Service (TaaS)	(not specified)	4GB	40GB
FHNW Adherence Monitor & SUPERCEDE framework	(not specified)	4GB	8GB – 2TB
FORTH EWIS & Cloud	x86_64	4GB	Est. 1.5TB/yr
IBM Angel-Eye	x86_64	1GB	Online 500MB
IBM ExpliSAT	(not specified)	20GB	Depends
IBM Anti-ROP	(not specified)	(not specified)	(not specified)

Table 25. SMESEC product hardware requirements

Conclusions:

- Most SMESEC products can run with a minimum of 4GB RAM and around 20GB of disk space (each). This means a quite reasonable memory/disk footprint for deployments.
- Systems that require more RAM handle either large volumes of data and could probably run in a centralized manner.

5.3.1 Virtualization & Containerization

Another consideration, related to hardware requirements, was the ability to run in virtualized environments and/or containers. Table 26 summarized the findings.

Product name	Hypervisor	Containers
ATOS XL-SIEM	✔ VirtualBox, XenServer	-
BD GravityZone	✔ VMware ESXi, Citrix Xen, Microsoft Hyper-V, Nutanix, Red Hat KVM and Oracle VM	-

CITRIX AppFirewall	✔ XenServer, Vmware, Hyper-V, KVM	✔
CITRIX Gateway	✔ XenServer, Vmware, Hyper-V, KVM	✔
CITRIX Secure Web Gateway	✔ XenServer, Vmware, Hyper-V, KVM	✔
EGM Test-as-a-Service (TaaS)		✔
FHNW Adherence Monitor & SUPERCEDE framework	✔ Virtualbox, Xen, VMWare	✔
FORTH EWIS & Cloud	✔ XenServer, QEMU	-
IBM Angel-Eye	-	✔
IBM ExpliSAT	-	✔
IBM Anti-ROP	-	✔

Table 26. SMESEC products in virtual machines and containers

Conclusions:

- Almost all products can run in virtualized environments, which allows a greater deal of flexibility when it comes to integration. Virtual machines can offer a far cheaper way to deploy the services.
- Also, a great majority has been tested to run in containers – and some other can be tested as well. As containers become more popular for micro-services deployment, it gives more options to consider for integrating all or groups of the products.

5.4 Software requirements

Regarding the software requirements, SMESEC product partners were asked to provide the required operating system and any other software that was needed to run their solution. No special dependencies needed other than runtime or open source libraries.

Product name	Operating system	Dependencies
ATOS XL-SIEM	Debian/Ubuntu	Apache Storm, Esper (open source)
BD GravityZone	Windows/Linux/Mac	-
CITRIX AppFirewall	N/A (hypervisor)	-
CITRIX Gateway	N/A (hypervisor)	-
CITRIX Secure Web Gateway	N/A (hypervisor)	-
EGM Test-as-a-Service (TaaS)	Linux	-
FHNW Adherence Monitor & SUPERCEDE framework	Linux (also mobile platforms)	Apache Storm, Esper (open source)
FORTH EWIS & Cloud	Linux	-
IBM Angel-Eye	Linux	-
IBM ExpliSAT	Linux	-
IBM Anti-ROP	Linux	-

Table 27. SMESEC product software requirements

Conclusions:

- Almost all products are capable of running on Linux for their server side components
- BD solutions runs on multiple operating systems as endpoints
- CITRIX solutions run on hypervisors, i.e. it is not an installable package
- Only open source packages/libraries are required; thus, all products can run standalone without any other commercial dependencies.

5.5 Cloud readiness

Cloud is nowadays gaining more and more ground as a deployment option. Table 28 shows the readiness of the contributed products for cloud deployment.

Product name	Cloud ready	Hybrid mode
ATOS XL-SIEM	Not tested	Not tested
BD GravityZone	✔ Server	✔

CITRIX AppFirewall	✔	✔
CITRIX Gateway	✔	✔
CITRIX Secure Web Gateway	✔	✔
EGM Test-as-a-Service (TaaS)	✔	-
FHNW Adherence Monitor & SUPERCEDE framework	✔	✔
FORTH EWIS & Cloud	✔	-
IBM Angel-Eye	✔ offline stage	-
IBM ExpliSAT	-	-
IBM Anti-ROP	✔ compilation	-

Table 28. SMESEC product cloud readiness

Conclusions:

- As the target machines (e.g. Linux) can be deployed on a public or private cloud, all products are expected to be able to run there. Furthermore, some of the products have been tested explicitly to run on major public clouds (e.g. AWS, Azure, etc.)
- An extra interesting capability is to be able to run in both cloud and on-prem mode in parallel and in sync. This option brings more requirements into the mix, which some of the products cannot meet (or at least are not tested yet).
- Ability to run on the cloud will give a greater freedom of deployment options and it can make it more accessible to SMEs that may not own the necessary hardware.

5.6 Inputs and Outputs

An interesting topic is what are the (high-level) inputs/outputs that an SMESEC product expects/products. A detailed analysis is provided in D2.2 [2], and the results of Table 29 summarize only the part of the information that was necessary for an early idea of the integration of the products.

Product name	Inputs	Outputs
ATOS XL-SIEM	Sensors, Logs, Firewalls	Alarms
BD GravityZone	Programs/Software	Alarms

CITRIX AppFirewall	Network traffic	Alarms, AppFlow
CITRIX Gateway	Network traffic	Alarms, AppFlow
CITRIX Secure Web Gateway	Network traffic	Alarms, AppFlow
EGM Test-as-a-Service (TaaS)	Tests	-
FHNW Adherence Monitor & SUPERCEDE framework	SIEM data	Events, Reports
FORTH EWIS & Cloud	Network traffic	Reports
IBM Angel-Eye	Programs/Software	Programs
IBM ExpliSAT	Programs/Software	Reports
IBM Anti-ROP	Programs/Software	Executables

Table 29. SMESEC product input and output

Conclusions:

- The inputs include three main sources: (i) logs, (ii) programs, and (iii) network traffic which are the most typical in SMEs.
- Outputs contain all those elements needed to build comprehensive dashboards with insights and visualizations (some of the products have this capability)

5.7 Endpoint protection

Table 30 summarizes what are the endpoints that can be protected by the contributed products. This refers to the general characteristics (like operating system). A special column has been added for IoT device protection, again without reference to specific characteristics.

Product name	Protect Endpoints	Protects IoT
ATOS XL-SIEM	-	(✔)
BD GravityZone	✔ Mac, PC, Android	-
CITRIX AppFirewall	-	-
CITRIX Gateway	✔ Laptops, Thin-clients, tablets	(✔)
CITRIX Secure Web Gateway	-	-

EGM Test-as-a-Service (TaaS)	-	✔
FHNW Adherence Monitor & SUPERCEDE framework	-	✔
FORTH EWIS & Cloud	-	(✔)
IBM Angel-Eye	-	✔
IBM ExpliSAT	-	
IBM Anti-ROP	-	✔

Table 30. SMESEC product endpoint protection

Conclusions:

- Two of the contributed products have the ability to address explicitly the desktop, server, mobile phone and tablet security for antivirus and secure access.
- Most products can operate in some way on IoT devices: that could be from their network traffic to the system software level.

5.8 Analytics & Reporting

Table 31 has three columns to show the output capabilities of the products in terms of analytics, exportability of results, and visualization.

Product name	Analytics & Reports	Exportable data	Visual dashboards
ATOS XL-SIEM	✔	✔ RabbitMQ	✔
BD GravityZone	✔	✔ Syslog	✔
CITRIX AppFirewall	(✔)	✔ AppFlow	✔
CITRIX Gateway	(✔)	-	✔
CITRIX Secure Web Gateway	-	-	-
EGM Test-as-a-Service (TaaS)	✔ Reports with statistics	-	✔
FHNW Adherence	✔	-	✔

Monitor & SUPERCEDE framework			
FORTH EWIS & Cloud	-	✔	✔
IBM Angel-Eye	-	-	✔ Offline stage
IBM ExpliSAT	✔ Coverage Report	-	-
IBM Anti-ROP	-	-	-

Table 31. SMESEC product analytics and reporting capabilities

Conclusions:

- Almost all products have to some degree the concept of analytics reports.
- There are different ways that products export their results to other platforms (such as the SMESEC unified framework), but they are open or RFC-based which makes the consumption of this information possible.
- Some of the products produce some visual dashboard for the results display. In some cases, they can be potentially used by the unified framework directly, or else, be synthesized by the exported raw data.

5.9 Risk assessment – Behaviour analysis

Finally, some advance characteristics include the ability to provide data insights (e.g. by applying machine learning or statistical analysis methods), behaviour analysis and risk assessments. This set of capabilities is considered more sophisticated as it often has to correlate data from various sources in order to extract a result with some confidence interval.

Product name	Data insights	Behaviour analysis	Risk assessment
ATOS XL-SIEM	–	-	✔
BD GravityZone	-	✔ For software to detect malicious behaviour	✔ Vulnerability assessment
CITRIX AppFirewall	(✔)	-	-
CITRIX Gateway	(✔)	-	-

CITRIX Secure Web Gateway	(✔)	-	-
EGM Test-as-a-Service (TaaS)	✔	-	-
FHNW Adherence Monitor & SUPERCEDE framework	✔	-	✔
FORTH EWIS & Cloud	✔	-	-
IBM Angel-Eye	-	-	-
IBM ExpliSAT	-	-	-
IBM Anti-ROP	-	-	-

Table 32. SMESEC product risk assessment capabilities

Conclusions:

- Some products can produce reports that go beyond the raw data and reveal more insights. The existence of processed data means less burden and traffic to other architecture components that will perform the data analysis.
- There is currently no contributed product focused on behaviour analysis, other than BD GravityZone which rather examines software behaviour.
- On the contrary, few products support risk assessment from raw events. This is an interesting point architecturally, as the collection of more events from all other products to them, can potentially reinforce their risk assessment capabilities.

6 Requirements and Capabilities

This section presents the basic requirements of the SMESEC pilot use cases in regard to the SMESEC product capabilities. This information is essential for identifying the current positioning of the SMESEC products to the needs of a very restricted but diverse group of SMEs, and form a basis for comparison to the benefits that an integrated architecture will bring.

6.1 Use case requirements

This section summarizes the findings on section 3, putting them into the context of the product capabilities.

The analysis is based on:

1) Business requirements: high-level business objectives for a security solution for SMEs.
2) Platform requirements: high-level technical objectives of the security solution.
3) Technical requirements: protecting assets, or protecting against attacks.

Note that the findings below come from the use case descriptions. In general, it should be expected that an SME can have all those requirements at the same time. The analysis focused on what are the key requirements per case and how they are met by the capabilities of the products.

6.1.1 Business requirements

Table 33 presents the *top* business requirements as they have been (explicitly) reported by pilot use cases in Section 2).

	SCYTL	UOP	WOS	GRIDP
Availability	✔	✔	✔	✔
Usability			✔	
Privacy	✔		✔	✔
Cost	✔	✔	✔	✔
Alerting		✔	✔	✔
Scalability			✔	✔

Table 33. SMESEC pilot use cases top business requirements

6.1.2 Platform requirements

Table 34 presents the *top* business requirements as they have been reported by use cases in Section 2.

	SCYTL	UOP	WOS	GRIDP
System integrity	✔	✔	✔	✔

Confidentiality	✔			✔
Non-repudiation		✔	✔	✔
Authentication	✔	✔	✔	✔

Table 34. SMESEC pilot use cases top platform requirements

6.1.3 Protection requirements

The following table shows the protection requirements as identified by the use case partners with their respective priorities as they are reflected from the requirement analysis in Section 3.

Protect (against)	SCYTL	UOP	WOS	GRIDP
Web application servers	1	1	4	4
Database servers	2			
Network traffic	3	5		
Web servers	4			
Email servers		3		
DDoS		1	5	1
Access abuse			2	
Software misuse			1	
Zero-day attacks			6	
Code injection			8	2
Man-in-the-Middle attacks			3	3

Table 35. SMESEC pilots protection requirements with priorities

Some conclusions that can be extracted from Table 35:

- Enterprise partners seem to have a strong interest on protecting: (i) web assets - application or content servers, (ii) database servers, (iii) email servers.
- Denial-of-Service attacks also seem to be of high concern for both enterprise and industrial partners, especially when exposing to the network an application server.
- IoT use cases focus a lot in lower-level aspects: physical access to the device and attempts to tamper it, protection of low-level code (injection), man-in-the-middle attacks.

6.2 Product capabilities

Products on the other hand provide some capabilities that will be used to match the requirements of the use cases. The following sections demonstrate how these products relate to the requirements mentioned in Section 6.1. The data for the tables below have been collected through analysis of the various feedbacks that partners have provided.

6.2.1 Business capabilities

Table 36 summarizes the key capabilities of the products in regard to the top business requirements. Notice that parameter of cost has not been examined in this survey as it focused on the technical characteristics.

	ATOS	BD	CITRIX	EGM	FHNW	FORTH	IBM
Availability	✔	✔	✔			✔	
Usability	✔		✔	✔	✔		✔
Privacy		✔	✔			✔	✔
Alerting	✔	✔	✔		✔	✔	✔

Table 36. SMESEC product business capabilities

6.2.2 Platform capabilities

Table 37 shows the capabilities of the product as related to the platform requirements of the use cases.

	ATOS	BD	CITRIX	EGM	FHNW	FORTH	IBM
System integrity	✔	✔		✔		✔	✔
Confidentiality		✔	✔				✔
Non-repudiation						✔	✔
Authentication			✔				
Scalability	✔		✔				

Table 37. SMESEC product top platform capabilities

6.2.3 Protection capabilities

Finally, the corresponding protection capabilities are shown for the SMESEC products.

Protection (against)	ATOS	BD	CITRIX	EGM	FHNW	FORTH	IBM
Web application servers		✔	✔			✔	
Database servers		✔	✔			✔	
Network traffic	✔		✔			✔	
Web servers		✔	✔			✔	
Email servers		✔	✔				
DDoS	✔		✔			✔	

Access abuse	✔		✔	✔		✔	✔
Software misuse		✔		✔		✔	✔
Zero-day attacks	✔	✔					✔
Code injection							✔
Man-in-the-Middle attacks							✔

Table 38. SMESEC product protection capabilities

Note that FHNW solution runs on top of all front-line tools and as such collects and processes logs and metadata, rather than protecting system and network assets directly.

6.3 Requirements vs. Capabilities

Putting side-by-side the tables of sections 6.1 and 6.2, it becomes apparent that the SMESEC product capabilities are covering the business and platform needs of the SMESEC pilot use cases.

More specifically, Table 39 shows the products that provide the capability for each of the objectives of Table 33 and Table 34.

	Pilot use cases	SMESEC products
Business objectives		
Availability	All	ATOS, BD, CITRIX, FORTH
Usability	WOS	ATOS, CITRIX, EGM, FHNW, IBM
Privacy	SCYTL, WOS, GRIDP	BF, CITRIX, FORTH, IBM
Cost	All	(not addressed)
Alerting	UOP, GRIDP	ATOS, BD, CITRIX, FHNW, FORTH, IBM
Platform objectives		
System Integrity	All	ATOS, BD, EGM, FORTH, IBM
Confidentiality	SCYTL, GRIDP	BD, CITRIX, IBM
Non-repudiation	All	FORTH, IBM
Authentication	All	CITRIX
Scalability	WOS, GRIDP	ATOS, CITRIX
Protection objectives		
Web application servers	SCYTL, UOP, WOS	BD, CITRIX, FORTH

Database servers	SCYTL, UOP	BD, CITRIX, FORTH
Network traffic	SCYTL, UOP	ATOS, CITRIX, FORTH
Web servers	SCYTL	BD, CITRIX, FORTH
Email servers	UOP	BD, CITRIX
DDoS	UOP, WOS, GRIDP	ATOS, CITRIX, FORTH
Access abuse	WOS, GRIDP	ATOS, CITRIX, EGM, FORTH
Software misuse	WOS	ATOS, CITRIX, EGM, FORTH, IBM
Zero-day attachs	WOS	BD, EGM, FORTH, IBM
Code injection	WOS, GRIDP	IBM
MiTM attacks	WOS, GRIDP	IBM

Table 39. SMESEC pilot requirements vs. product capabilities

Current analysis is only based on a comparison between requirements and capabilities as deducted by the technical documents that partners provided. It should be noted though, that it is not taking into account the added value that the integration of the SMESEC products will bring into the context of a unified framework.

7 Potential Improvements

The products that partners bring to SMESEC already cover a wide range in the spectrum of the security market. The market analysis performed showed that there are some new potential areas where the SMESEC products could be evolved in the near future. By applying a successful architecture, each improvement in one product could bring multiples of benefits for the SMESEC framework as a whole.

In the following sections, the current status is identified versus the expected status at the end of the project, based on the potential improvements that the partners have identified for their products.

7.1 Introduction

Primary criteria when discussing about the improvements have been:

1) The suitability for SMESEC use cases.
2) The suitability for SMEs as a target.
3) The evolvement of the security market in the next few years.

For the suitability to SMESEC use cases, feedback has been already available (as described in Section 2 and 6), whereas for SMEs as a target market, an extrapolation of the use case requirements was used. Finally, the results of the security market survey demonstrated some new trends and areas for development.

Figure 16 provides a visualization of the SMESEC products position in the security market landscape.

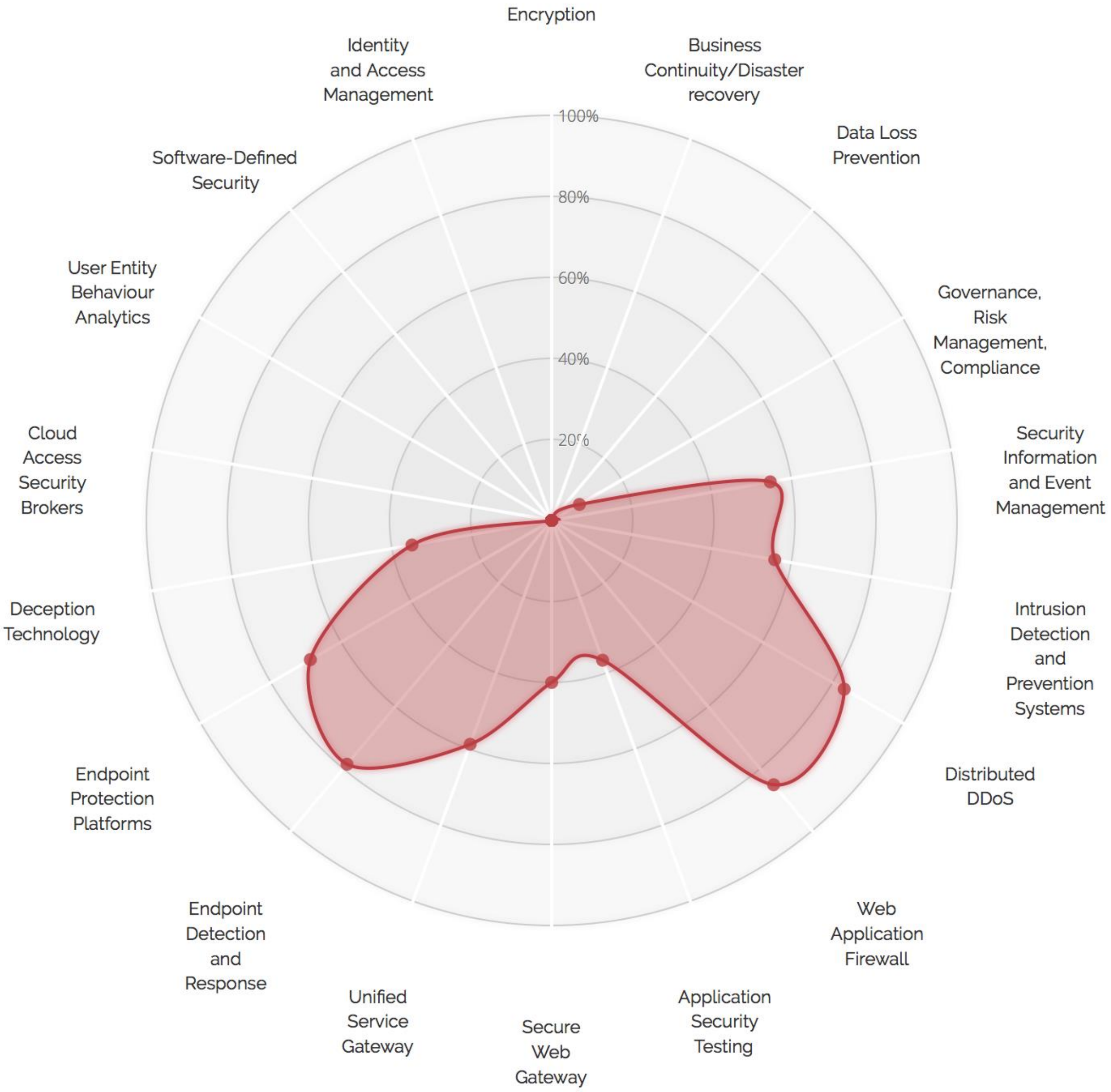


Figure 16. Current SMESEC products position in market

Based on the improvements presented in the following sections, and the expected added benefit that the integration will have, the positioning of the SMESEC framework may appear as in Figure 17.

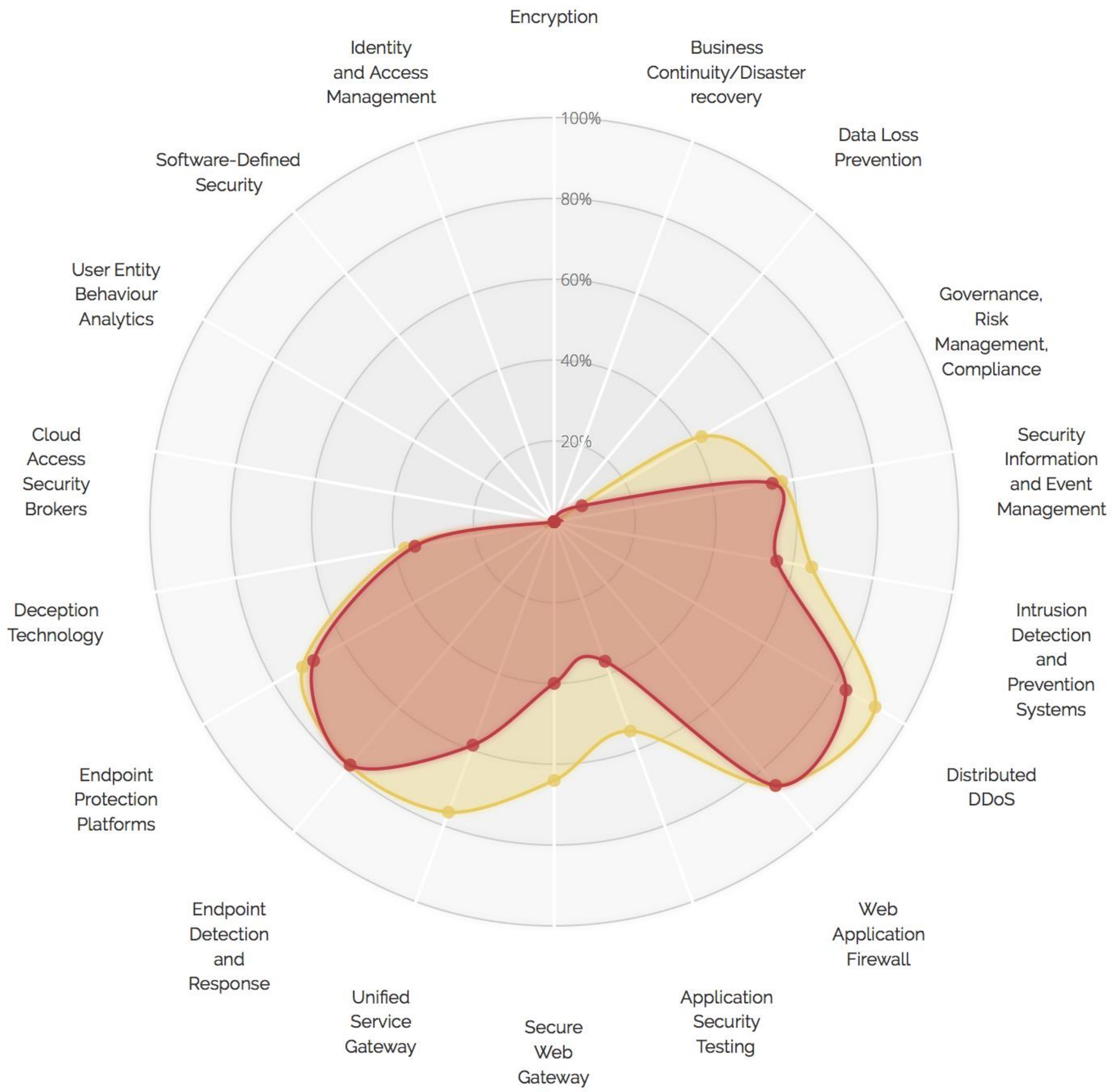


Figure 17. Security market coverage for the SMESEC framework

Annex I describes in more detail how the raw data for the two figures above have been created.

In the following sections a detailed description of the improvement for all SMESEC contributed products follows. The lists are indicative, as during the course of the project, many more technical extensions may be proposed as part of the integration process, or some others may be dismissed due to unsuitability with the proposed framework. It is though indicative of what SMESEC partners think attractive as future extensions of their products.

7.2 ATOS

A list of potential extensions to ATOS XL SIEM follows.

ID	Category	Potential extension
ATOS.PE01	Log management	Capture and store network flow data
ATOS.PE02	Cost-effectiveness	Overview of indicators about cybersecurity threats and attacks
ATOS.PE03	Protection	Extension of SIEM to IoT domain

Table 40. Potential extensions in ATOS XL-SIEM

7.3 BitDefender

A list of potential extensions for BitDefender GravityZone follows.

ID	Category	Potential extension
BD.PE01	Integrations	Integration of GravityZone with SIEM

Table 41. Potential extensions for BitDefender GravityZone

7.4 CITRIX

A list of potential extensions for Citrix products follows.

7.4.1 NetScaler AppFirewall

ID	Category	Potential extension
CITRIX.PE01	Deployment options	Deploy to cloud in as-a-service mode
CITRIX.PE02	Integrations	Integration with SIEM

Table 42. Potential extensions in Citrix AppFirewall

7.4.2 NetScaler Gateway

ID	Category	Potential extension
CITRIX.PE03	Deployment options	Deploy to cloud in as-a-service mode
CITRIX.PE04	Integrations	Integration with SIEM

Table 43. Potential extensions in Citrix Gateway

7.4.3 NetScaler Secure Web Gateway

ID	Category	Potential extension
CITRIX.PE05	Threat protection	Anti-malware protection
CITRIX.PE06	Threat protection	Anti-bot protection

CITRIX.PE07	Email security	Spam, malware, content filtering
CITRIX.PE08	Deployment options	Deploy to cloud in as-a-service mode
CITRIX.PE09	Integrations	Integration to SIEM

Table 44. Potential extensions in Citrix Secure Web Gateway

7.5 EGM

A list of potential product extensions for EGM Tool-as-a-Service follows.

ID	Category	Potential extension
EGM.PE01	Dynamic Application Security Testing	Test for fuzzing and brute force attacks
EGM.PE02	Dynamic Application Security Testing	Detect privileged access related vulnerabilities, linked to IoT systems
EGM.PE03	Dynamic Application Security Testing	Detect OWASP top-10, WASC & SANS top 25 vulnerabilities
EGM.PE04	Dynamic Application Security Testing	Detects application DoS vulnerabilities
EGM.PE05	Integrations	Integration with bug tracking tools
EGM.PE06	Protection	Tests for known IoT vulnerabilities with the full test suites

Table 45. Potential extensions in EGM Tool-as-a-Service

7.6 FHNW

A list of potential extensions for FHNW CYNET solution follows.

ID	Category	Potential extension
FHNW.PE01	Policy Management	Support commonly used policy templates
FHNW.PE02	Risk Management	Risk register
FHNW.PE03	Risk Management	Support for Risk Frameworks
FHNW.PE04	Risk Management	KRI (Key Risk Indicator) Library
FHNW.PE05	Risk Management	Risk Assessment Questionnaires
FHNW.PE06	Audit Management	Risk-based scoping
FHNW.PE07	Audit Management	Workpaper management
FHNW.PE08	Audit Management	Audit Calendar Management

FHNW.PE09	Threat & Vulnerability Management	Integration with 3rd party tools (patch management, vulnerability assessment, etc.) through an API definition with SMESEC partners' tools
FHNW.PE10	Incidence management	Data aggregation from multiple sources (SIEM, DLP, service desk, etc.) Business impact assessment (Both features above, though capability specific KPIs recorded by user or offered by integrated tools)
FHNW.PE11	Platform capabilities	Federated architecture
FHNW.PE12	Platform capabilities	Custom role-based dashboards

Table 46. Potential extensions in FHNW CYSEC

7.7 FORTH

A list with potential extensions for FORTH products follows:

ID	Category	Potential extension
FORTH.PE01	Traffic Filtering	Identify attacks that may cover multiple sessions and connections
FORTH.PE02	Standard Threat Protection	IPS profiles to activate/deactivate protections based on severity, protocols, confidence interval, etc.
FORTH.PE03	Administration, Logging and Reporting	Prioritize and send alerts to users
FORTH.PE04	Thread protection	Defense of web and applications on the Cloud
FORTH.PE05	Improvements	GPU for pattern matching

Table 47. Potential extensions in FORTH EWIS

7.8 IBM

A list of potential extensions for IBM products follows.

7.8.1 ExpliSAT

In Application Security Testing:

ID	Category	Potential extension
IBM.PE01	General features	Fully automated testing

Table 48. Potential extensions in IBM ExpliSAT

7.8.2 AngelEye

In Application Security Testing:

ID	Category	Potential extension
IBM.PE02	Integrations	Integration with WAF vendors
IBM.PE03	Integrations	Integration with MDM/EMM vendors
IBM.PE06	Protection	Automatic virtual patching tool - Learning of fuzz testing data
IBM.PE07	Simplicity	Automatic virtual patching tool - automatic updating

Table 49. Potential extensions in IBM AngelEye

7.8.3 Anti-ROP

ID	Category	Potential extension
IBM.PE04	General capabilities	Identify attacks without known attack patterns or signatures
IBM.PE05	General capabilities	Integration with MDM/EMM vendors

Table 50. Potential extensions in IBM AntiROP

7.9 Other desired extensions – use of other tools

The goal for SMESEC framework is to provide an affordable, easily deployable and manageable solution for supporting the security needs of SMEs. As such, it should provide as wide coverage as possible in the security market, and though the overall solution is expected to cover a very good portion of the market, there are still some areas where SMESEC has not presence.

According to a preliminary analysis, taking into account a very high-level integration design of the products, the areas that may be needed are:

- **Identity and Access Management**: this is important as a centralized service for identifying and authorizing user becomes important, mainly due to the large number of applications that need access to credentials. Having different identity databases makes management more difficult and moreover, security enforcement more difficult as more sources should be monitored.
- **User Entity Behaviour Analytics**: Behaviour analysis becomes more and more important in modern security systems. The ability to profile users and devices, identify patterns and recognize anomalies is becoming a critical feature for many applications as simple rule-based policies may fail to see the overall picture.
- **Cloud Access Security Broker**: As cloud becomes a vital part of the infrastructure of many SMEs, it is expected that integration of the cloud and on-premises infrastructure is going to play key role in future deployments. The easiness of deploying cloud services, coupled with the ability to simplify and monitor usage makes CASB an appealing offering for many SMEs.

It should be first examined if these extra capabilities can be offered by any combination of the existing products. Otherwise, it is possible to consider integrating one of the third-party platforms mentioned in Section 4, or leaving APIs open for future integration, should it be needed.

8 Conclusions

This report contains the results of an initial research on three main topics:

- SMESEC use case security requirements
- SMESEC contributed product capabilities
- The security market today and where SMESEC fits there

Firstly, the SMESEC use case analysis (as part of the work done in Task 2.1) focused on the technical requirements, architecture and security needs of the four examined SMEs. It also provided a prioritization of the needs in regard to known or expected incidents that led to a first risk assessment using the CYSFAM methodology.

In this part, the common high-level requirements of the use cases have been identified which are:

- Availability: services should be uninterruptedly up and running
- Usability: any security framework should not affect the user experience and expectations
- Privacy: for protecting sensitive information and maintaining the customer trust
- Cost: any solution should not require high deployment costs
- Alerting: a security framework should provide configurable alert system

In technical terms, there is also a number of assets that needs to be protected:

- Web servers and web applications: for protecting the apps based on HTTP(S)
- Email servers: that would break the business continuity
- Database servers: protecting the very backend of the business
- Network traffic: for protecting against malicious traffic and DDoS attacks
- Code injection in devices and apps: protecting own devices from spreading attacks

Secondly, the SMESEC products were examined in terms of their capabilities, technical requirements, and architecture. The feedback collected was useful for sketching a very high-level integration and understanding how both the individual products and their integration under a unified SMESEC framework matches the security of the pilot use cases.

A thorough technical analysis of the contributed products revealed that they provide a wide range capabilities to cover the high-level requirements. Besides, the integration effort should ensure that these requirements also stay on top during the design and implementation of the unified framework. This analysis also investigated possible integration strategies in regard to architecture, platform deployment and cloud readiness.

Following, a security market analysis identifies the key market segments in terms of technical capabilities. Apart from the traditional segments, some emerging ones are also presented as, according to analysts, they are going to have a key role in the years to come and SMESEC should benefit by embracing some of the new features and/or provide the hooks to connect with third-party products there.

Finally, based on the technical analysis of the contributed products and the market segment analysis, focus is given on placing the SMESEC framework in the security landscape. In the first phase, only as a sum of the products, but it is anticipated that the integration will produce some extra value to the overall solution. Some product extensions, as identified by partners, point to new features that would help SMESEC strengthen its position as a unified security framework for SMEs.

The information of this deliverable has been collected in a form of few targeted questionnaires directly from the SMESEC partners. The results have been further analysed in the other two deliverables of the Work Package and specifically:

- D2.2 explains in more detail the technical requirement of the SMESEC products, investigates integration points among them, and proposed some high-level design.
- D2.3, among others, contains a detailed explanation of the risk assessment process that has been followed for the analysis of the four pilot use cases.

The results of this deliverable will also benefit tasks in WP3 (architectural aspects), WP4 (validation on the SMESEC use cases) and WP6 (exploitation and dissemination activities in regard to market analysis).

Some key conclusions of this deliverable:

- The four pilot use cases represent the security needs of a large percentage of small-medium enterprises.
- The contributed products have a good coverage of the security market today and should cover the needs of the four pilot use cases.
- Technically, there is a lot of common ground among the products.
- A unified SMESEC framework will provide added-value to all individual products, multiplying the benefits for SMEs.

References

[1] SMESEC Security Products Unification Report, Deliverable 2.2, SMESEC project, http://www.smesec.eu

[2] SMESEC Security Awareness Report, Deliverable 2.3, SMESEC project, http://www.smesec.eu

[3] SME Performance Review, European Commission, http://ec.europa.eu/growth/smes/business-friendly-environment/performance-review-2016_en#annual-report

[4] Information security and privacy standards for SMEs, ENISA, https://www.enisa.europa.eu/publications/standardisation-for-smes

[5] Impact Assessment- Proposal for a Regulation of the European Parliament and of the Council, European Commission, https://ec.europa.eu/transparency/regdoc/rep/10102/2017/EN/SWD-2017-500-F1-EN-MAIN-PART-4.PDF

[6] Small and Medium-sized Enterprises: Local Strength, Global Reach, OECD, http://www.oecd.org/cfe/leed/1918307.pdf

[7] OSSEC software, Open source host-based IDS (HIDS), https://ossec.github.com

[8] AIDE software, Advanced Intrusion Detection Environment, http://aide.sourceforge.net

[9] LightHttpd software, Lightweight web server, https://www.lighttpd.net

[10] Bugzilla software, Issue tracking software, https://www.bugzilla.org

[11] ElasticSearch software, Search Analyze Visualize Data, https://www.elastic.co

[12] Fail2Ban software, Ban IPs with Malicious Signs, https://www.fail2ban.org/

[13] OpenStack Swift Project, Object Storage for OpenStack, https://wiki.openstack.org/wiki/Swift

[14] Loadsensing LS-G6, https://www.worldsensing.com/product/loadsensing/

[15] WorldSensing DLOG App, https://www.worldsensing.com/wp-content/uploads/2016/09/Loadsensing-technical-datasheet.pdf

[16] SCA121T Series, Stand Alone Inclinometer, http://murata.co.jp/products/sensor/pdf/sca121t_inclination_sensor.pdf

[17] WorldSensing, Mobility, City Operation Intelligence, https://www.worldsensing.com/solutions/mobility-software-solution-cities/

[18] GridPocket PowerVAS, http://www.gridpocket.com/products/machine-to-machine/

[19] OneM2M, Standards for M2M and IoT, http://www.onem2m.org

[20] ETSI M2M standards, http://www.etsi.org/technologies-clusters/technologies/internet-of-things

[21] GridPocket EcoTroks application, http://www.gridpocket.com/products/behavioral-energy-efficiency-program/

[22] OVH public cloud, https://www.ovh.com/us/

[23] Nginx, Opensource reverse proxy, https://www.nginx.com/resources/wiki/

[24] Zabbix, Enteprise-class Monitoring Platform, https://www.zabbix.com

[25] StrongSwan, Open Source IPsec-based VPN solution, https://www.strongswan.org

[26] OWASP Top-10 Project, https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

[27] Spruit, M. & Röling, M. (2014). ISFAM: the information security focus area maturity model. 22nd European Conference on Information Systems, Tel Aviv, Israel.

[28] Spruit, M. CYSFAM, Cyber Security Focus Area Maturity Model, in publication.

[29] FireCompass.com, Security Market Analysis, https://www.firecompass.com/about/

[30] Encryption market analysis, https://www.firecompass.com/security/market/encryption-e

[31] 2016 top picks for enterprise encryption tools, http://searchsecurity.techtarget.com/feature/Readers-2016-top-picks-for-enterprise-encryption-tools

[32] Top full disk encryption products, http://searchsecurity.techtarget.com/feature/The-top-full-disk-encryption-products-on-the-market-today

[33] Encryption software vendors, http://searchitchannel.techtarget.com/feature/Encryption-software-vendors

[34] VeraCrypt Open Source Encryption Software, https://veracrypt.codeplex.com, Apache License

[35] CryptTool Encryption Software, https://www.cryptool.org/en/

[36] DiskCryptor Encryption Software, https://diskcryptor.net/wiki/Main_Page

[37] 6 Vendors in IT Governance, Risk and Compliance, https://www.firecompass.com/blog/top-5-vendors-governance-risk-compliance-itgrc-market-rsac-2017/

[38] Top 25 Governance, Risk and Compliance Technology Providers, https://www.cioapplications.com/vendors/top-25-governance-risk-and-compliance-grc-technology-providers-2017-rid-30.html

[39] IT Governance, Risk and Compliance, https://www.firecompass.com/security/market/it-governance-risk-and-compliance-itgrc

[40] Top 5 Vendors in Data Loss Prevention (DLP) Technology at RSAC 2017, https://www.firecompass.com/blog/top-5-vendors-data-loss-prevention-dlp-technology-rsac-2017/

[41] Data Loss Prevention, https://selecthub.com/categories/data-loss-prevention

[42] Gartner Magic Quadrant for Enterprise Data Loss Prevention: What's Changed, https://solutionsreview.com/backup-disaster-recovery/gartner-magic-quadrant-for-enterprise-data-loss-prevention-whats-changed/

[43] Data Loss Prevention, https://www.firecompass.com/security/market/data-loss-prevention-dlp

[44] Unified Threat Management, https://www.firecompass.com/security/market/unified-threat-management-utm

[45] Reviews for Unified Threat Management (UTM) Worldwide, https://www.gartner.com/reviews/market/unified-threat-management-worldwide

[46] Gartner Magic Quadrant for SIEM 2016: not just for compliance anymore, https://techbeacon.com/highlights-gartner-magic-quadrant-siem-2016

[47] Security Information and Event Management, https://www.firecompass.com/security/market/security-information-and-event-management-siem

[48] Top Intrusion Prevention System Appliance, http://www.crn.com/slide-shows/security/240165891/top-intrusion-prevention-system-appliance-a-9-vendor-battle.htm

[49] Intrusion Prevention Detection Solution Vendor List, http://jafsec.com/Intrusion-Prevention/Intrusion-Prevention-Detection-A-B.html

[50] Intrusion Prevention System (IPS), https://www.firecompass.com/security/market/intrusion-prevention-system-ips

[51] DDoS protection service: Top vendors in the field, https://www.helpnetsecurity.com/2015/12/21/ddos-protection-service-top-vendors-in-the-field/

[52] The Best DDoS Protection Services, http://www.toptenreviews.com/business/internet/best-ddos-protection-services/

[53] Distributed Denial of Service (DDOS), https://www.firecompass.com/security/market/distributed-denial-of-service-ddos

[54] Enterprise Backup and Disaster Recovery Solutions Directory, https://solutionsreview.com/backup-disaster-recovery/backup-and-disaster-recovery-solutions-directory/

[55] Details on Niche Players in Gartner's DRaaS Magic Quadrant, https://solutionsreview.com/backup-disaster-recovery/details-on-niche-players-in-gartners-draas-magic-quadrant/

[56] Gartner Names 5 Cool Vendors in Business Continuity & DR, https://solutionsreview.com/backup-disaster-recovery/gartner-names-5-cool-vendors-in-business-continuity-dr/

[57] Business Continuity Management (BCM), https://www.firecompass.com/security/market/business-continuity-management-bcm

[58] Web Application Firewall, https://www.firecompass.com/security/market/web-application-firewall-waf

[59] Web Security Gateway Vendor List, http://jafsec.com/Web-Security/Secure-Web-Gateway-A-B.html

[60] Web Content Filtering Solutions, https://www.itcentralstation.com/categories/web-content-filtering

[61] Web Security Gateway (WS), https://www.firecompass.com/security/market/web-security-gateway-ws

[62] Gartner's 2017 Magic Quadrant for Endpoint Protection Platforms (EPP): What's Changed? , https://solutionsreview.com/endpoint-security/gartner-2017-epp-magic-quadrant/

[63] Top 10 Best Antivirus Software, https://www.top10bestantivirus.com

[64] Endpoint Security, https://www.firecompass.com/security/market/endpoint-security-eps

[65] Application Security Testing, https://www.firecompass.com/security/market/application-security-testing-ast

[66] Security Awareness and Training (SWT), https://www.firecompass.com/security/market/security-awareness-and-training-swt

[67] Top 5 Emerging Deception Technology Vendors at RSA Conference 2017, https://www.firecompass.com/blog/top-5-emerging-deception-technology-vendors-at-rsa-conference-2017/

[68] Deception Technologies, https://www.firecompass.com/security/market/deception-technologies-dct

[69] Gartner Magic Quadrant for Endpoint Protection Platforms, https://secure2.sophos.com/en-us/security-news-trends/reports/gartner/magic-quadrant-endpoint-protection-platforms.aspx

[70] Endpoint Detection and Response, https://www.firecompass.com/security/market/endpoint-detection-and-response-edr

[71] Top 5 Emerging Cloud Access Security Brokers (CASB) Vendors at RSAC 2017, https://www.firecompass.com/blog/top-5-emerging-cloud-access-security-brokers-casb-vendors-at-rsac-2017/

[72] 10 Cloud Access Security Brokers Partners Should Watch, http://www.crn.com/slide-shows/security/300081066/10-cloud-access-security-brokers-partners-should-watch.htm

[73] Cloud Access Security Broker, https://www.firecompass.com/security/market/cloud-access-security-broker-casb

[74] 19 Top UEBA Vendors, https://mobile.esecurityplanet.com/products/top-ueba-vendors.html

[75] Top 5 User Behaviour Analytics (UBA) Vendors at RSAC 2017, https://www.firecompass.com/blog/top-5-user-behaviour-analytics-uba-vendors-at-rsa-conference-2017/

[76] User Behaviour Analytics (UBA), https://www.firecompass.com/security/market/user-behavior-analytics-uba

[77] Identity and Access Management Solutions Directory, https://solutionsreview.com/identity-management/identity-management-solutions-directory/

[78] Identity and Access Management, https://www.firecompass.com/security/market/identity-and-access-management-iga

[79] Prometheus, https://prometheus.io/

[80] MicroFocus Fortify, https://software.microfocus.com/en-us/software/software-security-assurance-sdlc

[81] Incapsula, https://www.incapsula.com/

Annexes

8.1 Product extension analysis

8.1.1 Introduction

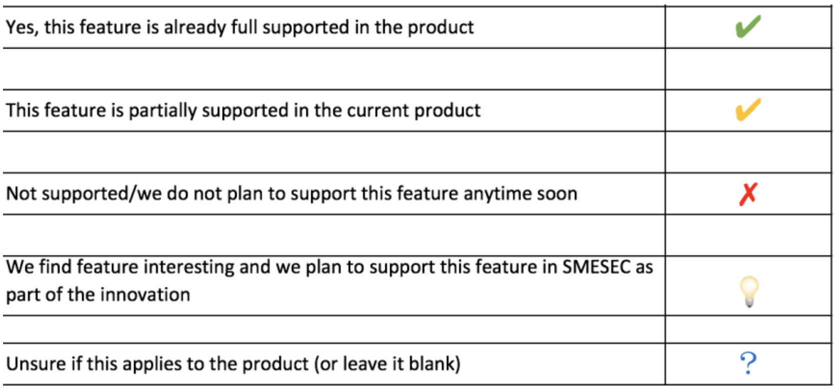
This annex contains some explanation on how Figure 16 and Figure 17 have been created.

For the analysis, the categorization of [1] has been used to identify the key technical features that a product (may) have in each of the market segments. These features were also organized in categories. Each SMESEC product partner has been identified to belong to one or more market segments as presented in Table 24 and they were asked to provide their feedback on the support of the various characteristics in their existing products. Moreover, to identify some extensions that may look relevant and feasible within the SMESEC framework.

It should be noted that these extensions are indicative; some of them may be not be that relevant, or some other new may be needed, depending on the proposed architecture. It is though some initial research on the technical aspects of the products, on what is the current position in the security market, and on where the product will be

8.1.2 About the analysis

Partners where asked to complete next to each characteristic one mark according to the following table:



Yes, this feature is already full supported in the product	✔
This feature is partially supported in the current product	✔
Not supported/we do not plan to support this feature anytime soon	✗
We find feature interesting and we plan to support this feature in SMESEC as part of the innovation	💡
Unsure if this applies to the product (or leave it blank)	?

Each characteristic was then assigned an equal weight. In reality, and once the architecture has been defined, some features may have greater importance thus higher weights, but for this initial analysis this factor is ignored.

The first score that has been produced (“now”) is essentially the percentage of characteristics implemented (fully ✔or partially ✔) versus all the available features. A second score has been also produced (“SMESEC”) when the extensions characteristics (□) are also considered as implemented.

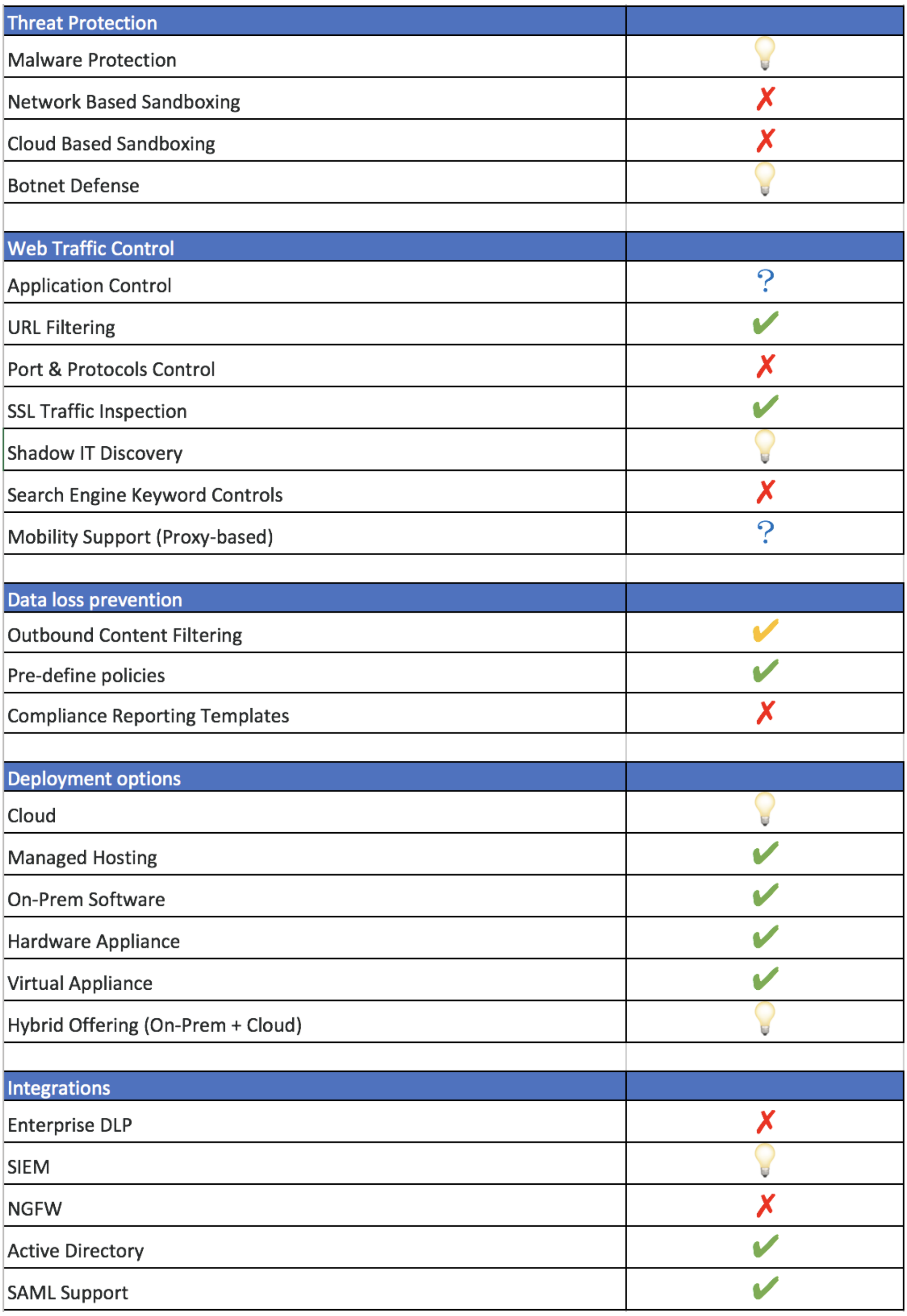
The final results appear in the following table.

Market	Score now	Score SMESEC
Intrusion Detection and Preventions Systems	**55.88%**	**64.71%**
Security Information and Event Management	**54.76%**	**57.14%**
Endpoint Detection and Response	**78.57%**	**78.57%**
Application Security Testing	**36.73%**	**55.10%**
Web Application Firewall	**85.19%**	**85.19%**
Endpoint Protection Systems	**68.75%**	**71.88%**
Unified Threat Management	**58.82%**	**76.47%**
Governance, Risk Management, Compliance	**7.89%**	**42.11%**
Deception Technology	**35.00%**	**37.50%**
Distributed DDoS	**83.33%**	**91.67%**
Secure Web Gateway	**40.00%**	**64.00%**

8.1.3 Example of analysis for a particular segment

shows an example of one product (NetScaler Secure Web Gateway). In this particular one, there are 4 feature categories with 25 distinct features. Currently the product supports 10 of them (fully ✔or partially ✔), whereas there are 6 more features that could be considered as potential extensions (□).

The score in this case are 10/25 for “Now” and 16/25 for “SMESEC”, which yields 40% and 64% respectively.



Threat Protection	
Malware Protection	💡
Network Based Sandboxing	✗
Cloud Based Sandboxing	✗
Botnet Defense	💡
Web Traffic Control	
Application Control	?
URL Filtering	✓
Port & Protocols Control	✗
SSL Traffic Inspection	✓
Shadow IT Discovery	💡
Search Engine Keyword Controls	✗
Mobility Support (Proxy-based)	?
Data loss prevention	
Outbound Content Filtering	✓
Pre-define policies	✓
Compliance Reporting Templates	✗
Deployment options	
Cloud	💡
Managed Hosting	✓
On-Prem Software	✓
Hardware Appliance	✓
Virtual Appliance	✓
Hybrid Offering (On-Prem + Cloud)	💡
Integrations	
Enterprise DLP	✗
SIEM	💡
NGFW	✗
Active Directory	✓
SAML Support	✓

Figure 18. Example of market coverage calculation