SHIELD

SECURING AGAINST INTRUDERS AND OTHER THREATS
THROUGH A NFV-ENABLED ENVIRONMENT

[H2020 - Grant Agreement No. 700199]

Deliverable D2.2

Updated requirements, KPIs, design and architecture

Editor Ludovic Jacquin (Hewlett Packard Enterprise)

Contributors H. Attak, L. Jacquin, V. Sallard (Hewlett Packard Enterprise), C. Fernandez, C. Dávila, B. Gastón (I2CAT), D. Katsianis, I. Neokosmidis, D. Xydias (INCITES), A. Litke, N. Papadakis, D. Papadopoulos (INFILI), E. Trouva (N.C.S.R. Demokritos), O. E. Segou, G. Xylouris, E. Kafetzakis (ORION Innovations), A. Lioy, M. De Benedictis (POLITO), G. Gardikis, K. Tzoulas (Space Hellas), A. Pastor, J. Núñez, D. Lopez (Telefónica I+D), T. Batista, R. Preto, F. Ferreira (UBIWHERE)

Version 1.0

Date February 28th, 2018

Distribution PUBLIC (PU)










Executive Summary

The present document summarises the main findings and conclusions of the project activities related to the identification of the use cases, the elicitation of the requirements, the high-level architectural design of the SHIELD platform and the roadmap for the SHIELD's demonstrators.

SHIELD offers security-as-a-Service in an evolved telco-like environment: it leverages Network Function Virtualisation (NFV) and Software-Defined Networking (SDN) for virtualization and dynamic placement of security appliances in the network. Virtual Network Security Functions (vNSFs) – which are part of a security Network Service (NS) –, Big Data analytics for real-time incident detection and remediation, as well as attestation techniques are the actors securing both the infrastructure and the services.

Three high-level use cases were identified as most relevant for the SHIELD framework:

- *Use Case 1:* An Internet Service Provider uses SHIELD to secure its own infrastructure. This use case involves the Internet Service Providers deploying NSs in their network to detect and mitigate incidents.
- *Use Case 2:* A Service Provider leverages SHIELD to provide advanced Security-as-a-Service services to customers. This use case assumes that security NSs, along with real-time incident detection and management, are offered as-a-Service to the Service Provider clients, such as enterprises, public bodies, etc.
- *Use Case 3:* Contributing to national, European and global security. This use case assumes that incident information is exposed, in a secure and private manner, to public cybersecurity authorities.

The next step identifies the high-level system requirements, which drives the design task. For the gathering of the requirements, three sources are used:

- Analysis of the three identified use cases.
- User stories, as drafted from various stakeholders inside the SHIELD consortium, expressing desired functionalities/interactions with users.
- Online surveys, aimed at prioritizing the use cases, collecting additional requirements and prioritising different business and technical factors.

The online surveys are targeted at persons, both within and outside the consortium, that are professionally engaged with information security tasks; for example, Appendix B is a written feedback provided by a cybersecurity agency of a member state of the European Union. It is organised in three parts: profiling of the experts, criteria comparison and organizational aspects. The criteria comparison part uses the Analytic Hierarchy Process methodology in order to prioritise the three use cases based on several criteria. The result of the analysis is that use case 2 is preferred by half of the interviewees (mainly Business), followed at a distance by use cases 1 and 3. The most important factors expected to affect the usability in all use cases are Data Leakage, Organization, Identity theft and Cybersecurity impact. On the contrary, the less important ones are Operational Transparency and Ease of use. Finally, the main results regarding the organisational aspects show a good predisposition to deploy security services in a cloud environment (around 93%), thanks to the flexibility and cost factors; concerns remain around the service's security.

A second survey uses the Fuzzy Analytic Hierarchy Process methodology in order to compare the different criteria and sub-criteria that affects the market adoption and evolution of the SHIELD platform. The most important criteria for the consortium to take into account is "Performance"; it is followed by "Ease of Use". The remaining criteria ("Other Platform Features", "Business/Strategy aspects", "SIEM-like functionalities" and "Technology Enablers") are almost of equal importance; this suggests that once appropriate performances and ease of use are achieved, the remaining criteria will become more important for the SHIELD solution. At a finer-grained level, the most important factors expected to affect the adoption of SHIELD are "Deployment and Support Simplicity", "Infrastructure and service attestation", and "Security-as-a-Service".

The requirements elicited from the available sources are divided into (i) platform functional requirements, (ii) non-functional requirements, (iii) service functional requirements and (iv) ethical & regulatory compliance requirements. The requirements range as wide as NS deployment and lifecycle management, analytics and visualisation, availability and scalability, specific vNSF solutions (such as traffic filtering), performance, usability, data retention, and much more.

Based on the considered use cases, the identified requirements, the state-of-the-art in NFV and data analytics architectures, a high-level architecture is proposed. This architecture encompasses all the entities needed by the SHIELD project:

- The Network Infrastructure shall be NFV-capable, i.e. supporting the execution and management of vNSF workloads in the network.
- The virtual Network Security Functions implement the traffic processing functionalities, as desired by the users.
- The vNSF Orchestrator (vNSFO) manages the vNSF lifecycle: deployment, configuration, termination.
- The vNSF Store contains the available vNSFs and associated security NSs (sets of vNSFs)
- The Trust Monitor attests the infrastructure and the services by verifying their integrity.
- The Data Analytics and Remediation Engine (DARE) analyses in real-time the information reported by the vNSFs and detects security incidents; then, it proposes remediation actions to mitigate the threats.
- The Security Dashboard is the graphical front-end of the platform, having the various actors interact with it.

Finally, the plan of the consortium for demonstrating the relevance of the SHIELD's platform is detailed. This plan includes the different required tasks as well as the roadmap to execute them.

Table of Contents

1. INTRODUCTION

The SHIELD project aims to provide a solution against new kinds of cyber-attacks affecting both the economy and the society. One of the main challenges is their fast-paced evolution, which takes advantage of legacy protection mechanisms that are usually monolithically designed to address specific attacks and are statically configured by human operators. SHIELD bridges the gap between the ever-evolving cyber-attacks and defences playing catch-up by leveraging the Network Functions Virtualisation (NFV) paradigm, big-data analytics for security and trusted computing mechanisms. SHIELD analyses the network to understand adversary possibilities, behaviours, intents and thus predict specific vulnerabilities and attacks. This approach also promotes openness, interoperability of security functions while offering an affordable security solution.

SHIELD virtualizes the security functions based on the NFV concept, as currently standardised by the European Telecommunications Standards Institute (ETSI): in the NFV design, a network function decouples its functionality from the hardware it requires. This permits a much more flexible environment, where the security functions can be distributed or scaled more efficiently. The functionalities of virtual Network Security Functions (vNSF) are generally categorised into: i) monitoring - aggregating security-related logs and metrics; and ii) reacting - protecting against attacks. These functions are assembled into security Network Services (NSs), which are ultimately instantiated in the network.

Using the inputs from the vNSFs, the Data Analysis and Remediation Engine (DARE) analyses the logs and metrics to detect potential attacks; once a suspicious pattern has been identified, the DARE recommends a set of actions to prepare for a potential attack or mitigate an on-going attack, by indicating the suitable reacting vNSF to be deployed at the appropriate network location. The DARE is based on state-of-the-art big data solutions. Coupled with an analytic engine, this allows SHIELD to use tailor-made security analysis modules to protect against attacks, and ideally by predicting them first.

Initially, SHIELD focuses on three different deployment models that address different economy and society needs: (i) SHIELD can be used by critical infrastructure providers – such as Internet Service Providers (ISP) – to protect their infrastructure; (ii) the SHIELD platform can be leveraged by Service Providers (SP) to provide Security-as-a-Service to customers; and (iii) national, European or global cybersecurity agencies can rely on SHIELD platforms deployed across multiple companies, providers to create a wider security network gathering attack information and potentially sharing insight between distinct entities.

Use Case 1: An ISP using SHIELD to secure their own infrastructure

In order to protect their own network infrastructure, ISPs usually have to deploy specific hardware that is very expensive, since this hardware has to be maintained by specialized operators. Furthermore, the operators may need to initially invest time to figure out the attack before being able to stop it. In this use case, the virtualization offered by SHIELD aims at dramatically reducing both costs by replacing specific hardware for vNSFs, as well as providing a central interface (the security dashboard) to present the implications of the gathered data, its analysis, and then act in the network.

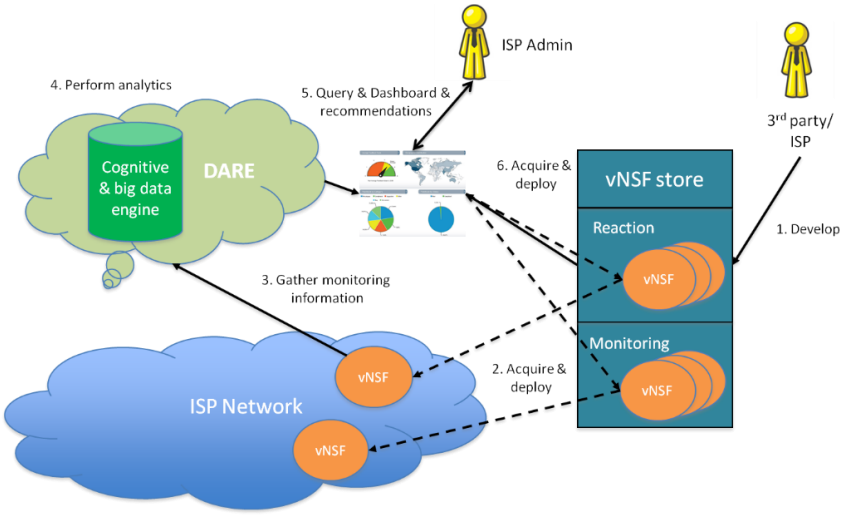


Figure 1 - ISP using SHIELD to secure their infrastructure

Use Case 2: A SP leveraging SHIELD to provide advanced SecaaS services to customers

SHIELD provides an ideal foundation for building enhanced SecaaS solutions, far beyond current offers. Using this SecaaS paradigm, the complexity of the security analysis can be hidden from the client (either a company or an SME), who can therefore be freed from the need to acquire, deploy, manage and upgrade specialised equipment.

In this use case, the Service Provider (SP) would be able to insert new security-oriented functionalities directly into the network of the customer, through its provided gateway or in the SP network infrastructure.

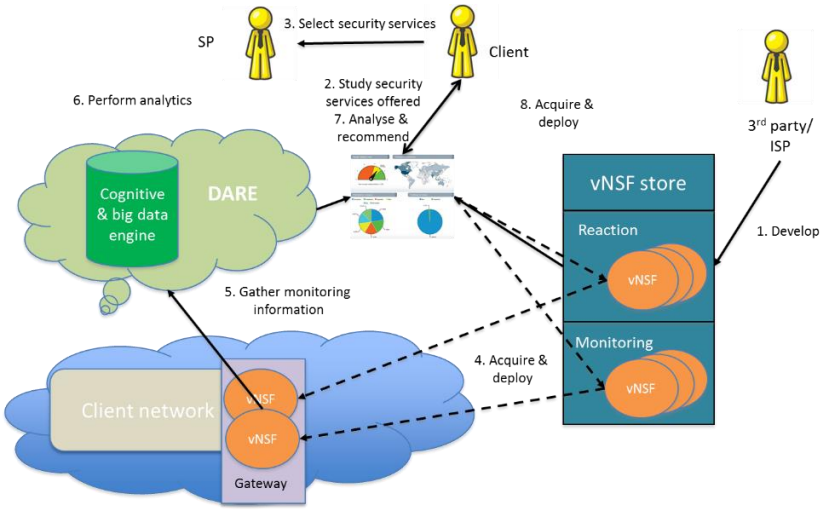


Figure 2 – SP using SHIELD to provide SecaaS capability

Use Case 3: Contributing to national, European and global security

The dashboard, available to authorised actors, accepts requests regarding threat models or acquired threat intelligence. This data can be retrieved by public cybersecurity agencies or computer security incident response teams (CSIRTs). The secure SHIELD framework offers, in this manner, a way of sharing threat information with third-parties who wish to synchronise information and research on measures to be taken on recent attacks, suffered by others. Currently, if a Cybersecurity agency wants to retrieve statistical information about a network,

it has to agree with the SP to deploy specific hardware on the infrastructure. This is a very costly procedure - both in terms of time and money - that makes it prohibitive in the current market situation. Particularly, attacks are constantly evolving and require a fast, reactive and flexible solution. Using SHIELD, Cybersecurity agencies can establish agreements with the SP and deploy vNSF quickly and without specific hardware in the infrastructure. The analysed data is accessible from the dashboard, after it was processed by the DARE.

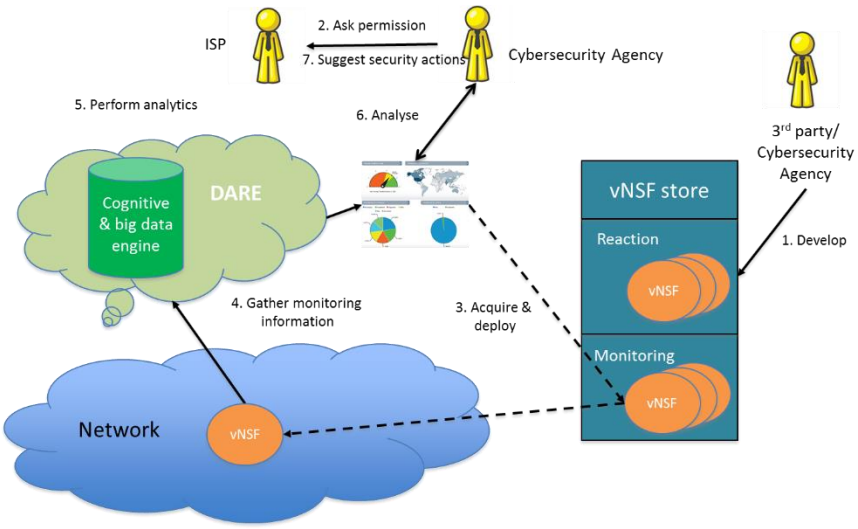


Figure 3 - SHIELD application to national, European and global cybersecurity

The remainder of this document is organised in four sections: Section 2 presents an analysis of the objectives of SHIELD, which leads to the requirements for the project; Section 3 details the technical solution chosen by SHIELD (i.e. main components and their interaction) and discusses the fulfilment of the requirements; Section 4 presents the plan for the SHIELD demonstrator; finally Section 5 concludes the document.

Four appendices are complementing the core document: Appendix A. summarises the main changes between **D2.1 "Requirements, KPIs, design and architecture"** [1] and this document – **D2.2 "Updated requirements, KPIs, design and architecture"**; Appendix B. is a written feedback, from a national cybersecurity agency, about the SHIELD use cases, requirements and KPIs received by the consortium and addressed in this document; Appendixes C1. And C2. present the questionnaire used for analysing the requirements, with the survey's results.

2. SHIELD OBJECTIVES

This section reports the methodology – and associated results – used for eliciting the requirements of the projects. The general scenario of SHIELD, along with the specific use cases, are analysed in order to specify the requirements based on the stakeholders' needs and the required infrastructure. The requirements of the different SHIELD stakeholders are obtained through standard techniques, such as questionnaires and focus groups. These requirements are then formalised and Key Performance Indicators (KPI) are associated with each requirement; these KPIs are the foundation for the evaluation of the project demonstrators.

2.1. Use cases analysis

The SHIELD survey analysing the requirements has been divided in three major parts. These parts consist of: Profiling of the experts, Criteria Comparison and Organization aspects. Apart from the traditional method of collecting experts' opinions, the survey uses the Analytic Hierarchy Process (AHP) methodology for the Criteria Comparison part.

In the first part, the problem under investigation is framed (i.e. its formation articulated) while the criteria and sub-criteria contributing to the achievement of the problem's objective are determined through interviews and/or group discussions with experts. The multi-level hierarchy is then constructed, consisting of three levels.

In the first level, the objective under investigation is shown in the ranking of the Use Cases considered.

Use Case 1: An ISP using SHIELD to secure their own infrastructure

Use Case 2: An SP leveraging SHIELD to provide advanced SecaaS services to customers

Use Case 3: Contributing to national, European and global security

In the second level, the criteria affecting the objective are determined.

- Relevance of the use cases – Social and economic impact of the use cases.
- Threats and vulnerabilities – Targeted threats or vulnerabilities addressed by the solution.
- Security solution aspects – Aspects that cybersecurity solutions must address (cost, ease of use, etc.)

Finally, in the third level, the criteria are further analysed into their relevance sub-criteria. Sub-criteria represent a specific feature characterizing a criterion. Identification of the criteria and their sub-criteria is accomplished based on the focus of their preferential independence.

- Relevance of the use cases – Social and economic impact of the use cases.
  - Organization: Considering your organization as an actor in the value chain.
  - EU market: Considering the economic impact of the solution.
  - EU society: Considering the social impact of the solution.
- Threats and vulnerabilities – Targeted threats or vulnerabilities addressed by the solution.

- **Denial of Service** - Attack that interrupts the systems of the victim not allowing external clients to access the victim's facilities.
- **Data Leakage** - Data being leaked by a rival company or by a third party which can extort the victim. It also affects the company's reputation.
- **Identity theft** - An internal account is compromised and the information is used to act in the name of the company.
- **Scam** - An attacker is dishonestly making money by deceiving the company.
- **Operational interruption** - An attacker is trying to interrupt the internal operation of the company, stopping or slowing down one or more production processes.

- **Security solution aspects** – Aspects that cybersecurity solutions must address (cost, easiness to use, etc.)
  - **Cost** – Economic cost of the security solution.
  - **Operational transparency** – the solution is not influencing (slowing down, changing processes, etc.) the usual operations of the company.
  - **Ease** - not requiring skills, expertise or training to use the solution.
  - **Cybersecurity impact** – the cybersecurity solution achieves a high security level for the addressed treats and vulnerabilities.
  - **Confidence/Privacy** – the cybersecurity solution is robust and cannot be compromised.

Once the hierarchical structure has been constructed and the criteria and sub-criteria have been determined, appropriate questionnaires are conducted and distributed to experts (step 2) for them to fill in.

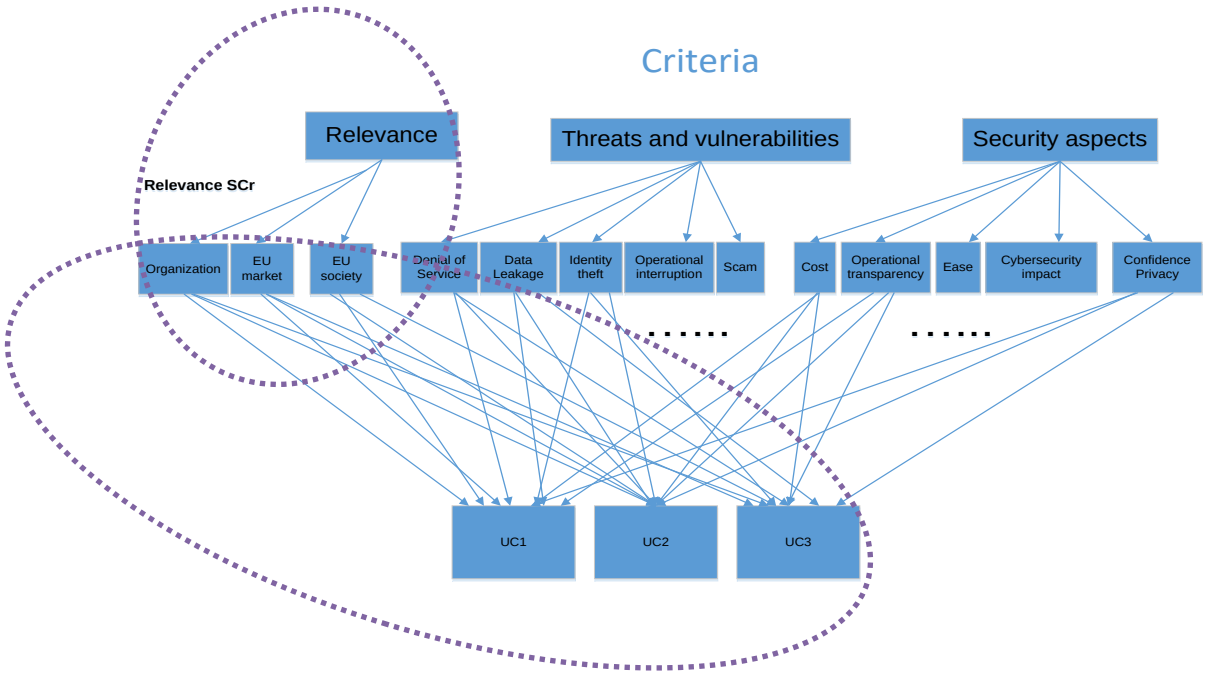


Figure 4 - Multi-Level Hierarchy

Main results concerning the criteria weight (Relevance of the use cases, Threats and vulnerabilities addressed by the solution, and Security solution aspects that cybersecurity

solutions must address) show that the Threats and Vulnerabilities (T&V) criterion is almost twice as important as the other criteria, which are of equal importance.

Furthermore, it is interesting to note that according to the experts' opinion regarding the sub-criteria importance, the most important factors expected to affect the adoption of all Use Cases (UCs) are Data Leakage, Organization, Identity theft and Cybersecurity impact. The experts envisage solutions that protect their infrastructure domains from threats and vulnerabilities which lead to leakage, identification of the thieves and achieves a high security level.

The least important factors are Operational transparency and Ease of use: the personnel responsible for using the proposed solutions in most of the organizations are qualified with advanced skills and expertise.

In the pairwise comparison, experts believe that UC2 (SecaaS) is more relevant to the majority of sub criteria (and especially in the sub-criteria related to the T&V criterion, which are twice more preferable) and precipitates the selection of SHIELD for an ISP in order to provide advanced SecaaS services to its customers as the endorsed solution. This is a clear indication that SHIELD could start in the market as-a-Sservice. Furthermore, the sub-criteria of T&V should be taken into account in the requirements' analysis of SHIELD with increased weight according to the survey. UC1 is the second most preferable solution followed by UC3.

Nevertheless, the most important aspects of a security solution, according to the survey, are Cybersecurity impact (high security level) and Confidence/Privacy (robust and hard to compromise). These sub-criteria are at the same time relevant to UC2 to more than 1/3 of the experts, leading to the conclusion that increased security levels with guaranteed privacy should be taken into account in the selected UCs. It is noticeable that the UC3 is more important for cyber-security impact and EU society (social impact of the solution). This is expected since in UC3, Cybersecurity agencies can establish agreements with the SP and deploy vNSF quickly and without extra cost in the infrastructure making UC3 preferable for Public authorities.

At the same time, UC1 is more relevant to sub-criteria like Organization, Confidence/Privacy, Operational interruption, and Denial of Service and Operational transparency, as UC1 replaces the specific hardware in an ISP by using SHIELD to secure their own infrastructure. Moreover, all the selected components act inside the ISP logic where provider's issues like confidence/privacy, operational interruption, denial of services and transparency are of great importance. For Organization aspects, part of the survey (3rd and last) traditional questions and analysis techniques have been used. For this part (3rd) most of the requirements and KPI have been collected and derived from Work Package 2 (WP2). This analysis follows in the next paragraphs.

A detailed analysis of the results can be found in Appendix C2. Survey's results. The questionnaire is presented in Appendix C1. Survey's questionnaire.

2.2. Factors influencing market adoption and evolution of SHIELD

Following the market analysis, which identified the main competitors of the SHIELD platform, T6.3 proceeded by proposing a roadmap to maximize the chances of SHIELD commercialization in the different market segments. In order to complete this task, specific feedback is needed by

collecting the expert's opinions from different stakeholders through standard techniques, such as questionnaires and focus groups.

The SHIELD consortium launched a second survey (November 2017) focused on the factors that will affect market adoption and evolution of the SHIELD solution. Apart from the traditional method of collecting experts' opinions, the survey uses the Fuzzy Analytic Hierarchy Process (FAHP) methodology for the Criteria Comparison Part (available in D6.3 [2]).

In the first level, the objective under investigation is defined. The factors that will affect market adoption and evolution of SHIELD solution are then ranked.

In the second level, the criteria, affecting the objective (factors) are determined.

- Technology Enablers - Foundation technologies (e.g. cloud, SDN/NFV, big data, open source) on which the platform is developed
- SIEM (Security information and event management) like functionalities, functionalities like user behaviour analysis, advanced analytics and threat mitigation
- Platform Features – Other features for added-value security, such as support for third party services, data export and infrastructure and service attestation
- Performance - Performance aspects, such as real-time operation, high availability and multi-threat support
- Business/Strategy aspects - Market related issues and compliance issues
- Ease of Use - Factors facilitating the use of the platform, such as preselected workflows, modularity, and deployment simplicity

Finally, in the third level, the criteria are further analysed into their relevance sub-criteria. Sub-criteria represent a specific feature characterizing a criterion. Identification of the criteria and their sub-criteria is accomplished based on the focus of their preferential independence.

- Technology Enablers - Foundation technologies (e.g. cloud, SDN/NFV, big data, open source) on which the platform is developed
    - Cloud/NFV/SDN Environment– Security Services running in the cloud outside or inside the company, supporting capacities for NFV+SDN management
    - Big Data technologies – Big Data technology applied (e.g. Hadoop, Spark etc.)
    - Open source - Open-source Solution, also implemented with open sourced tools and code, probably with commercial support behind
- SIEM (Security information and event management) like functionalities, functionalities like user behaviour analysis, advanced analytics and threat mitigation
    - Advanced threat mitigation - Automatic proposal of mitigation actions and enforcement of security through policies
    - Network & application analysis - Detection of ransomware activity, monitoring internet activity. Some examples are: access to files on file servers, identify root cause of bandwidth peaks on the network, abnormal application activity, application layer attack detection, fraud detection, including analytics such as statistics, descriptive and predictive data mining, machine learning, simulation and optimization to produce insights.
    - End User Monitoring/SUBA - Security User Behaviour Analytics, risk based profiling and behavioural analytics to identify statistical anomalies for network, user and device activity.

- Platform Features – Other features for added-value security, such as support for third party services, data export and infrastructure and service attestation
    - Support for third-party services and vNSFs – Capability of supporting third party services and different families of vNSFs, new vNSFs and analytics to adapt to new threats.
    - Data export and sharing - Data export and sharing with 3rd parties
    - Infrastructure and service attestation - Verification of the integrity of infrastructure and software, prevention of unauthorised modifications
- Performance - Performance aspects, such as real-time operation, high availability and multi-threat support
    - Real Time Monitoring - real-time views and threat visualizations of ongoing threat activity, collection of event data in near real time in a way that enables immediate analysis
    - SecaaS – Security as a service, High Availability of the security solution. Running the whole solution as a service, that allows scalability, redundancy and high availability
    - Multi-threat support - simultaneous attacks detection & mitigation
- Business/Strategy aspects - Market related issues and compliance issues
    - Capex -> Opex transformation and flexible pricing – Transforming the capital cost to Operational, lowering the threshold for players to enter the market, Solution with decreased cost, including lower installation and maintenance, equipment and SW costs. Flexible pricing model, per service, per use case, per data traffic, pay-as-you-go.
    - Support for new Business Models – Facilitating new players to enter the market, and traditional roles to be changed.
    - Compliance to technological Standards - support of open APIs), and standards protocols to be integrated with company systems and tools. This also includes data export and sharing capacity in standard formats.
    - Compliance to data privacy policies (GDPR[1] etc.) - Compliance to regulations and standards. No need for separate solutions for compliance, e.g.: privacy, audit and report.
- Ease of Use - Factors facilitating the use of the platform, such as preselected workflows, modularity, and deployment simplicity
    - Built-in templates and workflows - content management, management, event handling, use cases workflow to support incident response, Out-of-the-box use cases covering a variety of use cases, such as user activity monitoring, network monitoring, data exfiltration and malware activity, automation and out-of-the-box content, operational use cases (like templates).
    - Scalability/ Modularity - expandability of the platform, just by adding hardware resources. Ability for modular/incremental deployment.
    - Deployment and Support Simplicity – Easy setup, operations and maintenance; support for non-expert users.

[1] General Data Protection Regulation

Once the hierarchical structure has been constructed and the criteria and sub-criteria have been determined, appropriate questionnaires are conducted and distributed to experts (step 2) for them to fill in (available in D6.3 [2]).

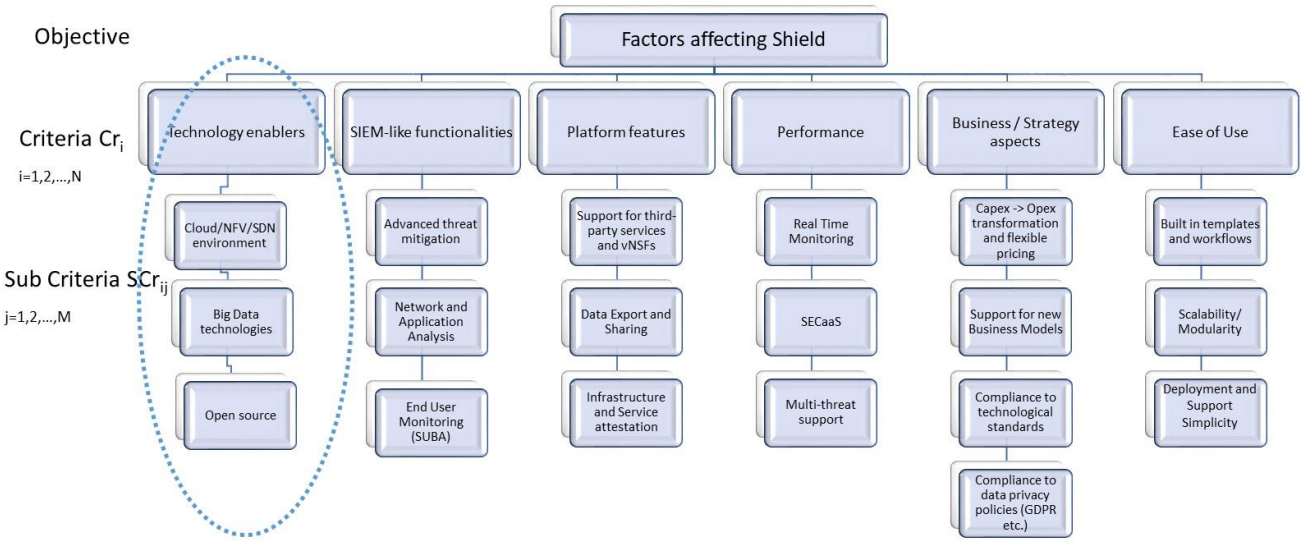


Figure 5 - Multi-level hierarchy of interrelated criteria and sub-criteria.

According to the 2nd survey results, "Performance" " was selected as the most important criterion; the market needs performant solutions that can cope with vast amounts of data under minimal response time. Based on this feedback, it can be deduced that the performance KPIs need to be reached independently of the underlying technology.

In terms of priority, "Performance" is followed by the "Ease to Use" criterion, which suggests that future solutions should be as accessible as possible and, at the same time, should be easily deployed and adopted. The remaining criteria ("Other Platform Features", "Business/Strategy aspects", "SIEM-like functionalities" and "Technology Enablers" in order of importance) are almost of equal importance indicating that the vendors/providers should give the same attention in the development of their solution, since their ranking can change in the near future. The fuzzy evaluation illustrates that there is a large degree of overlapping between the two first (Performance and Ease of Use) the four last criteria (Business/Strategy aspects, SIEM like functionalities, Platform Features, Technology Enablers). This is a clear indication that the ranking of these criteria may possibly change (a situation referred to as rank reversal) among the two first and between the other ones, especially when the solutions will become more mature.

The global priorities of sub-criteria weights indicate that the most important factors expected to affect the adoption of similar deployments in general are "Deployment and Support Simplicity", "Infrastructure and service attestation", and "SecaaS" (cloud and NFV deployments).

2.3. User stories

User stories target the specific features deemed most relevant for SHIELD. Such stories are derived from the use cases defined above, factoring in the results from the surveys and the market adoption considerations. Some features are implemented within SHIELD's lifecycle and for the targeted TRL level, while other operational features are currently in lower TRL levels (or out-of-scope within SHIELD) but are road-mapped for future work so as to improve the platform's operational capacity.

In this document, a tenant (or SHIELD client) encompasses a set of devices generating traffic that are monitored and protected by the SHIELD platform; and two (wide scope) user roles can perform actions on the platform, where Platform Operators are scoped to the entire platform, and Tenant Administrators are bounded to a specific tenant.

Table 1 – Platform user stories

Name	Description
Tenant management	As a Platform Operator, I want to perform Create, Read, Update, Delete (CRUD) operations over tenants.
Tenant administration	As a Platform Operator, I want to delegate the administration of tenant services on one or more operators.
Infrastructure troubleshooting	As a Platform Operator, I want to easily check the status of the infrastructure and quickly navigate to possible problems.
Infrastructure enumeration	As a Platform Operator, I want to navigate the infrastructure, drilling down to each device's details and status on request.
Resource allocation	As a Platform Operator, I want to allocate a quota of resources to a specific tenant.
Role taking	As a Platform Operator, I want to be able to take the role of a tenant administrator so that all the tenant functionality can be used.
Security service management	As a Platform Operator, I want to add new security services and edit or remove the available security services, which are available to all tenants of the Platform.

Table 2 - Tenant user stories

Name	Description
Service deployment	As an Operator, I want to pick a service from the catalogue and deploy it on my network.
Quota usage	As an Operator, I want to be able to monitor the amount of resources available for service deployments.

Incident reporting	As an Operator, I want to be able to see a list of incident records or incidents that happened in my network.
Incident notification	As an Operator, I want to be notified of critical events or events requiring user intervention.
Information sharing (a)	As an Operator, I want to be able to share with other entities the set of events and actions I recommend as a response.
Information sharing (b)	As an Operator, I want to be able to apply a response recommended by a third party when the same set of conditions occurs.
Service termination	As an Operator, I want to be able to remove a service from my network.
Service triggering	As an Operator, I want to be able to manually trigger periodic tasks.
Service configuration	As an Operator, I want to be able to configure each deployed service.
Action auditing	As an Operator, I want to be able to list previous actions and know who performed them.
Recommendation	As an Operator, I want to be able to see a list of recommendations from the DARE engine and choose which, if any, should be applied.
Recommendation customization	As an Operator, I want to be able to customise a recommended action before applying it to the network.

2.4. Requirements and KPIs

The requirements are collected mainly through online surveys. A publicly accessible online questionnaire is offered to relevant stakeholders, based on the SHIELD reference use cases. The complete survey is available in Appendix C1. Survey's questionnaire. The requirements detailed in this section are the result of the analysis of the information obtained in the survey, summarized in Appendix C2. Survey's results. Other requirements are consequences of the use cases proposed in SHIELD, and of regulations that can applied to SHIELD.

The requirements are accompanied by their description, their source (technical questionnaire, structural requirement or regulation) and the priority of implementation in function of their relevance to SHIELD. The requirements are grouped by functionality:

- Platform Functional Requirements (PF).
- Non-Functional Requirements (NF).
- Service Functional Requirements (SF).
- Ethical & Regulatory compliance requirements (ERC).

Each requirement has one or more associated KPIs in order to assess its fulfilment in the SHIELD platform. These KPIs are the starting point for the test plan, including simulated

threads/attacks, which will be addressed in deliverable "**D5.2 Final demonstration, roadmap and validation results**".

2.4.1. Platform Functional Requirements

ID: PF01	NAME: NS deployment
DESCRIPTION: The platform SHALL be able to deploy the NSs in different Points of Presence (PoPs) and domains. The deployment can occur within internal or external premises.	
KPI: - Deploy the same NS in two PoPs (datacentres or VIMs).	
SOURCE: TQ2	
PRIORITY: Required	

ID: PF02	NAME: NS and vNSF lifecycle management
DESCRIPTION: The platform SHALL be able to manage the full lifecycle of NSs and vNSFs (on boarding, instantiation, chaining, configuration, monitoring and termination).	
KPI: - Verify every phase of the lifecycle for each of the NSs deployed in SHIELD.	
SOURCE: Necessary to develop UC1, UC2 & UC3	
PRIORITY: Required	

ID: PF03	NAME: vNSF status management
DESCRIPTION: The platform SHALL allow the control of the lifecycle via a graphical user interface. The vNSF lifecycle should support events like START, STOP, MODIFY, DELETE.	
KPI: - Test the following functionalities via the user interface: NS deployment, vNSF configuration, NS termination.	
SOURCE: Necessary to develop UC1, UC2 & UC3	
PRIORITY: Required	

ID: PF04	NAME: Security data monitoring and analytics
DESCRIPTION: The platform SHALL be able to collect and analyse events from the vNSFs in real time in order to detect security incidents	
KPI:	

- Generate artificial security incidents and verify that these are properly detected, by checking internally generated events
SOURCE: Necessary to develop UC1, UC2 & UC3
PRIORITY: Required

ID: PF05	**NAME:** Analytics visualization
DESCRIPTION: The platform SHALL display a visualisation of the analytics' result.	
KPI: - Generate artificial security incidents and verify that the detected incident(s) and events are properly visualised in the dashboard	
SOURCE: Necessary to develop UC1, UC2 & UC3	
PRIORITY: Required	

ID: PF06	**NAME:** Ability to offer different management roles to several users (multi-user with possibility of configuring different roles).
DESCRIPTION: The platform SHALL provide domain management with accessibility to the resources of a domain by different users. The admin of a domain has to be able to create management users with different roles.	

KPI:
- Create the admin user of a domain.
- With the admin user of this domain:
  o Create other users with:
  ▪ Management privileges of NS.
  ▪ Monitoring privileges of the platform.
- Test if a management user of a NS can influence the lifecycle of a NS – such as accepting a proposed remediation, to the extent defined per operation (like instantiate and configure).
- Test if a monitoring user can access the dashboard of the platform in order to monitor the events.	

SOURCE: TQ4	
PRIORITY: Required	

ID: PF07	**NAME:** Service elasticity
DESCRIPTION: The platform COULD provide the mechanism to allow scalability of the NSs.	

KPI:
- Deploy at least one NS from the platform and analyse its correct operation.
- Verify:
  • Scale in, reducing CPU.
  • Scale out, adding memory.	

- Delete the NS
SOURCE: TQ6
PRIORITY: Optional

ID: PF08	**NAME:** Platform expandability
DESCRIPTION: The platform SHALL be easily extended to support new security services.	
KPI: - Deploy two or more different NSs from the platform and analyse their correct operation.	
SOURCE: TQ6	
PRIORITY: Required	

ID: PF09	**NAME:** Access control
DESCRIPTION: The platform SHALL provide a secure environment. Authentication mechanisms should control the access and restrict access only to authenticated users. Each user should be able to perform only the actions associated to his/her role (role-based access control).	
KPI: - Verify the authentication mechanisms for access control to the platform. - Verify that users are not allowed to perform actions which are not allowed for their role.	
SOURCE: TQ7, TQ24	
PRIORITY: Required	

ID: PF10	**NAME:** vNSF validation
DESCRIPTION: The store SHALL validate that the image of a vNSF is not manipulated, faked or invalid.	
KPI: - Replacing existing vNSF image shall be detected. - On-board vNSF with a corrupt/invalid image shall be detected.	
SOURCE: TQ7, TQ24	
PRIORITY: Required	

ID: PF11	**NAME:** vNSF attestation

DESCRIPTION: The platform SHALL check the provenance and integrity of a vNSF and, when applicable, its associated policies, before it starts to operate.
KPI: - Verify if the platform detects whether a vNSF and/or its policies have been manipulated, faked or invalid before these are instantiated and/or configured.
SOURCE: TQ7, TQ24
PRIORITY: Required

ID: PF12	**NAME:** Threat data sharing
DESCRIPTION: The platform SHALL allow to share threat data with a third entity. The granularity of such data depends on the severity and type of each attack.	
KPI: - Activate this functionality and verify that the logs can be sent to an external party.	
SOURCE: TQ38	
PRIORITY: Required	

ID: PF13	**NAME:** Mitigation
DESCRIPTION: The platform SHALL be able to trigger, in the case of an event, proper actions in order to mitigate a threat.	

KPI:
- Generate artificial security incidents and verify that the system reacts properly:
  o Deployment of new NS.
  o Configuration of vNSFs within the already deployed NSs.	

SOURCE: Necessary to develop UC1 & UC2	
PRIORITY: Required	

ID: PF14	**NAME:** Multi-user
DESCRIPTION: The platform SHALL accommodate multiple users, with isolated services and secure access to analytics.	
KPI: - Create multiple user accounts. - Verify that the services/analytics of a single user are not accessible from other user accounts.	
SOURCE: Necessary to develop UC2	
PRIORITY: Required	

ID: PF15	NAME: Service store
DESCRIPTION: The store SHALL allow selecting security services from the catalogue.	
KPI: - Publish a new NSs and associated vNSFs in the platform. - Verify that it is available to users (browse and deploy).	
SOURCE: Necessary to develop UC1 & UC2 and TQ7 & TQ24	
PRIORITY: Required	

ID: PF16	NAME: History reports
DESCRIPTION: The platform SHALL generate reports of past incidents based on historic data.	
KPI: - Generate artificial security incidents and request a report after a specific time, in the order of days. - Verify that the incident history is properly recorded.	
SOURCE: Necessary to develop UC1 & UC3	
PRIORITY: Required	

ID: PF17	NAME: Interoperability
DESCRIPTION: The platform SHALL expose openly-defined APIs for information exchange with third parties.	
KPI: - Use a test client to retrieve data via the API and confirm that the data is consistent with the actual status.	
SOURCE: Necessary to develop UC3	
PRIORITY: Required	

ID: PF18	NAME: Service composition
DESCRIPTION: The platform SHALL be able to compose security services by combining one of more of the available vNSFs.	
KPI: - Enter the NS composition section to pick at least 2 vNSFs, interconnect and configure them. - Deploy the newly composed NS and verify it is correctly instantiated and reachable by the vNSFO.	
SOURCE: Necessary to improve UC2, TQ6	
PRIORITY: Required	

ID: PF19	NAME: Network infrastructure attestation
DESCRIPTION: The platform SHALL verify that the network infrastructure executing the NSs is in a trusted state (network elements, server identity, software and their configuration).	
KPI: - Test that vNSFO provides information on newcomer nodes on the NFVI to the Trust Monitor. - Verify that the TM periodically attest the nodes. - Trigger an event of an untrusted node from TM. In response, the vNSFO removes, isolates or reconfigures such node.	
SOURCE: TQ7, TQ24, D3.1	
PRIORITY: Required	

ID: PF20	NAME: Billing framework
DESCRIPTION: The platform SHALL be compatible with a billing framework for the use of the security services. The clients should be able to access to the functionalities defined by their payment modality. It SHOULD be fully compliant to external mandatory requirements. For instance, if processing card payments as a payment service provider is part of the solution, it SHOULD be fully compliant with the Payment Card Industry Data Security Standard (PCI DSS).	
KPI: - Acquire one service through the store of services. - Allow access of the clients to their bought functionalities. - Verify the generation and availability of records files to be shared with billing framework	
SOURCE: UC2	
PRIORITY: Required	

ID: PF21	NAME: Operation Traceability
DESCRIPTION: The platform SHALL provide profile-related event generation for each of the user actions. E.g.: platform administrator, domain administrator, management user, etc.	
KPI: - Execute actions over the platform elements with the different user profiles. - Verify that the actions are logged.	
SOURCE: Telco best practices	
PRIORITY: Required	

ID: PF22	NAME: Management communication security
DESCRIPTION: The platform SHALL encrypt all the management communications.	
KPI: - Verify that all the user interactive connections make uses of ciphered protocols (SSH, HTTPs, etc.). - Monitoring traffic between different components should render no plain-text communications.	
SOURCE: Telco best practices, ePrivacy Regulation proposal	
PRIORITY: Required	

2.4.2. Non-Functional Requirements

ID: NF01	NAME: Response time
DESCRIPTION: The platform SHALL report incidents within a relatively short time (in the order of seconds).	
KPI: - Generate artificial incident and measure the delay of the system response.	
SOURCE: General requirement.	
PRIORITY: Required	

ID: NF02	NAME: Availability
DESCRIPTION: The core platform SHALL be able to recover in case of hardware failures.	
KPI: - Manually fail a hardware node and verify the platform recovery time (less than 1 min).	
SOURCE: General requirement.	
PRIORITY: Required.	

ID: NF03	NAME: Scalability
DESCRIPTION: The storage and processing capabilities of the platform SHALL be able to increase merely by adding resources to the system.	
KPI: - Install a new computing node in the SHIELD platform. - Verify the availability of the new node in the vNSFO. - Verify the increase in storage capacity and the decrease of processing time.	
SOURCE: General requirement, results of SHIELD road mapping survey (D6.3).	

PRIORITY: Required

ID: NF04	**NAME:** Data volume
DESCRIPTION: The platform SHALL be able to handle data in the order of Terabytes.	
KPI: - Inject traffic to the network. - Verify that the vNSF environment can monitor it, the Big Data Engine can analyse it and the dashboard and rest of the system can provide appropriate events and remediation suggestions.	
SOURCE: General requirement.	
PRIORITY: Required	

ID: NF05	**NAME:** Impact on perceived performance
DESCRIPTION: The platform SHALL not degrade the user experience when network traffic is proxy'd or analysed.	
KPI: - Activate the various service chains. - Verify that the user's quality of experience on the various services is not seriously degraded.	
SOURCE: General requirement.	
PRIORITY: Required	

ID: NF06	**NAME:** Performance Factors
DESCRIPTION: The platform SHALL offer an availability-related performance similar to carrier grade system. It includes recovery time and redundancy capability.	

KPI:
- Restart a vNSF in a service
  o Measure recovery time in reasonable time (e.g. less than 1 minute).
- Test DARE redundancy with one node failure.
  o Measure recovery time in reasonable time (e.g. less than 5 minute).	

SOURCE: Results of SHIELD road mapping survey (D6.3)	
PRIORITY: Required	

ID: NF07	**NAME:** Compliance to standards
DESCRIPTION: The platform SHALL conform to well-established standards, in particular with respect to data export (e.g. STIX) and input (e.g. NetFlow).	
KPI:	

- Feed the platform with standards-compliant inputs from external sources (e.g. NetFlow data captured from the Internet). - Verify that it is properly parsing them. - Validate the platform output with a standards-compliant parser (such as the STIX Validator https://github.com/oasis-open/cti-stix-validator).
SOURCE: Results of SHIELD road mapping survey (D6.3).
PRIORITY: Required

ID: NF08	**NAME:** Deployment and support simplicity
DESCRIPTION: The platform SHALL be easily installed and maintained, without the need of specific expertise.	
KPI: - Verify that the platform can be installed by someone outside the SHIELD technical team (yet with basic technical background), just by referring to the accompanying documentation.	
SOURCE: Results of SHIELD road mapping survey (D6.3), Criteria Ease to Use SC63 Deployment and Support Simplicity.	
PRIORITY: Required	

ID: NF09	**NAME:** vNSF hardening
DESCRIPTION: The vNSFs SHALL be hardened. All deployed NSs have to satisfy at least the following statements: - All management communications have to be encrypted. - The services have to have installed with the minimum set of applications to provide the vNSF function. - Applications have to expose only needed interfaces or APIs. If something is not used, it has to be disabled or removed. - Applications have to provide security events. - Applications have to provide access control allowing connections only from specific IPs.	
KPI: - For each vNSF offered in SHIELD platform it's necessary to audit, i.e.: o Inspect that all management traffic is encrypted. o Verify that the vNSF doesn't deploy and run unnecessary services (i.e. man pages, ftp, telnet, web services - if they are not necessary). o Configure a management access filter in the vNSF to allow only the access from an IP and verify if only it is possible to connect to the vNSF from this IP. o Try to access to the vNSF with wrong and correct management password and verify that provide the security events with these actions	

SOURCE: Telco best practices, ePrivacy Regulation proposal
PRIORITY: Required

2.4.3. Service Functional Requirements

ID: SF01	**NAME:** Content filtering
DESCRIPTION: A security service COULD provide URL filtering based on different configurable categories (e.g. political, violence, sex, social networks, etc.) for internet web browsing.	
KPI: - Test that the platform can deploy one or more NSs able to provide this service: o Check the content filtering using traffic related to 2 categories. o Verify that the logs or notifications in the platform dashboard inform about this.	
SOURCE: TQ8	
PRIORITY: Optional	

ID: SF02	**NAME:** Detect/Block access to malicious network locations
DESCRIPTION: A security service SHALL control access to malicious network locations, such as phishing servers, malware spreading websites, Command & Control (C&C) servers, etc. The user must be alerted and the access to the site could be blocked/allowed depending on the configured policy rule.	
KPI: - Test that the platform can deploy one or more NSs able to provide this service. o With the service in block mode, access to a malware web site: ▪ Verify if it is detected and the user is warned and the web access is blocked. ▪ Verify that the logs or notifications in the platform dashboard inform about this. o With the service in warning mode, access to a malware web site: ▪ Verify if it is detected and the user is warned. ▪ Verify that the logs or notifications in the platform dashboard inform about this.	
SOURCE: TQ9, TQ10, TQ27, TQ35	
PRIORITY: Required	

ID: SF03	**NAME:** Security assessments

DESCRIPTION: A security service COULD provide continuous vulnerability assessment on the network, hosts or applications.
KPI: - Test that the platform can deploy one or more NSs able to assess various security aspects of the internal network, hosts and applications.
SOURCE: TQ14
PRIORITY: Optional

ID: SF04	**NAME:** L4 traffic filtering
DESCRIPTION: A security service SHALL monitor traffic based on configuration rules. Traffic packets are filtering and specific traffic is either allowed, rejected or blocked based on a predefined set of rules (usually based on source IP, destination IP, destination port, etc.).	
KPI: - Test that the platform can deploy one or more NSs able to provide this service. - Verify filtering and blocking operation of this functionality. - Verify that the logs or notifications in the platform dashboard inform about this.	
SOURCE: TQ33, TQ15, TQ16	
PRIORITY: Required	

ID: SF05	**NAME:** Central log processing/SIEM
DESCRIPTION: A security service COULD collect and correlate security logs from different legacy user sources and generate alerts. This service is intended to provide the user with a way to process its security logs that are not generated by a vNSF in SHIELD.	
KPI: - Test that the platform can deploy one or more NSs able to provide this service. - Verify the correct reception/validation/processing of the logs.	
SOURCE: TQ19	
PRIORITY: Optional	

ID: SF06	**NAME:** Malware detection
DESCRIPTION: A security service COULD detect (and optionally clean) files with malware downloaded from Internet.	
KPI: - Test that the platform can deploy one or more NSs able to provide this service. - Verify this functionality after downloading malware infected. The user must be warned and these files must be deleted.	

- Verify that the logs or notifications in the platform dashboard inform about this.
SOURCE: TQ25
PRIORITY: Optional

ID: SF07	**NAME:** Spam protection
DESCRIPTION: A security service SHALL protect against unwanted emails, based on source reputation lists and content analysis.	
KPI: - Test that the platform can deploy one or more NSs able to provide this service. - Verify this functionality analysing if the service do the correct filtering of SPAM in the email. - Verify that the logs or notifications in the platform dashboard inform about this.	
SOURCE: TQ26	
PRIORITY: Optional	

ID: SF08	**NAME:** Denial of Service (DoS) Protection
DESCRIPTION: A security service SHALL protect against volumetric Denial of Service attacks.	
KPI: - Test that the platform can deploy one or more NSs able to provide this service (detect non-legitimate traffic). - Verify the volumetric protection by analysing its behaviour during traffic of the order of Gigabytes (5-10, and optionally 100s). - Verify that the logs or notifications in the platform dashboard inform about this to divert traffic for filtering. - Verify that the good traffic flows to its destination.	
SOURCE: TQ29	
PRIORITY: Required	

ID: SF09	**NAME:** Intrusion Detection/Prevention System
DESCRIPTION: A security service SHALL detect attacks with a wide range of techniques such as network flow or behaviour analysis and deep packet inspection.	
KPI: - Test that the platform can deploy one or more NSs able to provide this service (intrusion detection/prevention).	

- Verify this functionality analysing:
  o Alerting of malicious activities (infections, information leakage, configuration errors and unauthorized clients).
  o Blocking of malicious traffic.
- Verify that the logs or notifications in the platform dashboard inform about this.

SOURCE: TQ30, TQ32, TQ37
PRIORITY: Required

ID: SF10	**NAME:** Honeypots
DESCRIPTION: A security service COULD provide a Honeypot service that simulates or impersonates specific services (e.g., Windows computer, Web server, IoT or SCADA device, etc.) in order to detect malicious behaviours in the network.	
KPI: - Test that the platform can deploy one or more NSs able to provide this service. - Verify this functionality with traffic addressed to the Honeypot. - Verify that the platform can provide behaviour analysis after the attacker has operated during a determined amount of time or amount of commands (E.g. 1 hour of activity or 20 commands executed). - Verify that the logs or notifications in the platform dashboard inform about this intrusion.	
SOURCE: TQ34	
PRIORITY: Optional	

ID: SF11	**NAME:** Sandboxing
DESCRIPTION: A security service COULD provide a sandbox service for executing and analysing programs.	
KPI: - Test that the platform can deploy one or more NSs able to provide this service. - Verify the security logs generated in the platform dashboard.	
SOURCE: TQ37	
PRIORITY: Optional	

ID: SF12	**NAME:** Virtual Private Network (VPN)
DESCRIPTION: A security service COULD provide a secure tunnel service in order to connect the branch of a client with users on the Internet or other branches.	
KPI: - Test that the platform can deploy one or more NSs able to provide this service. - Verify the correct functioning of the traffic through the VPN.	

- Verify that the traffic is encrypted and that the communication metadata are deleted (unless used for billing).
SOURCE: TQ31, TQ22, ePrivacy Regulation proposal
PRIORITY: Optional

2.4.4. Ethical & Regulatory compliance requirements

The ethical requirements are derived from the relevant legislation:

- **General Data Protection Regulation: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance):** The GDPR is in place to safeguard citizens' rights in terms of privacy and data protection. It applies to all components that store or process personal data. It also includes data portability to ensure compliance with EU competition laws and avoid customer lock-in conditions.
- **Open Internet Regulation: Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union (Text with EEA relevance):** The Open Internet Regulation establishes rules for net neutrality. It lists traffic classification and rate limiting for the purpose of security as a fair practice. SHIELD should include a level of transparency on why limiting rules might be applied.
- **Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications):** This Directive is expected to be replaced by an ePrivacy Regulation that is being proposed. It applies to communication providers that need to ensure the security and confidentiality of personal communications, and it is extended to safeguard cookies and other online identifiers.
- **European Charter of Fundamental Human Rights, esp. Article 8(1)** on the protection of personal data, establishes privacy as a fundamental human right.
- **Treaty of Amsterdam (1997/1999 establishing the protected grounds against discrimination) & Treaty of Lisbon (2007/2009 making the ECHR Bill of Rights legally binding):** The definition of discrimination can be considered free-standing and useful to protect citizen rights in data processing activities that can profile their behaviour.

A detailed analysis of the ethical and regulatory framework that applies to SHIELD is included in deliverables **D3.2** [3] and **D4.2** [4], which provide ethical and regulatory compliance specifications for the vNSF ecosystem and the DARE. Based on the analysis and the input of SHIELD's external Ethics Advisor (Haralambos Mouratidis, University of Brighton), a set of requirements is also extracted fot the SHIELD platform. The basis for the derived requirements is that :

- SHIELD's end-to-end decision making needs to be transparent: This applies to processing (based on the GDPR) and to traffic management (based on the Open Internet Regulation).
- The data subject should be able to control their data .
- No unecessary processing or profiling shoud take place.
- There should be accountability and access to a Data Protection Officer and to all related Data Protection Information.
- In case of a data breach, there should be fast response and a timely notification should be sent by the Service Provider.

ID: ERC01	NAME: Access to and portability of personal data
DESCRIPTION: All components that process and/or store personal, identifiable information SHALL provide data subjects with a way to access and review their personal data. If the data processing does not require identification, the component is not required to provide access, unless the user can provide additional information enabling their identification (according to Article 11 of the GDPR).	
KPI: - An easy-to-use GUI should be available for a user who requires to review the data collected and the data processing activities performed by the SHIELD component. SHIELD components which process data, but which do not require identification must demonstrate that they are not in a position to identify the data subject. - Any data that can be used to identify or profile the user should be exportable in a standard format. The data should be portable to another service provider, to avoid customer lock-in conditions	
SOURCE: EU GDPR Section 2 (Art. 13-15, 20), Results of SHIELD road mapping survey (D6.3), fair competition	
PRIORITY: Required	

ID: ERC02	NAME: Data rectification and erasure
DESCRIPTION: All components that process and/or store personal, identifiable information SHALL provide data subjects with a way to request that their data be rectified or erased. If the data processing does not require identification, the component is not required to provide this functionality, unless the user can provide additional information enabling their identification (according to Article 11 of the GDPR).	
KPI: - An easy-to-use GUI should be available for a user to submit a request for erasure or rectification. - The subject's data should then be erased or rectified in the related storage medium.	
SOURCE: EU GDPR Section 2 (Art. 13-15).	

PRIORITY: Required

ID: ERC03	**NAME:** Access to related Data Protection information
DESCRIPTION: The platform SHALL provide the data subject with easy access to the following information: - The identity and contact details of the data controller(s) - The identity and contact details of the Data Protection Officer - The purpose of processing and categories of data concerned - The recipients of the collected data - A statement on transfer of data to third parties (including cross-border) - An interface that allows the user to lodge a complaint to the Data Protection Officer	
KPI: - An easy-to-use webpage should be available to the clients of SHIELD services, detailing this information.	
SOURCE: EU GDPR Chapter 3 (Art. 13-14).	
PRIORITY: Required	

ID: ERC04	**NAME:** Transparency in data processing
DESCRIPTION: The platform SHALL present visibly and transparently the technical information pertaining to the components' data processing. Data processing activities should be logged.	
KPI: - The user who chooses to on-board a vNSF or NS should be able to view its data processing specifications in the Store. This will allow the user to have a priori knowledge of the data processing capabilities of service he wishes to use. - The dashboard should also provide information on the data processing activities performed by the NS and active vNSFs. - Analytics engines should provide this information on their related user interfaces. - All additional UI elements should be added, with clear definition and should also avoid technical jargon.	
SOURCE: EU GDPR Chapter 2 (Art. 13-15), Chapter 4 Art. 30, ePrivacy Directive	
PRIORITY: Required	

ID: ERC05	**NAME:** Data retention
DESCRIPTION: The components storing and processing personal identifiable data SHALL define a specific data retention period.	

KPI: - The data retention period must be visible in the dashboard or any related user interface. - Data should be safely removed after the designated retention period.
SOURCE: EU GDPR
PRIORITY: Required

ID: ERC06	**NAME:** Transparency in traffic classification
DESCRIPTION: Components with the ability to classify traffic and apply throttling/limiting measures SHALL provide detailed information.	
KPI: - Every action to throttle or block traffic based on application type should be logged and attached to a specific security event, to prevent misuse of the system to restrict internet access to specific application providers.	
SOURCE: Open Internet Regulation (EU) 2015/2120 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015R2120	
PRIORITY: Required	

ID: ERC07	**NAME:** Notification obligation
DESCRIPTION: In the case of a breach in a component that processes personal data, the platform SHALL produce a breach notification. Data rectification or erasure should be accompanied with a notification to the data subject unless it is difficult or involves disproportionate effort, as per article 19 of the GDPR.	
KPI: - The Trust Monitor sends a notification if it detects a breach in a SHIELD NS.	
SOURCE: EU GDPR Art 19 & 33	
PRIORITY: Required	

ID: ERC08	**NAME:** Net Neutrality
DESCRIPTION: The platform SHALL not recommend actions that lead to user traffic penalization, unless explicitly required for threat mitigation. The net neutrality rules adopted by the European Parliament on 30 April 2016 aimed to strengthen net neutrality by requiring internet service providers (ISPs) to treat all traffic equally, without favouring some services over others. For this reason, no service could be used by an ISP to punish or to favour the traffic of a user respect the rest of the users.	
KPI: - Check that in the dashboard the user is informed about this condition before to apply a recommendation policy, i.e. a warning in the dashboard with the information.	

SOURCE: BEREC (Body of European Regulators for Electronic Communications).
PRIORITY: Required

ID: ERC09	**NAME:** Lawful Interception
DESCRIPTION: The vNSFs SHALL support LI capacities, or integrate a LI system, if the vNSF changes the public IP address (for Internet connection) or encrypts the internet traffic. LI capacities are defined by ETSI. Law enforcement agencies may require access to a number of transmitted telecommunications regarding a particular subject, target, date, etc. If network operators/service providers initiate encoding, compression or encryption of telecommunications traffic, law enforcement agencies require the network operators/service providers to provide intercepted communications in clear.	
KPI: - Verify if, in the affected vNSFs, it is possible to perform the LI for a specific user traffic according to ETSI definition.	
SOURCE: Council Resolution on the lawful interception of telecommunications http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31996G1104.	
PRIORITY: Required	

ID: ERC10	**NAME:** LEA Data Retention
DESCRIPTION: The vNSFs SHALL store the data associated to a user, if the vNSF changes the public IP address (for Internet connection). According to the directive "Directive (EU) 2016/680", article 5: "Member States shall provide for appropriate time limits to be established for the erasure of personal data or for a periodic review of the need for the storage of personal data. Procedural measures shall ensure that those time limits are observed." For telecommunications data, this time limit typically ranges from minimum of 6 months to at most 24 months.	
KPI: - Verify that the concerned vNSFs provide a way to store the information about the IP associated to the user during the established periods. - Verify that the concerned vNSFs erase the personal data after a given time.	
SOURCE: Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0680	
PRIORITY: Required	

ID: ERC11	**NAME:** Privacy and Security by-design
DESCRIPTION: Services SHALL be designed according to security and privacy best practices:	

• When identification of the individual is not necessary, data SHALL be anonymised or pseudonymised. • Easily readable specifications SHALL be available and the user should be able to understand the data processing capabilities of a given service or component. • Components that store identifiable data SHALL use encryption. • User behavioural profiling SHALL not be used unless it is considered necessary and proportional. • Remediation actions SHALL be transparent and not based on a user's behavioural history (e.g. profiling of religion, health, political views, race, gender etc.)
KPI: - Verify that every vNSF provide the compliance specifications in the Store. - Verify that the user are able to easily access this information. - Verify that the specific remediation actions are associated with specific security events.
SOURCE: GDPR Art.25, ePrivacy Directive, GDPR definition of profiling and EU non-discrimination law.
PRIORITY: Required

ID: ERC12	NAME: ePrivacy
DESCRIPTION: Services SHALL protect the contents of personal communications. A service should not inspect personal communications or store communications metadata for other purposes. The user should be notified if any online identifiers are being used by a service (e.g. login credentials, a device ID etc.)	
KPI: • Verify the data retention period for inspected communication metadata (e.g. packet headers, device IDs etc.)	
SOURCE: ePrivacy Directive & Proposal for ePrivacy Regulation	
PRIORITY: Optional (pending finalisation of the ePrivacy Regulation)	

3. SHIELD SOLUTION

3.1. Architecture overview

The SHIELD project aims at securing against intruders and other threats through a vNSF-enabled environment. To achieve this goal, the architecture is articulated around different components, illustrated in Figure 6 and described more deeply in this section.

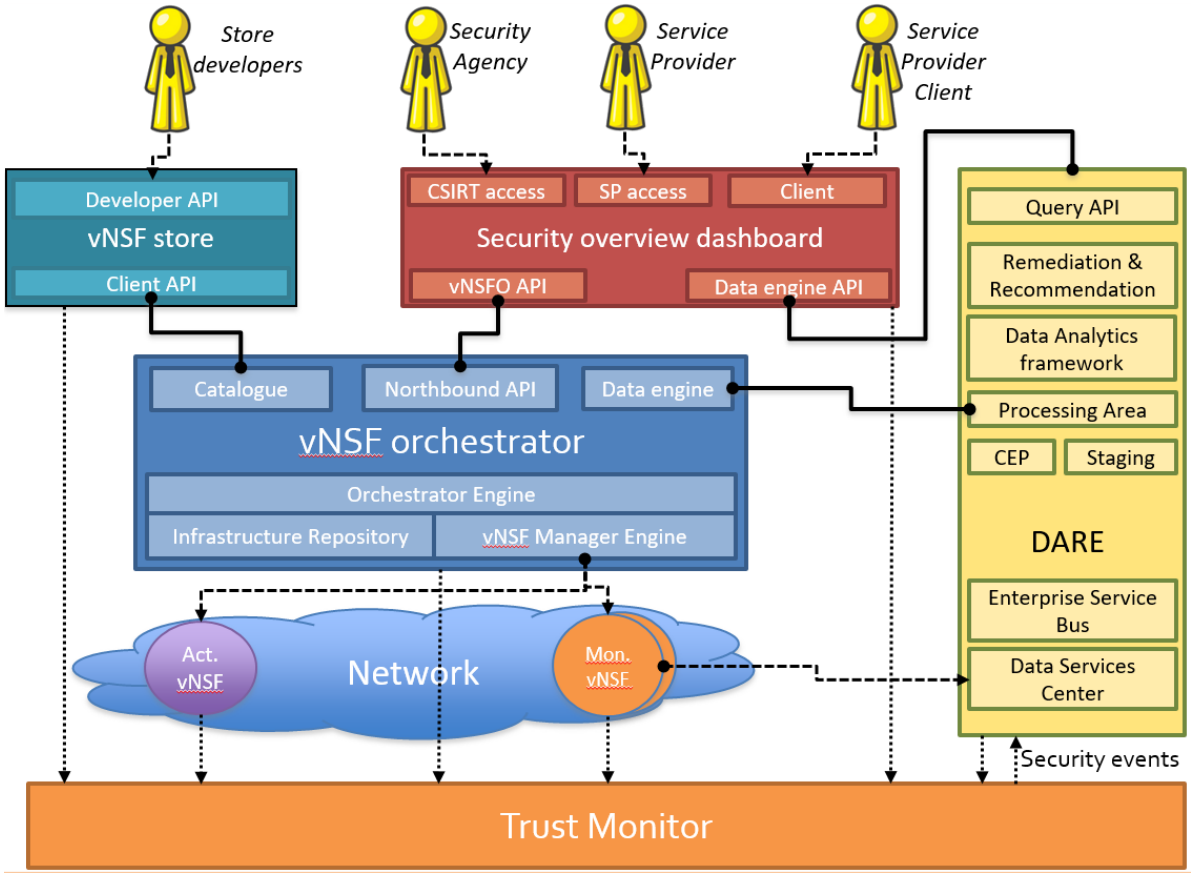


Figure 6 - SHIELD architecture overview

3.1.1. Description of the SHIELD's main components

In a nutshell, the Network infrastructure is the running space for the vNSFs, the DARE stores and analyses the security logs and events provided by the former; and finally the security dashboard presents the results to the operator. These core components are supported by i) the vNSF store, which holds the vNSFs images; ii) the vNSFO, which manages the NSs and their vNSFs; and iii) the Trust Monitor, which verifies that the SHIELD platform is trusted at all time.

3.1.1.1. Network infrastructure

The network infrastructure supports the instantiation of Virtual Network Security Functions (vNSFs). Creating a NS, the vNSFs can be considered as security appliances dynamically deployed on the network infrastructure. SHIELD identifies two main types of vNSFs:

1. Monitoring vNSFs are devoted to gather information about the network, generate alarms and triggers in case of ongoing attacks.
2. Acting vNSFs apply the necessary mitigations to pre-empt attacks and protect against known vulnerabilities and threats, or mitigate them as a security incident evolves. The proper acting vNSF is chosen depending on the kind of threat detected (if not already present).

The network infrastructure interacts with the Trust Monitor in order to authenticate the integrity of each network component. The network infrastructure is interconnected with the vNSFO allowing the deployment of vNSFs, their lifecycle management and the collection of monitoring data. Monitoring vNSFs inspect captured data and provide valuable information to the Data Service Engine component of the DARE. The network status is reported periodically since more complicated events (i.e. an attack using multiple vectors), could sometimes not be detectable by individual vNSFs but can be inferred by the DARE. These interactions are illustrated in Figure 6.

Given the ETSI NFV specifications [5] [6] [7] [8] [9] [10], the network infrastructure layer includes the physical and virtual nodes (commodity servers, VMs, storage systems, switches, routers etc.) on which the services are deployed. Following the ETSI NFV infrastructure working group (focused on the specification of the NFV infrastructure), a few logical domains are considered to disaggregate the complexity of the required capabilities (see Figure 7):

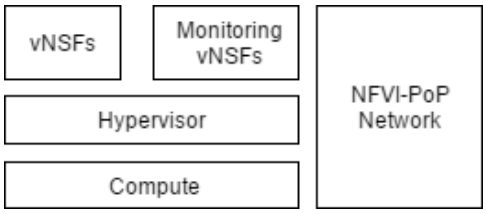


Figure 7 - High-level view of NFV Infrastructure

- The Compute domain, operates at the lowest level; it is composed of the computing and storage slices. This comprises the generic high-volume servers and storage. The underlying physical elements are abstracted by the hypervisor, as it allows aggregation of these resources across many discrete servers and assignment of them to vNSFs. The compute domain should collect metrics on the performance of the physical resources and make them available to the Orchestrator.
- The Hypervisor domain, operating at a virtual level, provides abstraction of the hardware to the vNSFs. This supports capabilities such as portability and scalability of the vNSFs. The hypervisor is also responsible for the allocation of the compute domain resources to the VMs and provides a management interface to the vNSFO which supports the loading and monitoring of VMs and vNSFs. The hypervisor is also responsible for network connectivity between VMs hosted either on the same or different physical servers. The NFVI Hypervisor domain should be able to implement hardware resource abstraction, virtual resource lifecycle management mechanisms (coordinated by the vNSFO), and to provide to the vNSFO monitoring information with minimal impact on the vNSFs workload performance.
- The Network domain, operating both at virtual and hardware levels of the network slice. It comprises all the generic high-volume switches interconnected of a network, which can be configured to supply infrastructure NSs. The NFVI network domain should

implement an SDN approach to provide network virtualization capabilities inside the NFVI-PoP (creation of multiple distinct domains over one single physical network using VLANs).

Finally, physical devices of the network infrastructure embed a hardware security component, such as a Trusted Platform Module, which can be used as root of trust for verifying all the logical domains and layers on this device. This hardware security component is not enough,careful attention is therefore required in the selection of firmware and software layer to allow the trust verification of the device and the vNSFs it executes.

3.1.1.2. Virtual Network Security Function

If left up to the supplier, the vNSF ecosystem can be highly heterogeneous. SHIELD supports such diversity. Yet, some constraints must be met in order for vNSFs to securely interact with the platform. This section deals with the architectural constraints for a vNSF. Specific details on the implementation mechanisms and APIs, as well as communication channels, will be specified later. A detailed design of NSs and their vNSFs is provided in **D3.2 ("Updated specifications, design and architecture for the vNSF ecosystem")** [3].

In terms of vNSF architecture, the main differentiating factor in SHIELD is the addition of the attestation capacity to the platform. This directly impacts the technical implementation of the vNSF that can be deployed there.

Each vNSF has a series of interfaces, separating each type of data into different interfaces and thus allowing traffic segmentation. This level of segmentation introduces some complexity, but also allows better service isolation:

- One interface is used for communication with the vNSFO, allowing configuration and control connections. Any administrative functionality should run on this interface. If possible, this interface should be named "management".
- Another interface is used for communication with the DARE, used to report incidents. If possible, this interface should be named "monitoring data".
- A third interface should be used for attestation operations only, where available. This interface, if present, should be called "attestation".

The data plane interfaces should be prefixed by "data_" and followed by a suffix indicative of their purpose. An example would be "data_in" and "data_out" for a proxy vNSF.

The SHIELD developers will supply in time a set of example NS and vNSF descriptors and comprehensive documentation. These shall enable third party developers to package existing and new NSs or vNSFs in accordance to SHIELD's platform guidelines.

3.1.1.3. vNSF orchestrator

The vNSF orchestrator, or vNSFO, is responsible for managing the lifecycle of NSs. To that end, the vNSFO interacts with each of the other modules to obtain data on the vNSFs, to receive deployment and configuration requests, or to convey data of running nodes. The vNSFO also communicates with the vNSF Manager to delegate the management of the vNSFs that are part of the requested NS. Detailed data about those processes is available at different interaction

points of the platform being: the Store-vNSFO, vNSFO-Security Dashboard, vNSFO-DARE and vNSFO-Infrastructure.

The vNSFO internals are described as follows:

- The NS and vNSF Managers handle the lifecycle of the NSs and vNSFs. The related operations include the provisioning and instantiation (deployment on the infrastructure), configuration (modification of internal status), scaling (increase/decrease capacity used by the VMs) and termination of virtual machines to release the allocated resources on the infrastructure.
- Repositories and registries containing run-time information, such as running instances of both NSs and vNSFs, and an insight of the available NFVI resources.
- Connectors and APIs that allow requesting data from other inter-related components running in SHIELD, as well as exposing data from the vNSF environment to other components.

3.1.1.4. vNSF store

The vNSF store acts as a nexus between the vNSFO and the developer, which can register, manage vNSFs and make them available for later use. The following vNSF data is provided to the store:

- The **service descriptor** contains information such as the developer's identity or versioning information (metadata), but it can also provide technical details concerning deployment requirements (e.g. vCPUs, image location) and any other metadata required for proper validation within the store.
- The software **images** contain the functionality that is instantiated. The number of images contained in a vNSF is related to the number of Virtual Deployment Units (VDU), which is at least one.
- The **security descriptor** contains information required to validate its integrity as well as the integrity of the files embodying the service, at all the critical moments (on boarding, deployment and runtime).

The store provides two interfaces to cover this functionality:

- The **Developer API** provides interaction with the vNSF developer. It allows to i) upload a new NS or vNSF, ii) update its information, and iii) remove it. These operations are valid for managing both the vNSF descriptors and the vNSF images.
  Before a NS can be instantiated within the platform, the developer must upload it to the store. All the uploaded data is stored in the catalogue's sub-components. The update operation is useful when developing a new version for a NS or vNSF, as the developer can update it on the store, which also keeps track of the history. Finally, the deletion of a NS or vNSF and all its tracked versions is possible too.
- The **Client/deployment API** provides interaction with the vNSFO. It is later detailed in the Store-Orchestrator interface.

Besides the functionality described above, the store also performs internal operations for:

i) Validating the vNSF descriptor
   The descriptor must contain proper metadata, so that its vNSF can be properly instantiated later on. The store verifies this during the vNSF upload.
ii) Validating the vNSF images

Similarly to the descriptor, the images must be valid as well. Upon uploading an image, a preliminary unitary deployment should be performed to verify that it can run properly.

iii) Supporting the vNSF attestation

The security descriptor carries an integrity proof per VDU. The store validates the integrity of the file images against this proof. When the deployment stage starts, the hash is used to attest whether the running instances of the vNSF corresponds to the ones retrieved from the store. Extra information is passed to the Trust Monitor in order to allow it to perform run time verification. The integrity of the security descriptor itself is checked via digital signature using a certificate known to belong to the submitter.

3.1.1.5. Trust Monitor

The Trust Monitor is the component in charge of monitoring the trustworthiness of the SHIELD infrastructure. This is achieved by a combination of authentication and integrity verification techniques: each node joining the infrastructure must be properly authenticated and must also provide a proof of the integrity of its software stack, by leveraging Trusted Computing (TC) mechanisms.

Integrity is also checked periodically to detect compromised software and if so, timely inform the security expert to take appropriate action via the security dashboard (typically, to quickly isolate the compromised node and reconfigure the infrastructure in order to maintain its expected functionality). Integrity is an important concern, not only with the code of the components executed on the nodes, but also with their configuration - both at initialization (i.e. configuration files) and runtime (i.e. memory state, particularly relevant for components updating their configuration dynamically, such as OpenFlow switches). These actions are accompanied by log events and alarms, to provide evidence about the history status of the infrastructure, both for audit and eventual forensic analysis.

Integrity monitoring is based on the Trusted Computing paradigm and its Remote Attestation [11] workflow. Each node is equipped with a Trusted Platform Module (TPM) chip to provide a hardware root of trust. Additionally, suitable software is installed to measure all the relevant actions (from the boot phase up to the applications) and to report them in a secure and trusted way. The integrity report is digitally signed with a hardware key from the TPM and includes the values of the secure TPM registers (i.e. the Platform Configuration Registers – PCRs) as well as the log of all tracked software events as measured by the Integrity Measurement Architecture (IMA) Linux component. The elements in this integrity report are then checked against a whitelist of values for known-good software components and valid configurations.

Devices not based on Linux (such as the hardware network switches), shall also embed a TPM and provide equivalent measurement mechanisms so that the Trust Monitor can evaluate their integrity.

3.1.1.6. Data Analysis and Remediation Engine

The Data Analysis and Remediation Engine (DARE) is an information-driven Intrusion Detection and Prevention System (IDPS) platform that stores and analyses heterogeneous network information, previously collected via monitoring vNSFs. It features cognitive and analytical components capable of predicting specific vulnerabilities and attacks. The processing and

analysis of large amounts of data is carried out by using Big Data, data analytics and machine learning techniques. By processing data and logs from vNSFs deployed at strategic locations of the network, the DARE components provide information for the development of cybersecurity topologies (mitigation recipes), meaning that in case malicious activity is detected, they implement remediation activities, either by recommending actions through the means of a dashboard and accessible API, or by (optionally) triggering task-specific countermeasures. The DARE platform provides flexible support for both new security capabilities and reconfiguration of existing security controls. Also, the DARE aims at facilitating its extension with multiple data analytics engines by providing a clear API to work with the collected data.

The DARE consists of three main components: the data acquisition and storage module, the data analytics engine and the remediation engine.

The data acquisition and storage module is responsible for the ingestion of the selected datasets and their preparation for further processing. This module is composed of different types of data collectors and workers following the Apache Spot [12] architecture. It therefore supports network flow, Domain Name System (DNS) and web proxy logs collection and transformation. These three aspects are considered the main data sources that can be used by any IDPS, thus they are adapted to the needs of SHIELD. The ingest chain has been appropriately designed to support both a centralised collection and pre-processing architecture (i.e. pushing raw unprocessed data from the vNSFs to the DARE filesystem) as well as a distributed one (using agents at the monitoring vNSFs to locally preprocess and filter data before dispatching it to the DARE). The considered actions are the following: i) cleaning to remove erroneous samples; ii) curating by adding metadata that helps in the indexing process; iii) enriching the samples by correcting misspellings or missing fields; and iv) integrating datasets if necessary. In order to take advantage of other data types produced by the vNSFs, such as alerts and metrics, additional collectors and workers are also being developed, so that they can be integrated to the DARE ingestion mechanism.

The data analytics engine leverages two different Data Analytics modules (while opening the platform for the inclusion of new modules in the future) using a wide range of complementary detection techniques along with open source frameworks and solutions.

The cognitive Data Analytics module produces packet and flow analytics by using scalable machine-learning techniques. To this end, it involves the latest distributed computing technologies (e.g. Apache Spot, Spark, Hadoop Distributed File System (HDFS), Kafka, Hive) to allow for stream and/or batch processing of large amounts of data, scalability, load balancing, open data models and concurrent running of multiple machine-learning applications on a single, shared, enriched data set.

The threat detection procedure of the cognitive module is based on the Apache Spot [12] framework. Specifically, the ingested data is available for searching, for use by machine learning algorithms, to be transferred to law enforcement, or as an input to other systems. Subsequently, the system uses a combination of machine learning tools to run scalable machine learning algorithms (e.g. Latent Dirichlet Allocation - LDA), not only as a filter for separating bad traffic from the benign one, but also as a way to characterize the unique behaviour of network traffic. Finally, and in addition to machine learning, a process of context enrichment, noise filtering, whitelisting, and heuristics is applied to network data, in order to present the most likely patterns that may comprise security threats.

A dependable security Data analysis module that is based on a combination of Big Data analytics and machine learning techniques to process and analyse a vast amount of network data, as well as automatically discover and classify cybersecurity threats. It receives network flows from the distributed storage system to detect anomalous behaviours related to security issues. Once a suspicious behaviour is detected, an anomaly classifier is set responsible of classifying it among different network attacks (e.g., Distributed Denial of Service (DDoS), network scan). This module is adapted to the DARE in order to collaborate with the cognitive Data Analysis module, covering different techniques and approaches that improve the analysis results done by SHIELD.

Finally, the Remediation engine uses the analysis from the data analytics modules and is fed with alerts and contextual information to determine a mitigation plan for the existing threats. It performs in real-time or near-real-time, generating a cybersecurity topology for a detected threat, which is converted into a high-level abstraction of a remediation recipe. The Remediation Engine's main goal is to incorporate a combination of recommendations and alerts that provide relevant threat details to all interested parties using the dashboard and the direct application of countermeasure activities by triggering specific vNSFs via the vNSFO (e.g. block/redirection of network flows). Available information generated by the engine can be used in order to assist SP and Computer Emergency Response Team (CERT) management decision-making. Moreover, it may optionally include automatic remediation.

Last but not least, SHIELD uses a combination of datasets in order to train and test the algorithms. These datasets are obtained from data used in other initiatives in the field of security or the monitoring of university networks, after proper anonymisation.

3.1.1.7. Security dashboard

The SHIELD platform provides an intuitive and appealing graphical user interface allowing its authenticated and authorized users to access SHIELD's security dashboard. From this dashboard, operators have access to monitoring information showing an overview of the security status as well as allowing operators to take actions and react to any detected vulnerability. Billing features will also be present in the security dashboard allowing providers to measure and charge operations made by clients (for instance, the acquisition/instantiation of a new vNSF).

Being the only interface available to a SHIELD user the Dashboard is the operational gateway to the platform. As such, it provides security-related features comprising vNSF and NS lifecycle management, threat detection notifications, threat mitigation actions review and application, untrusted nodes alerts, service status, and information exchange with cyber agencies, either by interacting with the platform itself or through a Representational State Transfer (REST) API tailored for such purpose.

Additional operation and maintenance features related to typical tenant and user management, as well as auditing, shall also be provided; these features are implemented in a simplified fashion as the project's main goal is not to produce a comprehensive user management platform (and other third-party implementations may be introduced to address that).

3.1.2. Inter-component communication

3.1.2.1. Store-vNSFO

The interaction between the Store and the vNSFO takes place after a client initiates a request on the Dashboard for the deployment of a given NS. The Dashboard queries the Store, which will obtain the pertinent SHIELD packages of the NS and vNSFs from its catalogue, and convey the onboarding request to the vNSFO. As the request traverses the Store before reaching the vNSFO, any change on the Store's catalogue (due to addition, update or deletion) of vNSFs or NSs is transparent to the vNSFO.

This process uploads the specific contents of the orchestrator-specific package(s) to the Orchestrator, making these available for future instantiations. Specifically, the vNSF and NS descriptors (vNSFD and NSD), metadata and configuration scripts are transmitted to the vNSFO. When applicable - that is, if the package includes the image(s) of the VDUs - these will be registered in the VIM prior to the NS instantiation. Once that data is available to the Orchestrator, the instantiation is possible.

Further interactions are expected when the vNSFO requests the Store for vNSF or NS related information; as registered during the onboarding process that the developer initiated in a previous time.

3.1.2.2. Store-Trust Monitor

The Trust Monitor needs read access to the Store in order to retrieve the data required for performing the attestation of the vNSF: the list of components executed inside the vNSF and their configuration; with a special emphasis on the custom ones not present in standard Linux distributions, which would require a special entry in a whitelist used by the Trust Monitor. The Trust Monitor does not write any information to the Store.

3.1.2.3. Orchestrator-Network infrastructure

The interaction between the vNSFO and the network infrastructure allows, on one hand, the vNSFO to perform operations on vNSFs related to its life-cycle management (e.g., start, stop, terminate, scale) or any other kind of action (e.g., configure, start an internal service), as well as actions directed to the underlying VIM. On the other hand, any kind of feedback or data monitoring can be supported through this interaction; for instance, allowing to check the status of the vNSFs or its configuration.

3.1.2.4. vNSFO-Trust Monitor

The Trust Monitor receives from the vNSFO two types of information: the current configuration of the infrastructure (active physical nodes, virtual components hosted at each node, logical connectivity) as well as network flow tables. The latter is possible once the vNSFO interacts with an SDN controller. After the SDN controller has configured the network, the rules applied on the network elements are actively checked against the rules on the SDN controller to ensure that the network is always behaving as intended and that there is no alteration of the rules.

3.1.2.5. vNSFO-DARE

Although most of the communication between the orchestrator and the DARE is done through the dashboard, the vNSFO and the DARE can still have some limited direct communications. Specifically, this communication is unidirectional (from the vNSFO to the DARE) and it refers to aspects like: i) the topology of the network, ii) the user's assignment of the different vNSFs and NSs to clients (enabler for multi-tenancy), and iii) information about the placement of the instantiated NSs with their vNSFs. This information is useful to the DARE in order to identify and react to the threats

3.1.2.6. vNSFO-Security Dashboard

The communication between the vNSFO and the security dashboard is designed to be unidirectional, from the dashboard to the vNSFO. Note that the automatic remediation functionality designed in the DARE is processed through the dashboard and not directly through the vNSFO. The reason being that all decisions (human or automatic) should be catalogued, transparent, and therefore reported and addressed by the dashboard.

SHIELD specifies a single northbound API in the vNSFO to be used by the dashboard. This API exposes the functionality to apply a specific recommendation, such as instantiating an NS, removing a previously deployed recommendation, withdrawing an NS or isolating a node that was reported untrusted.

3.1.2.7. DARE-Trust Monitor

The DARE module is the event analytics central point of the infrastructure. It can accept security events from the Trust Monitor in order to enrich its analytics operations and have a more precise view of the infrastructure state. The Trust Monitor provides to the DARE alarms related to two classes of events:

- Detection of a compromised physical node, either as a whole or as the specific compromised virtual instances hosted at the node.
- Failed enrolment of a new node (i.e. a node which attempted to join the infrastructure but failed either at the authentication or the initial integrity validation steps).

The Trust Monitor does not receive any information from the DARE.

3.1.2.8. DARE-vNSF

The ingest component of the DARE is responsible for the data captured or transferred into Apache Spot, which is transformed and loaded into solution data stores. This is highly important, as it ensures the integrity of the data and its quality in further processing steps.

Heterogeneous network information is captured via specialized vNSFs, which collect overall networking events that are relevant for threat detection. In particular, data collected from monitoring vNSFs include: network flow information (NetFlow, sFlow and so on), DNS logs, proxy server and application logs as well as generated events.

The transfer of information from the vNSFs to the DARE is done both in “push” and “pull” mode. In the “push” case, the vNSFs publish data (e.g. events) to the DARE using an API to be defined. In the “pull” case, the DARE polls the vNSFs. Daemons running in the background capture the generated network data - reading from file system paths in the vNSFs- and transfer it into Apache Spot. These daemons detect new files generated by vNSFs or data generated previously and left in the path for their collection. The use of either pull or push mechanism to get data from its source gives the opportunity to choose each time the optimal solution.

By the time the network data is captured, it shall be translated into a human-readable format (.csv) by using dissection tools, such as nfdump [13] and tshark [14]. This operation is to be done on the vNSFs. Once the data is transformed, it is transferred and stored in the HDFS both with its original format (binary) and in Hive tables. Prior to storage, data filtering might need to be employed to sanitise data and remove unwanted information. The transfer of data could be implemented using a messaging system, like Kafka, so as to achieve a reliable, scalable and distributed solution. Note that this only applies to the interaction with the monitoring vNSFs.

3.1.2.9. DARE-Security Dashboard

The security overview Dashboard is the component responsible for visualizing analytics and presenting them to the users. The Remediation component of the DARE provides detected incidents details and associated mitigation action to the Dashboard, showing an overview of the network security status. Each occurrence or expected security issue is displayed and clearly marked for severity, and a remedial or preventive measure is proposed.

The Dashboard features an intuitive graphical web-based, as well as a RESTful API for third-party applications, to query information concerning recommendations from DARE, security events past operations performed within the infrastructure, provided said applications have the proper authorization.

The Dashboard also includes a billing framework, enabling charge-back and/or show-back in an Enterprise IT environment, or SecaaS billing within the context of a Managed Security Services Provider, therefore providing consumption-based billing i.e. Operational expenditure (OPEX) rather than Capital Expenditure (CAPEX). This billing model could be based on counter, time, volumetric considerations or on a fixed usage fee per NS or vNSF.

The information from the Data Analysis engine, together with interaction from the Dashboard, are received by the vNSFO in order to automatically deploy further NSs, if needed. These actions improve the system visibility of a potential t hreat, and mitigate it via the deployment of countermeasures, comprising task-specific NSs that can block or redirect network traffic.

3.1.2.10. Trust Monitor-Security Dashboard

The Trust Monitor notifies the Security Dashboard about compromised physical nodes or any compromised virtual instance hosted on the node. The Dashboard presents the incident to the user, and a remediation is proposed (e.g. to exclude the physical node from the NFV infrastructure or to terminate a NS). The Trust Monitor does not receive any information from the Security Dashboard.

3.2. Technical solutions to requirements

In this section, the requirements specified in Section 2.4 are further analysed. Specifically, the requirements are mapped to the different components of SHIELD where they apply (Section 3.2.1); compliance to the requirements is then presented, including a high-level justification. On the one hand, the platform requirements are itemised to each component (Store, Dashboard, Orchestrator, DARE and Trust Monitor). On the other hand, the ones related to service functionalities are grouped together to create the different vNSFs to be developed in the scope of the project.

Non-Functional and Ethical & Regulatory compliance requirements are not addressed in this section since they apply broadly to all the component and vNSF implementations. These requirements are addressed in the specifications documents **D3.2** [3] and **D4.2 "Updated specifications, design and architecture for the usable information-driven engine"** [4].

3.2.1. Platform's requirements fulfilment

The architectural proposal described in the previous section has been elaborated with the aim of achieving the general high-level requirements of Section 2.4. In this context, Table 4 summarises the requirements that each component is responsible for, whilst Table 5 explains how the proposed design is compliant with the requirements set.

Table 3 - Components and requirements alignment

Components	Requirements	Description
DARE	PF04, PF08, PF13, PF16, PF18, PF22	Data analysis and remediation engine (DARE) is responsible for capturing data, analysing it, generating security events and proposing potential remediation actions.
Store	PF02, PF10, PF11, PF15, PF22	A centralized digital repository for NSs and vNSFs.
Dashboard	PF03, PF05, PF06, PF07, PF09, PF12, PF13, PF14, PF15, PF16, PF17, PF20, PF21, PF22	The dashboard is responsible for giving a security and a system overview to the users.
Orchestrator	PF01, PF02, PF03, PF07 PF11, PF13, PF22	The Orchestrator is responsible for managing the lifecycle of virtual network functions by controlling the workflows required for basic operations.
Trust Monitor	PF08, PF11, PF16, PF19, PF22	The trust monitor is responsible for verifying the infrastructure state (trusted or untrusted).

Table 4 - Compliance to requirements

Requirement	Compliance	Justification
PF01. vNSF and NS deployment	Yes	The SHIELD architecture assumes private or public NFVI-PoPs, distributed in the network, which can host virtualised network functions.
PF02. vNSF lifecycle handling	Yes	The vNSFO implements all the standard functionalities of a typical NFV MANO stack, as defined by ETSI, for managing all the steps of the lifecycle of NSs and vNSFs.
PF03. vNSF lifecycle management	Yes	The vNSFO allows management commands to be dispatched towards the vNSFs.
PF04. Data analytics	Yes	The DARE component collects and analyse metrics and logs in real time in order to detect security incidents.
PF05. Analytics visualization	Yes	The security Dashboard is the component responsible for visualizing analytics and presenting them to the users.
PF06. Ability to offer different management roles to several users.	Yes	The Dashboard includes an authentication/authorization service for managing roles.
PF07. Service elasticity (Optional req.)	Partial	The vNSFO provides the option to manually scale up and down the vNSF instances.
PF08. Platform expandability	Yes	The SHIELD platform offers well-documented APIs and interfaces as well as guidelines so that third parties can easily develop new security functions and services.
PF09. Access control	Yes	The Dashboard includes an authentication/authorization service for managing roles.
PF10. vNSF validation	Yes	The vNSF Store is responsible for validating vNSF images and notifying of any manipulation.
PF11. vNSF attestation	Yes	The Trust Monitor attests deployed vNSFs.
PF12. Log sharing	Yes	The Dashboard exposes to third parties the log and incident data, retrieved from internal SHIELD components.
PF13. Mitigation	Yes	The DARE suggests mitigation actions that can be pushed to the vNSFO for deployment of new vNSFs, configuration of existing ones etc.

PF14. Multi-User	Yes	The SHIELD network infrastructure (NFVI) is multi-user by nature. The vNSFO and DARE support multiple users with access restrictions.
PF15. Service store	Yes	The vNSF store advertises both individual vNSFs as well as composite NSs consisting of two or more vNSFs chained together.
PF16. Historic reports	Yes	The DARE saves all processed incidents in a database, so that historic reports can be requested and retrieved via the query API.
PF17. Interoperability	Yes	The interfaces of the Dashboard are publicly documented and compliant to open standards, as well as accessible to third parties.
PF18. Service composition	Yes	The vNSF store advertises NSs, i.e. sets of vNSFs chained together. The vNSFO is capable of deploying and properly configuring these services, fully supporting service function chaining (SFC).
PF19. Network Infrastructure attestation	Yes	The Trust Monitor is responsible for verifying that the network infrastructure is in trusted state. The network infrastructure elements embed the required hardware root of trust.
PF20. Billing framework	Yes	The Dashboard allows a user (e.g. vNSF developer) to define a price for the services it provides and keeps track of which ones are used by a tenant.
PF21. Operation Traceability	Yes	The Dashboard keeps a log for every action a user performs. Each log entry records the user, its role, the time & date and the action itself. This log is available on-demand to the appropriate roles.
PF22. Management communication security	Yes	Each SHIELD component (DARE, Store, Orchestrator, Dashboard, Trust Monitor) uses secure interfaces (e.g. HTTPS).

3.2.2. vNSFs and data analytics required

This section presents a preliminary list of vNSFs (Table 6) and of data analytics (Table 7) required to address the service requirements. Note that this list does not include ancillary services such as data adaptation services. Moreover, each vNSF can cover one or more functional requirement, and some of the vNSF listed here may be based on the same implementation but used with very different goals or configuration. The table includes also examples of implementations for each vNSF. These off-the-shelf implementations may not fulfil all requirements for the specific vNSF; the objective of providing candidate implementations is to prove that each function has at least one solution, with some maturity, that can be used as a starting point for the service.

Table 5 - List of vNSFs

Requirements	Name	Description	Example implementations
SF01, SF02, SF06	Content filtering	Provides a mechanism to filter URL, and scans downloaded files	Squid [15], pfsense [16]
SF02, SF04	Detect access to malicious services	Warns about different malicious software other than web based	Suricata [17], snort [18]
SF03	Security assessments	Active vulnerability scanner	OpenVAS [19]
SF03	Security assessments	Configuration engine	CFEngine [20], rudder [21]
SF07	SPAM protection	Blocks delivery of spam to the protected network	ASP [22]
SF08, SF09	DOS protection	Protects against volumetric attacks and potentially specific 0-day vulnerabilities	IPTables [23], pfsense [16]
SF09	IDPS/DPI	Prevents and detects security incidents	Suricata [17], Snort [18], nDPI [24]
SF10	Honeypot	Allows malicious traffic to be redirected to the tool for further study	Several, depending on the service being emulated
SF11	Malware sandbox	Allows automated malware analysis	Cuckoo [25]
SF12	VPN	Allows outside clients to connect as well as inter branch connections	OpenVPN [26], StrongSWAN [27]

Requirement SF05 (Central log processing/SIEM) specifies a mechanism to allow the inclusion of external sources of information into the SHIELD platform. It can be fulfilled by interfacing the legacy system directly into the DARE, implementing an interface to the DARE ingestion system.

Table 6 - List of data analytics

Requirements	Name	Description	Example implementations
SF05	Central log processing/SIEM	Security logs analysis and correlation in near real time, alert issuing	HDFS [28], Hive [29], Kafka [30], NoSQL DBs [31]
SF08, SF09	DOS protection	Prevent and detect security incidents based on advanced analytics and trained engines	Hadoop [32], Spark [33], Spot [12], Storm [34]
SF09	IDPS/DPI	Detect unknown and insider threats and characterize network traffic behaviour.	Hadoop [32], Spark [33], Spot [12], Storm [34]

3.2.3. Scalability of the SHIELD platform

This section presents, for each major component of SHIELD, the architectural or technical reasons that make it scalable to address the need of the project.

3.2.3.1. Network infrastructure

Upscaling the environment may refer to adding new infrastructure nodes or adding new compute hosts[2]. OpenStack is responsible for managing the nodes in the network infrastructure, provides an OpenStack-Ansible repository[3] to facilitate scaling operations (e.g. to add, remove, recover a host after a failure etc.). Ceilometer[4] is a component of OpenStack's Telemetry project that monitors resources used in every node and send alarms based on specified "triggers". Scale up can then be monitored in terms of performance. Ceilometer can be used to measure[5] CPU load (MHz), RAM consumption (Gb), the total amount of instances (max number of instances spawned) and total operation time (msec). Neutron testing is also important in order to estimate control plane performance (networking) with the addition of multiple nodes. OpenStack has published a full list of test plans for this purpose. These OpenStack tests extend the number of compute nodes up to the scale of 10^3, the number of workloads (VMs) up to the scale of 10^4. For Neutron, performance issues might be expected in the scale of 10^2.

[2] OpenStack environment scaling: https://docs.openstack.org/openstack-ansible/latest/admin/maintenance-tasks/scale-environment.html (Retrieved Feb 2018)
[3] OpenStack-Ansible repository https://git.openstack.org/cgit/openstack/openstack-ansible-ops (Retrieved Feb 2018)
[4] OpenStack Ceilometer: https://docs.openstack.org/ceilometer/latest/ (Retrieved Feb 2018)
[5] Test plan for 1000 compute nodes: https://docs.openstack.org/performance-docs/latest/test_plans/1000_nodes/plan.html (Retrieved Feb 2018)

3.2.3.2. Virtual Network Security Function

Upscaling/Downscaling refers to the scaling of the resources provisioned to each vNSF. OSM which is part of the vNSFO and is responsible for managing the vNSF, can perform upscaling and downscaling although a vNSF needs to be stopped, re-provisioned and then started again; and OSM does not currently handle autoscaling (on-the-fly re-provisioning).
Autoscaling, however, is supported by OpenStack through Heat, its orchestration service. In that case, OpenStack Ceilometer can also be used to set "trigger" events to further automate resource re-provisioning. In order for autoscaling to work, a load balancer should be in place, to monitor and distribute the loads across all the VMs on the scaling group. Hence, autoscaling can detect, increase, decrease, and replace instances without manual intervention even across thousands of instances.

3.2.3.3. vNSF orchestrator

A single vNSFO oversees the infrastructure in the SHIELD environment. New PoPs are manually registered in the orchestrator, either during first configuration or during runtime. Through that process, the different VIMs and nodes are described and referenced in the orchestrator for future access, as well as the required SDN controllers that manage the network infrastructure's devices.

While there is no built-in support for high availability and clustering – at the moment – in the implementation chosen for SHIELD, it is possible to replicate and share the view and management of the infrastructure across different instances of the vNSFO. For instance, that can be done in a) a replicated form (all orchestrators managing the same portions of the infrastructure) or b) separately (every orchestrator to control a specific section of the infrastructure, for instance per PoP). Both can significantly improve the degree of availability of the orchestration. For any of these options, the PoP(s) would be first registered into the specific vNSFO(s), each with its infrastructure manager, nodes and SDN devices; any component interfacing with the vNSFOs would be required to register to the different vNSFOs to access data. Extra logic on top would select specific vNSFO from the available pool (former case) or provide consensus agreement (Paxos [35], Raft [36], etc.) for the establishment of a cluster; the infrastructure view would be aggregated and its coordination, under the view of an internally designated master.

3.2.3.4. vNSF store

The Store is built on top of open source technologies that address scalability by design, be it scale in/out, concurrency, rate limiting and data storage.

The REST backend is leveraged by Eve [37], which provides features for API rate limiting on a per-user/method basis; where appropriate `X-RateLimit-` headers are provided with every response and proper HTTP codes sent out so the caller can pace itself. Resource level cache controls where `Cache-Control` and `Expires` headers are included so cache-enabled consumers can perform resource-intensive request only when really needed. Flask [38] supports the web application server with features such as split by subdomain or URL path where different functionalities may be dispatched to separate application instances; caching

backends to speed up responses and a pool of workers dedicated to run asynchronous tasks. Load balancers may also be deployed to split the load through multiple servers running the API.

The data storage is backed-up by MongoDB [39]: being a NoSQL database, scalability was addressed from the start. Out-of-the-box it provides automatic mechanisms for sharding, clustering and load balancing. Sharding is available in several policies be it Range Sharding, where documents are partitioned across shards based on the key value; Hash Sharding, where documents are distributed according to an MD5 hash of the key value; and Zone Sharding, where specific rules govern data placement in a sharded cluster, be it by geographic region, by hardware configuration, or by application feature (such rules can continuously refine data placement and MongoDB will automatically migrate the data to its new zone). Scaling is topped with Cluster Scale, in which the database can be distributed across hundreds of nodes, often in multiple data centres; Performance Scale, in which it sustains thousands of read and writes per second while maintaining strict latency Service-Level Agreements (SLAs); and Data Scale, where it can store over one billion documents in the database.

3.2.3.5. Trust Monitor

The Trust Monitor registers the physical nodes of the NFVI to periodically attest them. Apart from this information, the Trust Monitor does not keep the trust's status of the infrastructure (it can be retrieved from the reports stored the DARE if needed). Hence, different instances of the Trust Monitor can be deployed on segmented parts of the NFV infrastructure to scale-out. Moreover, aggregation of attestation results among different Trust Monitor instances could be achieved (e.g. via an API gateway) to ease the interaction between other components of the SHIELD infrastructure and the Trust Monitor cluster.

The current technology used for securing the integrity report of a node is the TPM; by design, TPMs are not high-performing cryptographic coprocessors. Currently, the order of magnitude for a TPM to sign a report is in hundreds of milliseconds. A multi-threaded Trust Monitor implementations can easily scale up to hundreds of nodes to monitor.

3.2.3.6. Data Analysis and Remediation Engine

The DARE leverages a number of state-of-the-art open-source technologies incorporated in the Cloudera Distribution for Hadoop (CDH), a comprehensive Hadoop-based data management platform. CDH includes an integrated set of horizontal scaling services for effective storage and processing of large volumes of data across a multi-node cluster. These services are configured in the available cluster nodes/hosts with one or more functions called roles. Each role determines which daemons run on a given host. The main framework upon which the different DARE analytics modules are based is Apache Hadoop, a distributed big data computing platform that is capable of breaking up data processing tasks and distributing them on multiple nodes for parallel processing. DARE takes advantage of Hadoop's two main components, HDFS which is the distributed fault-tolerant storage system and MapReduce which is the processing engine capable of splitting simple data operations between multiple nodes. For the streaming processing needs of the platform, Apache Spark is also incorporated as a distributed computing system which can process data more efficiently in multi-node architectures by using in-memory capabilities. Spark is capable of performing streaming processing and also contains MLlib, a scalable machine learning library that provides distributed computing implementations of

common learning algorithms, featurisation capabilities, tools for constructing, evaluating and tuning machine-learning pipelines, saving and loading models etc. Since the ingested data is collected from diverse and different sources, a real-time streaming application that collects and transforms multiple streams of data is needed. Apache Kafka acts as the scalable data collection mechanism of the DARE, designed to partition and persist large amounts of messages, thus materializing real-time processing by being able to accumulate and process data at high speed.

The chosen tools (Hadoop, Spark, and Kafka) are scalable by design since the main goal of the associated communities is to develop big-data tools.

The scalable and flexible architecture of the CDH framework allows the effortless addition of new nodes/hosts to the existing cluster with the help of an installation wizard that can be followed in the cluster's web-based User Interface (UI). It should be noted that this procedure does not automatically create service roles on the new hosts. Instead, the user has to follow a separate procedure to customize the assignment of new role instances, using a simple configuration wizard that evaluates the hardware configurations of the hosts, to either allow the manual installation of required services roles to new hosts or to determine the best hosts for each role and assign them automatically.

3.2.3.7. Security dashboard

The Dashboard backend provides operational features and all the interactions with the remaining components of SHIELD. The frontend handles all the user interactions and uses of the backend to accomplish the user's requests and convey notifications to the user.

The backend is built around Eve [37], Flask [38], MongoDB [39] (whose scalability mechanisms are already described in section 3.2.3.4.) and RabbitMQ [40] for notifications and messaging. Being an asynchronous message broker, it provides features such as clustering - for high availability and throughput - and federation across multiple availability zones and regions. Clustering allows for the connection of multiple machines (nodes) together to form a single logical broker, mirroring several or all the features across the nodes, whereby a client connecting to the closest node is seamlessly aware of all the queues in the cluster, even if they are not located on that node. Federation allows a queue on one node to receive messages published to a queue on another. Messages may also be moved between federated queues to follow the consumers.

The frontend is an AngularJS-built [41] web application, so scaling in is done through more performant hardware and scale out, caching, concurrency and rate limiting are achieved using web proxies and load balancers.

4. SHIELD DEMONSTRATIONS

During the first year of the project, the SHIELD consortium demonstrated the current advances by presenting four different demonstration scenarios, with three of them being partial demos (i.e. focusing on specific components) and the fourth one being an end-to-end integrated demonstration. Specifically, SHIELD presented the following capabilities:

- SDN switch attestation by detecting an unauthorized change of network rules and also by detecting the presence of an unauthorized SDN controller on the network.
- vNSF attestation by detecting the unusual behaviour of a vNSF and an unauthorized vNSF.
- Data leakage attack detection by using the DARE to detect a malicious DNS tunnel exfiltrating data from a company private network.
- DDoS detection and remediation using an end-to-end SHIELD deployment, composed by the vNSFO deploying a vNSF, the vNSF sending data to the DARE, the DARE detecting the attack and producing a remediation recipe, with, finally, the dashboard showing the attack and sending the remediation recipe to the vNSF.

During the first year, SHIELD followed a scenario-based approach. Specifically, one of the most relevant attacks were selected, according to the survey done in D2.1 [1] and then, the development phase focused on solving the identified attacks. However, several issues arose during this second phase, basically due to heterogeneous levels of maturity of some components and the limited training for the AI algorithms.

For the planning of the Year 2 demo, a different approach is considered. All the functionalities are analysed parallel and in integrated end-to-end scenarios, including all components developed in the first 18 months of SHIELD. This ranges from functional cybersecurity testing of the SHIELD vNSFs to the different analytics engines (considering the different AI algorithms that they can use and their training needs), along with the Dashboard, Store and the Orchestrator. The output of this analysis and the testing done in the real facilities is a complete list of functionalities, characteristics and defined constraints in terms of the scale that can be supported by the SHIELD testbeds. At minimum, the network infrastructure of the SHIELD testbeds should be able to support the most complicated scenarios that would require potentially all the SHIELD vNSFs to be operational concurrently. Moreover, the DARE should be able to process all the generated data and correlate it in near real time. The hardware components for the 2 PoPs used for the demonstrations are listed in Table 7 while the hardware used in the DARE is listed in Table 8. The testbeds' compute nodes would permit to increase the number of virtual machines to a few dozen, while monitoring network performance degradation at the same time (i.e. Neutron performance). In an actual operational environment, the service provider can scale up to thousands of compute nodes (as discussed in section 3), based on the performance measurements retrieved from SHIELD's demonstrations.

Table 7 – PoPs hardware listing

	PoP 1 - Athens	PoP 2 - Barcelona
Compute nodes	1 server (all-in-one)	1 server (all-in-one)
Networking nodes	1 switch, 1 router	1 switch, 2 routers

Currently, the Athens PoP is an all-in-one OpenStack deployment (controller, network, compute and storage node on the same server). Non-vNSF components (e.g. Talaia engine, POLITO recommendation and remediation engine etc.) are deployed on three additional ESXi [42] servers. Each server (PoP or non-vNSF) of the Athens testbed features:

- 128GB RAM
- Logical processors: 40
- Processor type: Intel(R) Xeon(R) CPU E5-2640 v4 @ 2.40GHz
- Sockets: 2
- Cores per socket: 10
- Hyperthreading enabled

The PoP server has 2 TB of disk storage (in RAID 1 for redundancy), while each non-vNSF server have one 480GB Solid State Drive complemented with five 1TB of disk storage.

The Barcelona PoP follows a similar installation to the all-in-one OpenStack deployed in Athens, where controller, network, compute and storage for vNSFs are provided by a single server. Other computing and storage nodes, which host the non-vNSF part of the SHIELD functionality, are to be deployed on a 3-node OpenStack cluster with high availability and failure tolerance. The PoP server has equivalent specification to the Athens PoP server.

Table 8 – DARE hardware listing

Node type	RAM	Fast storage	Historical storage	Computation capacity
Orchestrator	128GB RAM DDR4	300GB SSD	24TB HDD	2 x E5-2660V4 (14C @ 2GHz)
2 x Workers	64GB RAM DDR4	3TB SSD	-	2 x E5-2623v4 (4C @ 2.6GHz)

The hardware of the DARE testbed in Barcelona is dedicated to the Big Data Machine Learning processes needed to correlate and process all the collected information from the VNSFs.

For the Year 2 scenario, SHIELD considers to demonstrate:

- improved intelligent detection and classification of attacks (e.g. with advanced L7 DDoS, a worm-based or malware-based attack),
- a scaled-out network service featuring multiple vNSFs to pre-empt/detect/mitigate multivector threats (e.g. such as a rapidly propagating worm with malware payload),
- an advanced Intrusion Detection and Prevention scenario (e.g. a backdoor or data exfiltration attack, browser exploitation etc.)
- other possible scenarios relating to the cybersecurity needs of specific verticals (e.g. VPN detection, etc.).

SHIELD D5.1 [43] includes some feedback received by SHIELD and a list of demo requirements that need to be achieved during the Year 2 have been identified. The SHIELD demo should also cover all the mandatory requirements exposed in D2.1 [1] and updated in this document. The rest of the requirements, as well as the feedback received in the Y2 review will be used to drive the development of the final demo.

The SHIELD demonstrator is a lab-based demo, which aims to attract stakeholders while demonstrating cybersecurity attacks in a controlled and secured environment. In order to be able to achieve those expectations, the consortium agreed on a plan that would lead SHIELD

development process towards a demo for mid-September 2018. The objective is to present it in a conference during the last trimester of 2018. This plan is composed by two elements.

Firstly, Deliverable D5.1 [43] includes a traceability matrix that has been developed to map specific requirements (WP2) with the specifications (WP3/WP4) of the components that need to be tested in end-to-end scenarios. Integration and functional tests were then created and associated with each requirement and component, thus providing a methodology to verify each requirement or to complete functional testing of a specific component, as shown in Figure 8. This work does not include only the components that implement each requirement but rather the entire chain of components needed to verify the requirement end-to-end. Note that bold rows are mandatory requirements. Secondly, this table implies several development tasks which have been identified and organized in a Gantt diagram for 2018, which is shown in Figure 9 and complements the integration plan presented in D5.1 [43]. The Gantt diagram shows that the first phase is focused on the development, analysis and testing of the vNSFs as well as on the analysis of the analytics engines. A testing framework for cyber-attack simulation or execution is being developed concurrently, to test the cybersecurity capabilities of the platform, while the AI algorithms are being trained with POLITO's specialised, anonymised traffic dataset (refer to D5.1 [43] for more information). Once we have identified a complete list of functionalities, characteristics and limitations, the scenarios will be finalised (April 2018). After the scenario definition, the project will focus on the development of the orchestration/store and the analytics engines, in order to show the different scenarios of the demo. Note that integration will start from the beginning of the implementation phase and will last until the end of the project, which means that components will be integrated while they are developed (continuous integration). Moreover, the dashboard implementation activities, which do not depend on the capabilities of the vNSFs or the analytics engines, starts from the beginning of the development phase.

D2.1 & D2.2			D3.1										D4.1			
Type	ID	Name	vNSFs & lifecycle management									Attestation	Data Intelligence			
			L7 filter	L3 filter	mcTLS	HTTP/S analyser	vDPI	L7 Fordward	vIDS	vNSFO	Store	Trust monitor	Acq & Storage	Analysis	Rec/Mit	Dashb.
			NCSRD	*PoliTo*	*TID*	*TID*	*ORION*	*POLITO*	*NCSRD*	I2CAT	UBI	HPE, POLITO	SPH	INFILI, TALAIA	POLITO	UBI
Platform Functional Requirements	**PF01**	**vNSF and NS deployment**	**NCSRD**	**POLITO**	**TID**	**TID**	**ORION**	**POLITO**	**NCSRD**	**I2CAT**						
	PF02	**vNSF lifecycle management**	**NCSRD**	**POLITO**	**TID**	**TID**	**ORION**	**POLITO**	**NCSRD**	**I2CAT**	**UBI**				**POLITO**	
	PF03	**vNSF status management**	**NCSRD**	**POLITO**	**TID**	**TID**	**ORION**	**POLITO**	**NCSRD**	**I2CAT**						**UBI**
	PF04	**Security data monitoring & analytics**			**TID**	**TID**	**ORION**		**NCSRD**				**SPH**	**INFILI, TALAIA**		
	PF05	**Analytics visualisation**					**ORION**							**INFILI, TALAIA**		**UBI**
	PF06	**Ability to offer different mgmt roles to several users**	**NCSRD**	**POLITO**			**ORION**	**POLITO**	**NCSRD**	**I2CAT**					**POLITO**	**UBI**
	PF07	Service Elasticity								I2CAT						UBI
	PF08	**Platform Expandability**										**POLITO**		**INFILI, TALAIA**	**POLITO**	
	PF09	**Access Control**								**I2CAT**	**UBI**	**HPE, POLITO**				**UBI**
	PF10	**vNSF validation**	**NCSRD**	**POLITO**	**TID**	**TID**	**ORION**	**POLITO**	**NCSRD**	**I2CAT**	**UBI**					
	PF11	**vNSF attestation**							**NCSRD**	**I2CAT**	**UBI**	**POLITO**				
	PF12	**Log Sharing**								**I2CAT**	**UBI**	**HPE, POLITO**	**SPH**	**INFILI, TALAIA**	**POLITO**	**UBI**
	PF13	**Mitigation**	**NCSRD**	**POLITO**	**TID**		**ORION**	**POLITO**		**I2CAT**				**INFILI, TALAIA, I2CAT**	**POLITO, I2CAT**	**UBI**
	PF14	**Multi-user**	**NCSRD**	**POLITO**			**ORION**	**POLITO**	**NCSRD**	**I2CAT**						**UBI**
	PF15	**Service Store**	**NCSRD**	**POLITO**	**TID**	**TID**	**ORION**	**POLITO**	**NCSRD**		**UBI**					**UBI**
	PF16	**History Reports**										**HPE, POLITO**	**SPH**	**INFILI, TALAIA**		**UBI**
	PF17	**Interoperability**								**I2CAT**	**UBI**	**HPE,POLITO**		**INFILI, TALAIA**		**UBI**
	PF18	**Service Composition**							**NCSRD**					**INFILI, TALAIA**		**UBI**
	PF19	**Network Infrastructure Attestation**								**I2CAT**		**HPE**				
	PF20	**Billing Framework**	**NCSRD**	**POLITO**			**ORION**	**POLITO**	**NCSRD**		**UBI**					**UBI**
	PF21	**Operation Traceability**								**I2CAT**	**UBI**	**HPE, POLITO**			**POLITO**	**UBI**
	PF22	**Communications security**	**NCSRD**	**POLITO**	**TID**	**TID**	**ORION**	**POLITO**	**NCSRD**	**I2CAT**	**UBI**	**HPE, POLITO**	**SPH**	**INFILI, TALAIA**	**POLITO**	**UBI**
Platform Non-Functional Requirements	**NF01**	**Response time**	**NCSRD**	**POLITO**	**TID**	**TID**	**ORION**	**POLITO**	**NCSRD**	**I2CAT**	**UBI**	**HPE, POLITO**	**SPH**	**INFILI, TALAIA, I2CAT**	**POLITO**	**UBI**
	NF02	**Availability**	**NCSRD**	**POLITO**	**TID**	**TID**	**ORION**	**POLITO**	**NCSRD**	**I2CAT**	**UBI**	**HPE, POLITO**	**SPH**	**INFILI, TALAIA, I2CAT**	**POLITO**	**UBI**
	NF03	**Scalability**	**NCSRD**	**POLITO**	**TID**	**TID**	**ORION**	**POLITO**	**NCSRD**	**I2CAT**			**SPH**	**INFILI, TALAIA, I2CAT**	**POLITO**	
	NF04	**Data Volume**											**SPH**	**INFILI, TALAIA, I2CAT**		
	NF05	**Impact on perceived performance**	**NCSRD**	**POLITO**	**TID**	**TID**	**ORION**	**POLITO**	**NCSRD**				**SPH**	**INFILI, TALAIA, I2CAT**		
	NF06	**Performance factors**	**NCSRD**	**POLITO**	**TID**	**TID**	**ORION**	**POLITO**	**NCSRD**	**I2CAT**	**UBI**	**HPE, POLITO**	**SPH**	**INFILI, TALAIA, I2CAT**	**POLITO**	**UBI**
	NF07	**Compliance to standards**	**NCSRD**	**POLITO**	**TID**	**TID**	**ORION**	**POLITO**	**NCSRD**	**I2CAT**	**UBI**	**HPE, POLITO**	**SPH**	**INFILI, TALAIA, I2CAT**	**POLITO**	**UBI**
	NF08	**Deployment and support simplicity**								**I2CAT**	**UBI**	**POLITO**	**SPH**	**INFILI, TALAIA, I2CAT**	**POLITO**	**UBI**
	NF09	**vNSF hardening**	**NCSRD**	**POLITO**	**TID**	**TID**	**ORION**	**POLITO**	**NCSRD**	**I2CAT**	**UBI**	**POLITO**				
Service Functional Requirements	SF01	Content filtering							NCSRD	I2CAT	UBI			INFILI, TALAIA	POLITO	
	SF02	**Detect/block access to malicious websites**	**NCSRD**		**TID**		**ORION**		**NCSRD**	**I2CAT**	**UBI**			**INFILI, TALAIA**	**POLITO**	
	SF03	Security assessments												INFILI, TALAIA	POLITO	
	SF04	**L4 traffic filtering**		**POLITO**			**ORION**		**NCSRD**							
	SF05	Central log processing/SIEM	NCSRD	POLITO			ORION		NCSRD	I2CAT				INFILI, TALAIA	POLITO	UBI
	SF06	**Malware detection**	**NCSRD**	**POLITO**	**TID**		**ORION**		**NCSRD**	**I2CAT**	**UBI**	**POLITO**	**TID**	**TID**		
	SF07	**Spam protection**	**NCSRD**						**NCSRD**							
	SF08	**DoS protection**	**NCSRD**	**POLITO**			**ORION**		**NCSRD**					**INFILI, TALAIA**	**POLITO**	
	SF09	**Intrusion Detection/Prevention System**		**POLITO**	**TID**	**TID**	**ORION**	**POLITO**	**NCSRD**					**INFILI, TALAIA**	**POLITO**	
	SF10	Honeypots					ORION		NCSRD					INFILI, TALAIA	POLITO	
	SF11	Sandboxing								I2CAT	UBI				POLITO	UBI
	SF12	VPN								I2CAT	UBI				POLITO	UBI
Ethical & Regulatory Compliance	**ERC01**	**Access to personal data**	**NCSRD**	**POLITO**	**TID**	**TID**	**ORION**		**NCSRD**	**I2CAT**	**UBI**		**SPH**	**INFILI, TALAIA, I2CAT**		**UBI**
	ERC02	**Data rectification and erasure**	**NCSRD**	**POLITO**	**TID**	**TID**	**ORION**		**NCSRD**	**I2CAT**	**UBI**		**SPH**	**INFILI, TALAIA, I2CAT**		**UBI**
	ERC03	**Access to related Data Protection information**								**I2CAT**	**UBI**					**UBI**
	ERC04	**Transparency in data processing**								**I2CAT**	**UBI**					**UBI**
	ERC05	**Data retention**	**NCSRD**	**POLITO**	**TID**	**TID**	**ORION**		**NCSRD**	**I2CAT**	**UBI**		**SPH**	**INFILI, TALAIA, I2CAT**		**UBI**
	ERC06	**Transparency in traffic classification**	**NCSRD**			**TID**	**ORION**		**NCSRD**	**I2CAT**	**UBI**					**UBI**
	ERC07	**Notification obligation**								**I2CAT**		**HPE, POLITO**				**UBI**
	ERC08	**Net Neutrality**														**UBI**
	ERC09	**Lawful Interception**	**NCSRD**	**POLITO**	**TID**	**TID**	**ORION**		**NCSRD**				**SPH**	**INFILI, TALAIA, I2CAT**	**POLITO**	**UBI**

Figure 8 - Assignment of development responsibilities per partner for each component and feature

Nombre	Fecha de...	Fecha de fin
Agreement on the Gantt and responsabilities	22/01/18	2/02/18
VNF implementation	5/02/18	30/03/18
PF13: Mitigation	5/02/18	2/03/18
Descriptors and on-boarding	5/03/18	30/03/18
Analysis of VNFs	5/02/18	6/04/18
Store and Orchestrator in facilities	5/02/18	2/03/18
Facilities for testing vNSF ready	5/02/18	2/03/18
List of functionalities	5/02/18	2/03/18
Testing	5/03/18	30/03/18
Functionalities linked to possible scenarios	2/04/18	6/04/18
Analysis of Analytics engines	5/02/18	6/04/18
Accessing to real data	5/02/18	23/02/18
List of functionalities	5/02/18	23/03/18
Testing	26/02/18	23/03/18
Functionalities linked to possible scenarios	26/03/18	6/04/18
Analysis of the Orchestrator	19/02/18	16/03/18
Analysis of the Store	19/02/18	16/03/18
Scenarios definition	9/04/18	20/04/18
Integration	5/02/18	14/09/18
Dashboard implementation	6/02/18	29/06/18
PF06, PF09: Access control	6/02/18	26/02/18
PF06: Management roles	27/02/18	19/03/18
PF14: Multi-user	20/03/18	23/04/18
PF16: History reports	27/02/18	23/04/18
PF17: Interoperability	24/04/18	14/05/18
PF12: Log Sharing	15/05/18	4/06/18
PF01, PF02, PF03: Unify SHIELD dashboard wit...	28/05/18	29/06/18
PF05: Unify SHIELD dash. with Talaia dash.	28/05/18	29/06/18
PF05: Unify SHIELD dash with Spot dash.	28/05/18	29/06/18
Orchestrator implementation	5/03/18	29/06/18
PF02: vNSF lifecycle management	5/03/18	20/04/18
PF03: vNSF status management	23/04/18	25/05/18
PF07: Service elasticity	28/05/18	22/06/18
PF18: Service composition	28/05/18	22/06/18
PF01: deployment on internal and external pre...	11/06/18	29/06/18
Analytics implementation	1/05/18	16/07/18
PF13: Mitigation	1/05/18	16/07/18
PF04: Real time	1/05/18	16/07/18
PF18: Service composition	28/05/18	29/06/18
Cybersecurity policies implementation	1/05/18	26/07/18
PF13: Mitigation	1/05/18	26/07/18
ERC6: Transparency in traffic classification	1/05/18	4/06/18
Store implementation	6/02/18	21/05/18
PF08: Provide ways to upload new vNSFs	6/02/18	5/03/18
PF10: vNSF validation	6/03/18	16/04/18
PF15: Service store	6/03/18	21/05/18
ERC4: Transparency in data processing	6/02/18	21/05/18
Attestation Implementation	6/02/18	9/07/18
PF11: vNSF attestation	6/02/18	28/05/18
PF19: Network Infrastructure attestation	6/02/18	28/05/18
ERC7: Notification Obligation	29/05/18	9/07/18

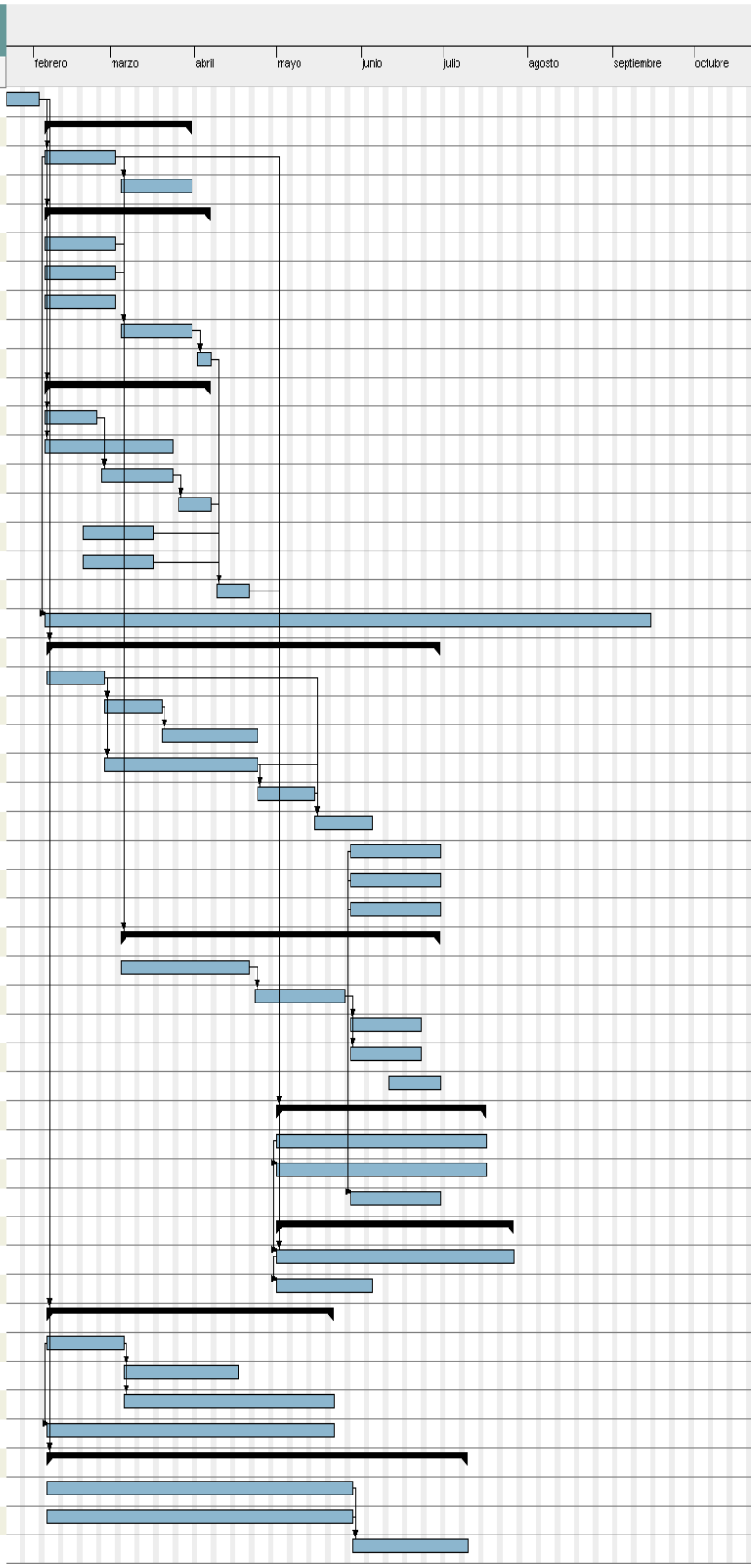


Figure 9 - Gantt of the Year 2 demo roadmap

5. CONCLUSION

This document presents the analysis of the use cases, the identification and prioritisation of the requirements, the high-level architecture of SHIELD and its components, the main inter-component interfaces and the plan for demonstrating the SHIELD platform. The SHIELD partners contributed to this endeavour, achieving consensus among the consortium members on the proposed architectural vision.

The requirements collected via the online surveys contribute to produce a technical solution, well aligned to both the market needs and the recent trends in NFV architectures and big data analytics. These requirements lead to the design of a system that is reasonably complex and feasible to implement; it is also compatible with existing state-of-the-art IT, cloud and network infrastructures. In addition, the proposed architecture is compliant with the current technical approach and terminology of ETSI Industry Specification Group (ISG) NFV.

Furthermore, a technical analysis of the proposed architecture shows that the SHIELD design effectively accommodates all the identified requirements and the defined use cases.

Using the overall architecture as reference, the project can proceed to the next tasks, which are the detailed definition of the SHIELD's components such as the NSs, the vNSF store and orchestrator, the big data store and security analytics module, etc. Deliverables D3.2 [3] and D4.2 [4] summarise the outcome of this work. The detailed specification phase is followed by the implementation, integration and assessment phases; the goal is to build the SHIELD's platform and evaluate it against the different requirements presented in this document. The result of the assessment will be presented in deliverable D5.2 [44], which will be published at the end of the project.

REFERENCES

[1] “Deliverable D2.1. "Requirements, KPIs, design and architecture",” February 2017. [Online]. Available: https://www.shield-h2020.eu/shield-h2020/documents/project-deliverables/SHIELD_D2.1_Requirements_KPIs_Design_and_Architecture_v1.0.pdf.

[2] “Deliverable D6.3. “Interim Report on Exploitation Activities”,” [Online]. Available: https://www.shield-h2020.eu/shield-h2020/documents/project-deliverables/SHIELD_D6.3_Interim_Report_on_Exploitation_Activities_v.1.0.pdf.

[3] “Deliverable D3.2. Updated specifications, design and architecture for the vNSF ecosystem,” [Online].

[4] “Deliverable D4.2. Updated specifications, design and architecture for the usable information-driven engine,” [Online].

[5] ETSI NFV ISG, “ETSI GS NFV 001 v1.1.1 Network Functions Virtualisation; Use Cases,” ETSI, 2013.

[6] ETSI NFV ISG, “ETSI GS NFV 002 v1.1.1 Network Functions Virtualisation (NFV); Architectural Framework,” ETSI, 2013.

[7] ETSI NFV ISG, “ETSI GS NFV 003 v1.1.1 Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV,” ETSI, 2013.

[8] ETSI NFV ISG, “ETSI GS NFV 004 v1.1.1 Network Functions Virtualisation (NFV); Virtualisation Requirements,” ETSI, 2013.

[9] ETSI NFV ISG, “ETSI GS NFV-PER 002 V1.1.1 Network Functions Virtualisation; Proof of Concepts; Framework,” ETSI, 2013.

[10] ETSI, “Network Functions Virtualisation,” 27 5 2014. [Online]. Available: http://www.etsi.org/technologies-clusters/technologies/nfv.

[11] G. Coker, “Principles of remote attestation,” *International Journal of Information Security,* vol. 10, pp. 63-81, 2011.

[12] “Apache Spot,” [Online]. Available: https://spot.apache.org/.

[13] “nfdump,” February 2018. [Online]. Available: https://github.com/phaag/nfdump.

[14] “TShark,” February 2018. [Online]. Available: https://www.wireshark.org/docs/man-pages/tshark.html.

[15] “SQUID,” [Online]. Available: http://www.squid-cache.org/.

[16] “PFSense,” [Online]. Available: https://pfsense.org/.

[17] “Suricata,” [Online]. Available: https://suricata-ids.org/.

[18] “Snort,” [Online]. Available: https://www.snort.org/.

[19] “OpenVAS,” [Online]. Available: http://www.openvas.org/.

[20] “CFEngine,” [Online]. Available: https://cfengine.com/.

[21] “Rudder project,” [Online]. Available: http://www.rudder-project.org/mailman/listinfo/rudder-security.

[22] “ASP: anti-spam project,” [Online]. Available: http://www.thockar.com/assp-home/.

[23] “Linux IPTables,” [Online]. Available: http://www.linuxguide.it/command_line/linux_iptables_firewall-c25_en.html.

[24] “nDPI,” February 2018. [Online]. Available: https://www.ntop.org/products/deep-packet-inspection/ndpi/.

[25] “Cuckoo sandbox,” [Online]. Available: https://cuckoosandbox.org/.

[26] “OpenVPN,” [Online]. Available: https://openvpn.net/.

[27] “StrongSwan: the Open Source IPsec-based VPN Solution,” [Online]. Available: https://www.strongswan.org/.

[28] “Apache HDFS,” [Online]. Available: https://hadoop.apache.org/docs/r1.2.1/hdfs_design.html.

[29] “Apache Hive,” [Online]. Available: https://hive.apache.org/.

[30] “Apache Kafka,” [Online]. Available: https://kafka.apache.org/.

[31] “NoSQL DBs,” [Online]. Available: http://nosql-database.org/.

[32] “Apache Hadoop,” [Online]. Available: https://hadoop.apache.org/.

[33] “Apache Spark,” [Online]. Available: https://spark.apache.org/.

[34] “Apache Storm,” [Online]. Available: https://storm.apache.org/.

[35] L. Lamport, “The Part-time Parliament,” *ACM Trans. Comput. Syst.,* vol. 16, no. 2, pp. 133-169, 1998.

[36] “Raft,” February 2018. [Online]. Available: https://raft.github.io/.

[37] “Eve: a Python REST API framework designed for human beings,” [Online]. Available: http://python-eve.org/.

[38] “Flask: a micro webdevelopment framework for Python,” [Online]. Available: http://flask.pocoo.org/.

[39] “MongoDB: a NoSQL document-oriented database,” [Online]. Available: https://www.mongodb.com/.

[40] “RabbitMQ: a message broker software,” [Online]. Available: https://www.rabbitmq.com.

[41] “AngularJS: a JavaScript-based frontend web application framework,” [Online]. Available: https://angularjs.org.

[42] “ESXi,” VMware, February 2018. [Online]. Available: https://www.vmware.com/products/esxi-and-esx.html.

[43] e. a. O. Segou (ed.), “Integration results of SHIELD HW/SW modules,” *SHIELD Deliverable D5.1,* January 2018.

[44] “Deliverable D5.2. Final demonstration, roadmap and validation results,” [Online].

[45] A. M. A. Bahurmoz, “The analytic hierarchy process at DarAl-Hekma, Saudi Arabia,” *Interfaces,* vol. 33, pp. 70-78, 2003.

[46] T. L. Saaty, “A scaling method for priorities in hierarchical structures,” *Journal of Mathematical Psychology,* vol. 15, pp. 234-281, 1977.

[47] e. a. G. Dede, “Theoretical estimation of the probability of weight rank reversal in pairwise comparisons,” *European Journal of Operational Research,* vol. 252, pp. 587-600, 2016.

[48] e. a. G. Dede, “Convergence properties and practical estimation of the probability of rank reversal in pairwise comparisons for multi-criteria decision making problems,” *European Journal of Operational Research,* vol. 241, pp. 458-468, 2015.

[49] N. Gerdsri and D. F. Kocaoglu, “Applying the Analytic Hierarchy Process (AHP) to build a strategic framework for technology road mapping,” *Mathematical and Computer Modelling,* vol. 46, pp. 1071-1080, 2007.

[50] “LimeSurvey,” [Online]. Available: https://www.limesurvey.org/.

[51] “MathWorks MATLAB,” [Online]. Available: http://www.mathworks.com/.

LIST OF ACRONYMS

Acronym	Meaning
AHP	Analytic Hierarchy Process
API	Application Programming Interface
CAPEX	Capital Expenditure
CERT	Computer Emergency Response Team
C&C server	Command & Control server
CR	Consistency Ratio
CRUD	Create, Read, Update, Delete (operations)
DARE	Data Analysis and Remediation Engine
DDoS	Distributed Denial of Service
DNS	Domain Name System
DoS	Denial of Service
DPI	Deep Packet Inspection
ETSI	European Telecommunications Standards Institute
HDFS	Hadoop Distributed File System
IDPS	Intrusion Detection and Prevention System
IMA	Integrity Measurement Architecture
IoT	Internet of Things
IPS	Intrusion Prevention System
ISG	Industry Specification Group
ISP	Internet Service Provider
KPI	Key Performance Indicator
LDA	Latent Dirichlet Allocation
MANO	Management & Orchestration
NF	Non-Functional (requirement)
NFV	Network Function Virtualisation
NFVI	NFV Infrastructure
NS	Network Service
OPEX	Operational expenditure
PCR	Platform Configuration Register

PF	Platform Functional (requirement)
PoP	Point of Presence
REST	Representational State Transfer
SDK	Software Development Kit
SDN	Software-Defined Network
SF	Service Functional (requirement)
SFC	Service Function Chaining
SIEM	Security Information and Event Management
SLA	Service-Level Agreement
SP	Service Provider
TC	Trusted Computing
TPM	Trusted Platform Module
UC	Use Case
UI	User Interface
VDU	Virtual Deployment Unit
vNSF	virtual Network Security Function
vNSFO	vNSF Orchestrator
vNSFD	vNSF Descriptor
VPN	Virtual Private Network
WP	Work Package

APPENDIX A. MAIN CHANGES FROM D2.1 TO D2.2

This appendix summarises the main changes of this document with regards to the previous deliverable D2.1 [1].

- Section 2.1 presents only the use case analysis result; most of the methodology is in Appendix C.
- Section 2.2 is new and focuses on the survey used to rank the factors and technological criteria that impact SHIELD's market adoption.
- Section 2.4 has been updated and extended:
  - Update of the description and KPI.
  - New Platform Functional requirements: PF21 (Operation Traceability) and PF22 (Management communication security).
  - New Non-Functional requirements: NF06 (Performance Factors), NF07 (Compliance to standards), NF08 (Deployment and support simplicity) and NF09 (vNSF hardening).
  - New Ethical & Regulatory Compliance requirements section.
- The "Data workflow" section has been removed since more detailed diagrams are available in the specification deliverables D3.2 [3] and D4.2 [4].
- Section 3.1's subsection has been updated to match the specification documents.
- Section 3.1.2.4 (vNSFO-Trust Monitor) has been updated and 3.1.2.10 (Trust Monitor-Security Dashboard) since the Trust Monitor sends notifications to the DARE and the Dashboard. The Dashboard presents the security incident – with a proposed remediation - to an operator who can act on it.
- Section 3.2.1 (Platform's requirements fulfilment) has been updated based on the new requirements.
- Section 3.2.3 (Scalability of the SHIELD platform) has been added; this section presents a high-level description of the features and technologies that make the SHIELD platform scalable by design.
- Section 4 (SHIELD demonstrations) has been added; this section details the roadmap of the consortium for demonstrating the SHIELD platform. The testbed for the demonstrations is presented, as well as the development GANTT diagram.
- Appendix B (Feeback from cybersecurity agencies) has been added; this appendix is composed of two feedback received from cybersecurity agencies about SHIELD's use cases, requirements and architecture. Whilst most of the comments have been addressed in this document, some feedback are out of the scope of the project. SHIELD does not focus on additional security tools - such as penetration testing – and the security processes that need to be in place around SHIELD: any organisation deploying SHIELD should complement it with those tools and processes.

APPENDIX B. FEEDBACK FROM CYBERSECURITY AGENCIES

Editor's note: this appendix presents two feedback written by officers from cybersecurity agencies from member states of the European Union. The views presented herein are personal and do not necessarily reflect the official position of each agency. The detailed feedback from these agencies has already been incorporated in the Requirements and KPIs of Section 2.

First cybersecurity agency feedback (MND/SSE)

This feedback was collected by specialised officers of the Greek Ministry of National Defense (MND), also affiliated with the Hellenic Army Academy (SSE). SSE hosts and maintains a data center running several critical applications for the Greek Army. SSE organizes and runs the National (Greek) Cyber Defense Exercise "Panoptis 2014-2017". SSE also participates in "Locked Shields", which is the world's largest and most advanced international technical live-fire cyber defense exercise. Here is the written feedback received about the SHIELD Use Cases and requirements.

SHIELD Use Cases

The SHIELD platform could be greatly beneficial in contributing to national, European and global security by offering a way of sharing threat information with third parties, as being mentioned in Use Case 3. It should be taken into consideration, though, that there are cases where a public sector agency would like to avoid exposing the kind of attacks it has suffered in public. For this reason, disclosure and/or conversations regarding security vulnerabilities are usually handled privately and all relevant information is announced in public only after the issue has been resolved. In such cases, measures should be taken so that the synchronized information in the SHIELD framework has no attribution to the specific agency that suffers the attack.

In the same concept, consideration should be given on where the DARE will be deployed. There are cases where agencies in public sector prefer or are obliged to not export to the cloud any kind of data residing in their internal infrastructure. The SHIELD platform should then have to be developed in house and maybe use some kind of proxying for having access to information needed from the cloud (e.g. malware signatures, Yara rules[6], updates, etc.). This issue has already been addressed in the project's platform functional requirements as **PF01** but it only refers to vNSFs and not to the DARE.

Information exchange is a key element in strengthening cyber security. From this aspect, it might be useful for SHIELD to have the capability of importing in its database information provided by other threat intelligence platforms that use open standards for threat information sharing. One such platform that is widely used in NATO is the Malware Information Sharing Platform[7] (MISP), a free and open source software helping information sharing of threat and cyber security indicators. A new MISP instance can be installed locally as part of the platform's infrastructure and will start with an empty database. Its built-in sharing functionality allows data sharing and information exchange between different installations, as well as automatic synchronization of events and attributes among instances, while all acquired data is locally stored, ensuring that the queries for information remain confidential. Exporting data in the STIX

[6] Yara Rules Repository: http://yararules.com/
[7] MISP - Open Source Threat Intelligence Platform: http://www.misp-project.org/

format (XML and JSON) is also supported (including export in STIX 2.0 format), hence ensuring SHIELD's compliance with well-established standards (NF07).

SHIELD Requirements and KPIs

SHIELD's high-level requirements are overall very well-established, in the sense that they depict the combined capabilities of state-of-the-art cybersecurity products. Here follows a list of comments and suggestions regarding the projects requirements, KPIs and architectural design:

Since SHIELD will be responsible for the whole security of its internal infrastructure, it should also be used as the inventory database of authorized and unauthorized asset (devices and software) information. Based on the asset information, it will be able to detect and prioritize threats. PF19 states that the platform shall verify that the network infrastructure is in a trusted state and the relevant KPI refers to the periodic attestation of the nodes. It may be beneficiary to explicitly add as a KPI the modification of the network infrastructure by the addition of a new network device, since SHIELD should also generate alerts for this type of events. For example: "SHIELD should actively or passively scan the network infrastructure for connected devices and produce alerts if there is differentiation from its inventory list."

In the same context, if a system has a running port, protocol or service that has not been authorised it should be reported by the SHIELD platform. Defining a KPI for this requirement should also be considered.

In SF03, a continuous vulnerability assessment is being offered as an optional feature. Correlating this assessment's output with the captured network traffic logs, in order to determine whether vulnerabilities are being exploited in real time, may also be considered for implementation. However, given the project's mature stage in design and definition of objectives, such a feature may be difficult to be implemented.

PF09 sets a requirement for access control to the platform. SHIELD should also check for access violations to the network systems that it protects and should also monitor the use of administrative privileges. For example, running a web browser as an administrator should produce an alert and a general violation of the least privilege enforcement should be detected. This requirement may also be set under the umbrella of SF09, as part of security policy and configurations violation.

Another consideration that should be taken into account is the amount of network traffic that the platform itself will be generating and whether this might impact the user experience (not the user of the platform but the user of the organization that the platform protects). Since this is related to resource monitoring, it could be mentioned either under network infrastructure scalability (3.2.3.1) or as an additional KPI of NF05 where the impact on performance is discussed, or even under PF04 (if the collection of resources usage metrics is also scheduled).

According to SHIELD design description, the platform is responsible for automatically applying the appropriate remediation to a security event. However, there might be cases where the proposed remediation cannot be applied or it doesn't mitigate the treat. For example, if the remediation requires the instantiation of a NS that is currently unavailable or if the proposed MSPL configuration cannot be imported/applied, then remediation may not be available. In these cases there should be a way for the platform to try different approaches like implementing perimeter security, firewalling, applying advanced access restrictions etc. The

addition of this type of requirement with the appropriate KPI might also need to be considered under PF13.

Second cybersecurity agency feedback (CESICAT)

CESICAT is the Catalan agency for cybersecurity, which is in charge of the infrastructure of the Catalan government (acting as an ISP). CESICAT is also responsible for promoting protection against cybersecurity threats, not only for public Catalan bodies, but also for companies and organisations.

After presenting the project to the CESICAT's representatives, including the head of innovation, the head of the response to threats service, and the director of CESICAT, they provided us with the following feedback.

Regarding the use case 3 "Contributing to national, European and global cybersecurity", they like the idea of the use case and they would focus on the following aspects:

- They are more interested in getting the "big picture" - vectors of attack on a large scale and evolution of a given threat (number of machines infected, amount of traffic generated, etc.), rather than having fine-grained data from the individual users (something that according to them may be understood from the use-case).
- They are particularly interested in following "malware campaigns": tracking infection, scope of influence, how the malware propagates and how to detect it.
- The main blocker to communication between ISPs and Cybersecurity agencies is legislation, not technology.
- If they were able to see ISPs data, they would be interested to know:
    1. If a certain ISP is a channel of propagation for a given threat.
    2. If the ISP has already deployed measures to mitigate the threat,
        - if not, could the ISP deploy such measures?
    3. If the cybersecurity agency can develop (or promote development of) specific functions.

More generally, they think that the next generation of cybersecurity measures should be based on prediction; this is a topic they want to focus on. Moreover, they are also interested in anomaly detection (to monitor how these anomalies become threats) and mutation of current anomalies.

APPENDIX C1. SURVEY'S QUESTIONNAIRE FOR REQUIREMENTS ANALYSIS

SHIELD survey for requirement analysis

This survey is designed to gather requirements for the SHIELD project. This survey does not involve the collection of personal data. All responses are anonymous and are not linked to any individual. (http://incites.eu/poll/index.php/856874)

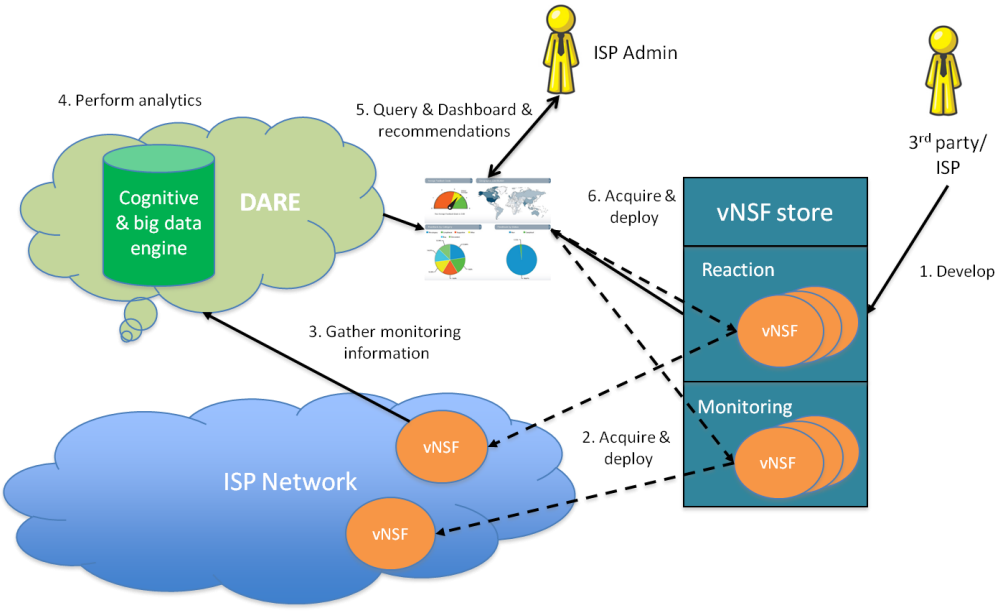
SHIELD in a nutshell

The SHIELD project combines Network Functions Virtualisation (NFV), Security-as-a-Service (SecaaS), Big Data Analytics and Trusted Computing (TC), in order to provide an extensible, adaptable, fast, low-cost and trustworthy cybersecurity solution. It aims at delivering IT security as an integral service of virtual network infrastructures that can be tailored for Internet SPs and enterprise customers - including SMEs- in equal terms. Virtualised Network Security Functions (vNSF) provide software instantiations of security appliances that can be dynamically deployed into a network infrastructure. In line with the NFV concept and going beyond traditional SecaaS offerings, vNSFs can be distributed within the network infrastructure close to the user/customer. This may allow to radically improve performance while reducing response time. Summarizing, SHIELD is a NFV based Intrusion Detection and Protection (IDPS) solution for ISPs.

Specifically, SHIELD studies 3 use-cases:

Use Case 1: An ISP using SHIELD to secure their own infrastructure

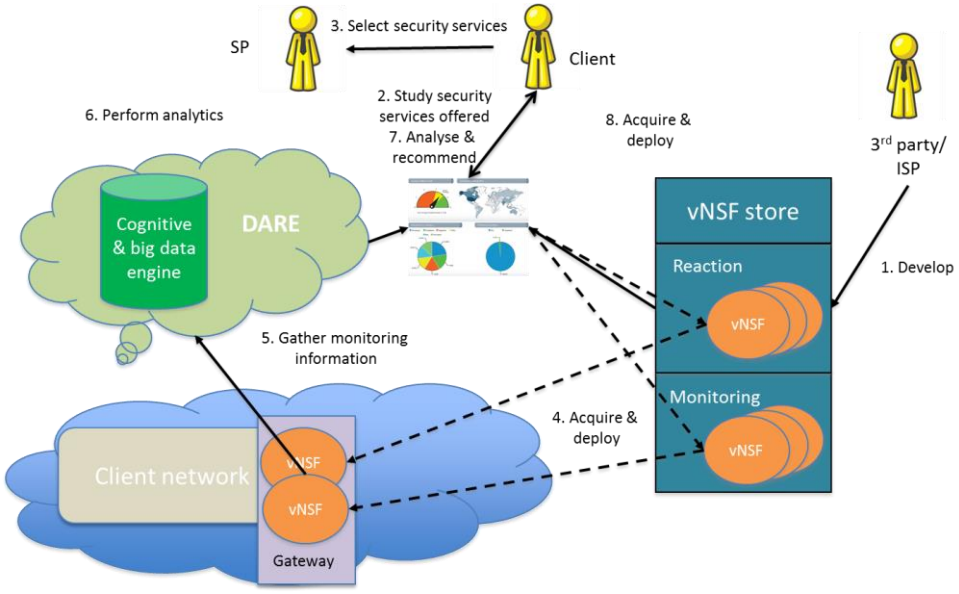
In order to protect their own network infrastructure, ISPs have to deploy specific hardware which is very expensive since this hardware has to be updated and maintained by very specialized operators. The virtualization offered by SHIELD in this use case aims to dramatically reduce this cost by replacing specific hardware for vNSFs (virtual Network Security Functions), as well as providing a central interface (dashboard) to understand the gathered information and to act in the network.



Use Case 2: An ISP leveraging SHIELD to provide advanced SecaaS services to customers

As aforementioned, SHIELD provides an ideal foundation for building enhanced SecaaS services, far beyond current offerings. Using this SecaaS paradigm, the complexity of the security analysis can be hidden from the client (either a company or an SME) who can be freed from the need to acquire, deploy, manage and upgrade specialised equipment.

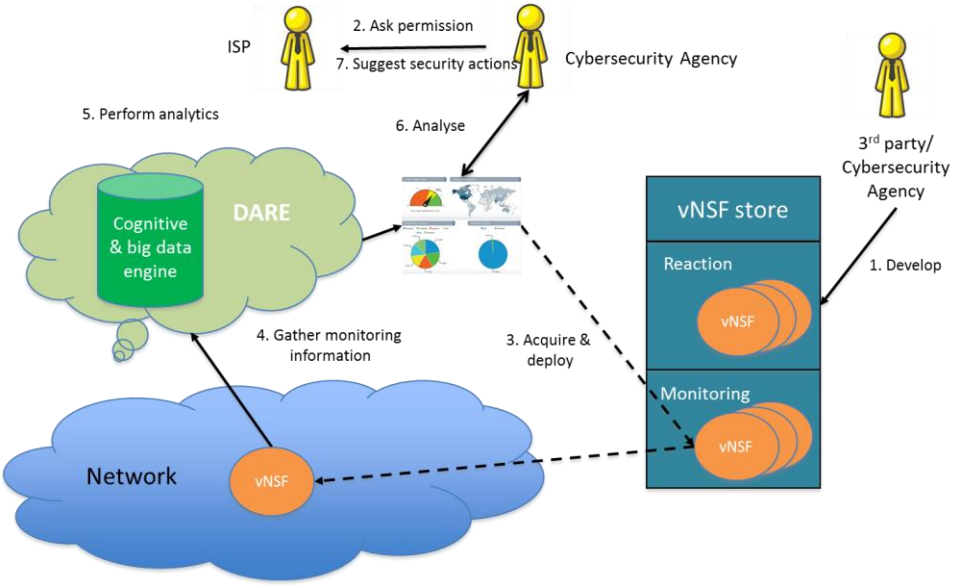
In this UC, the ISP would be able to insert new security-oriented functionalities directly into the local network of the user, through its provided gateway or in the ISP network infrastructure.



Use Case 3: Contributing to national, European and global security

Through the dashboard, available to authorised actors, ad-hoc requests regarding threat models or some data regarding acquired threat intelligence can be retrieved by, for instance, public cybersecurity agencies. The secure SHIELD framework offers, in this manner, a way of

sharing threat information with third-parties who wish to synchronise information and research on measures to be taken on recent attacks, suffered by others. Currently, if a Cybersecurity agency wants to retrieve statistical information about a network, it has to agree with the SP and deploy specific hardware on the infrastructure. This is a very costly procedure in both, time and money, which makes it prohibitive for the current market situation. Note that attacks are constantly evolving and require a fast reactive and flexible solution. Using SHIELD instead, Cybersecurity agencies can establish agreements with the SP and deploy vNSF very fast and without cost in the infrastructure. Moreover the data is automatically accessible through the dashboard because the unification of the data treatment done in the data engine.



Methodology

This Survey uses the Analytic Hierarchy Process (AHP) methodology. Each criterion (or sub-criterion) is rated according to its degree of relative importance to another criterion (or sub-criterion) within the group in the basis of pair wise comparison. The consistency of replies are tested. Please indicate your preference by providing a number indicating the relative importance using the following nine point scale:

As shown in the table below when a criterion have an equal importance, it takes score (1). This usually happens when a criterion is compared to itself. When one criterion is from equally to moderate importance compared to another, it takes the score (2) and so on.

Level	Description
1	Equal importance of both elements
3	Moderate importance of one element over another
5	Strong importance of one element over another
7	Very strong importance of one element over another
9	Extreme importance of one element over another
2,4,6,8: Intermediate values	

Questions

By completing this survey, you allow the SHIELD partners to use this information to extract the requirements of the SHIELD platform. The personal data collected is restricted to the "Profiling" section and it is crucial to assist the SHIELD partners to gain a clear picture of your background to understand your concerns regarding the objectives of SHIELD. Moreover, note that the data is not traceable back, so you can not be identified from it and hence, it is considered an anonymous survey. If you have any doubt about this statement, please refer to the person who has sent you the request.

In addition, the survey results are not published and are only used within the SHIELD project generalized and aggregated. After the results of the survey have been extracted, the surveys have been destroyed.

Profiling

1. Type of organization (dropdown menu)
- *Research centre*
- *Academia*
- *ISP/Operator*
- *SME*
- *Industry*

2. Position in organization (dropdown menu) - *Depending on previous response*
- *Technical*
- *Business*
- *Other*

3. Rank your familiarity with the proposed use-cases in decreasing order

- *Use Case 1: An ISP using SHIELD to secure their own infrastructure*
- *Use Case 2: An ISP leveraging SHIELD to provide advanced SecaaS services to customers*
- *Use Case 3: Contributing to national, European and global security*

4. How many employees work in your company?

(Less than 50, 51-100, 101-500, More than 500)

5. What's your knowledge about virtualization services?

(Low, medium, high)

Criteria comparison

The following criteria is used in this survey.

- Relevance of the use cases – Social and economic impact of the use cases.
  - Organization: Considering your organization as an actor in the value chain.
  - EU market: Considering the economic impact of the solution.
  - EU society: Considering the social impact of the solution.
- Threats and vulnerabilities – Targeted threats or vulnerabilities addressed by the solution.
- Security solution aspects – Aspects that cybersecurity solutions must address (cost, easiness to use, etc.)

6. In your opinion, which of these aspects is more important for a cybersecurity solution like SHIELD

Relevance	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	T&V
Relevance	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Security aspects
T&V	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Security aspects

7. Please rate the importance (pairwise comparison) to your organization of each one of the following relevance's sub-criteria.

Organization	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	EU market
Organization	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	EU society
EU market	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	EU society

In each use case (UCx) the full title has been used

Use Case 1: An ISP using SHIELD to secure their own infrastructure

Use Case 2: An ISP leveraging SHIELD to provide advanced SecaaS services to customers

Use Case 3: Contributing to national, European and global security

Importance of the use cases

8. Which one of the three use-cases is more relevant to your organization (as an actor in the value chain)?

Use case 1	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 2
Use case 1	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 3
Use case 2	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 3

9. Which one of the three use-cases do you think is more relevant to the EU market (economic impact)?

Use case 1	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 2
Use case 1	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 3
Use case 2	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 3

10. Which one of the three use-cases do you think is more relevant for the EU as a whole (social impact)?

Use case 1	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 2
Use case 1	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 3
Use case 2	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 3

Threats and vulnerabilities

11. Please rate the importance (pairwise comparison) of each one of the following threats or vulnerabilities to your organization

Denial of Service - Attack that interrupts the systems of the victim not allowing external clients to access to the victim's facilities.

Data Leakage - Data being leaked by a rival company or by a third party which can extort the victim. It also affects to the company's reputation.

Identity theft - An internal account is compromised and the information is used to act in the name of the company.

Scam - An attacker is dishonestly making money by deceiving the company.

Operational interruption - An attacker is trying to interrupt the internal operation of the company, stopping or slowing down one or more production processes.

Denial of Service	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Data Leakage
Denial of Service	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Identity theft
Denial of Service	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Scam
Denial of Service	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Operational interruption
Data Leakage	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Identity theft
Data Leakage	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Scam
Data Leakage	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Operational interruption
Identity theft	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Scam
Identity theft	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Operational interruption
Scam	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Operational interruption

12. Which one of the three use-cases is more important for the Denial of Service T&V?

Use case 1	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 2
Use case 1	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 3
Use case 2	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 3

13. Which one of the three use-cases is more important for the Data Leakage T&V?

Use case 1	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 2
Use case 1	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 3
Use case 2	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 3

14. Which one of the three use-cases is more important for the Identity Theft T&V?

Use case 1	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 2
Use case 1	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 3
Use case 2	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 3

15. Which one of the following use-cases is more important for the Scam T&V?

Use case 1	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 2
Use case 1	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 3
Use case 2	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 3

16. Which one of the following use-cases is more important for the Operational interruption T&V?

Use case 1	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 2
Use case 1	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 3
Use case 2	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 3

17. Do you think there are other treats or vulnerabilities that must be targeted by SHIELD?

Description response.

Security solution aspects

18. Please rate the importance (pairwise comparison) of each one of the following aspects of a cybersecurity solution

Cost – Economic cost of the security solution.

Operational transparency – the solution is not influencing (slowing down, changing processes, etc.) the usual operations of the company.

Ease - not requiring skills, expertise or training for using the solution.

Cybersecurity impact – the cybersecurity solution achieve a high security level for the addressed treats and vulnerabilities.

Confidence/Privacy – the cybersecurity solution is robust and cannot be compromised.

Cost	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Operational transparency
Cost	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Ease
Cost	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Cybersecurity impact
Cost	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Confidence/Privacy
Operational transparency	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Ease
Operational transparency	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Cybersecurity impact
Operational transparency	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Confidence/Privacy
Ease	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Cybersecurity impact
Ease	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Confidence/Privacy
Cybersecurity impact	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Confidence/Privacy

19. Which one of the following use-cases is more important regarding the "Cost" Security Solution Aspect?

Use case 1	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 2
Use case 1	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 3

Use case 2	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 3

20. Which one of the following use-cases is more important regarding the "Operational transparency" Security Solution Aspect?

Use case 1	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 2
Use case 1	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 3
Use case 2	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 3

21. Which one of the following use-cases is more important regarding the "Ease" Security Solution Aspect?

Use case 1	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 2
Use case 1	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 3
Use case 2	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 3

22. Which one of the following use-cases is more important regarding the "Cybersecurity impact" Security Solution Aspect?

Use case 1	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 2
Use case 1	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 3
Use case 2	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 3

23. Which one of the following use-cases is more important regarding the "Confidence/Privacy" Security Solution Aspect?

Use case 1	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 2
Use case 1	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 3
Use case 2	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Use case 3

24. Do you think there are other security solution aspects that must be achieved by SHIELD?

Description response.

Organisation aspects

25. What is the estimated volume of traffic your organisation manages on a daily basis?

Description response.

26. What is the expected availability of the networks, services, etc. in your organisation?

Description response.

27. Is it acceptable for your company deploy the security services outside of your company? (e.g. in the cloud)

(Yes, in a cloud inside of the company; Yes, in a cloud outside of the company; No)

27a. Is your company currently running any of its security services in the Cloud?

(Yes, in a cloud inside of the company; Yes, in a cloud outside of the company; No)

27 b. If yes. Please, describe the services.

Description response.

28. Is it acceptable for your company to provide access to a third party in order to outsource or to share the security management?

(Yes, No)

29. How often would you rely on virtualised security appliances?

(Not at all, sometimes, often, very often)

30. Which do you consider as the strongest advantage of using virtualised security appliances?

Description response.

31. Which do you consider to be the most important disadvantage/weakness of virtualised security appliances?

Description response.

32. Would you like to restrict access to some Internet pages?

(Yes, No, Don't know)

33. Would you like to be warned/asked if you are about to open a scam web page or a web page that might infect your device with a virus or malware?

(Yes, No, Don't know)

34. Would you like to block the access if you are about to open a scam web page or a web page that might infect your device with a virus or malware?

(Yes, No, Don't know)

35. Does your company use a proxy with anti-virus?

(Yes, No, Don't know)

36. Would you be willing to pay for the new security services?

(Yes, No, Don't know)

37. Would you be willing to pay your Internet provider for added-value security features?

(Yes, No, Don't know)

38. How often do you conduct security assessments (remote security scan)?

Description response

39. Which technology is in place to protect network segments from hostile traffic?

(Firewalls, Router/switch ACLSs, Reverse proxy, other (please specify))

40. Is it acceptable for your company sent application security logs to a centralize server in the cloud outside of your company?

(Yes, No, Don't know)

41. What aspects of your current network security process would need improvements? (Costs, Level of security, mobility support, security policies, predicting confidential information)
42. Which kind(s) of security application for malware detection have you deployed or planning to deploy?

(Antivirus, spam protection, phishing protection, other (please specify))

43. What kind of network security application would be you interested in deploying virtualized as a vNSF?

(Denial of service protection, Intrusion detection/prevention system, security gateway, Deep packet Inspection, Firewalls, Honeypots, Web Proxy, other (please specify))

44. Do you foresee any additional need or functionality in the use cases, not already mentioned?

Description response.

45. Would you be willing to share your company's security logs and monitoring information to a third party Cybersecurity certified agency (e.g. public) to contribute to national, European and global security?

Description response.

APPENDIX C2. SURVEY'S RESULTS (REQUIREMENTS ANALYSIS)

The survey results has been grouped and analysed based on two main areas. First, the AHP (Analytic Hierarchy Process) methodology group of questions is focused in business interest. Second technical aspects that cover specific needs on the SHIELD implementation.

AHP [45] [46] is a structured technique for dealing with complex decisions based on a rational and comprehensive framework for decomposing an unstructured complex problem into a multi-level hierarchy of interrelated criteria, sub-criteria and decision alternatives. By incorporating judgments on qualitative and quantitative criteria, AHP manages to quantify decision makers' preferences. The relative priorities of the criteria, sub-criteria and alternatives are finally calculated by a mathematical combination of all these various judgments. Each criterion (or sub-criterion) has been rated according to its degree of relative importance to another criterion (or sub-criterion) within the group in the basis of pair wise comparison. The consistency of replies has been tested.

In the first step, the problem to be investigated has been framed (i.e. its formation articulated) while the criteria and sub-criteria contributing in the achievement of the problem objective have been determined through interviews and/or group discussions with experts within the consortium. The multi-level hierarchy is then constructed, consisting of three levels.

This procedure is based on pairwise judgments of the experts from the second to the lowest level of the hierarchy. At each level, the criteria (and sub-criteria) are compared pair-wisely according to their degree of influence in the use cases and based on the specified criteria at the higher level (dot lines grouping). The "Importance of the use cases" per sub criteria has been calculated from data in the homonym section of the questionnaire. The described comparisons are conducted using the standardized nine levels scale shown in Table 9.

Table 9 - The Ranking Scale

Level (Intensity of importance)	Definition
Equal importance of both elements	1
Moderate importance of one element over another	3
Strong importance of one element over another	5
Very strong importance of one element over another	7
Extreme strong importance of one element over another	9
Intermediate values	2,4,6,8

The experts indicate their preference by providing a number that indicates the relative importance using the nine-point scale. As shown in Table 9 when a criterion has an equal importance, it takes score (1). This usually happens when a criterion is compared to itself. When one criterion, compared to another, is of equal to moderate importance, it takes the score (2) and so on.

The hierarchy, criteria and sub-criteria were conducted by SHIELD partners. Invitations were sent to all partners within the project as well as to customers and experts in order to have a well balanced mix of experts between SMEs, industry, research institutes, academia, ISP operators and government agencies from various European countries (France, Greece, Luxembourg, Portugal, Spain, Italy and United Kingdom). The main expertise of the people who responded lies primarily in the field of technology and secondly in Business.

The online questionnaires were conducted and completed during a period of 1 month (middle October to middle November 2016) with the final set of 26 experts. From the 26 experts who initially participated in the survey, 8 questionnaires were discarded as inconsistent, since their associated Consistency Ratio (CR) was >0.1 (only for the results of questions number 6 to 23 in the AHP method). Nevertheless, all questionnaires were included in the overall results (for the questions number 24 to 45 Organization Aspects).

This sample (18 experts) can be assumed as a sufficient size for the purpose of an AHP analysis since the changes in the probability rank reversal when an additional expert is added to the group are below 1% at M=15 (where M is the number of experts) [47] [48] [49].

The pairwise comparisons were conducted by a web-based survey/road mapping platform incorporating all elements of the AHP framework, where experts accessed the platform and filled in the questionnaires. In detail, experts were asked to determine the criterion (or sub-criterion) of his/her preference - for every pair of criteria (or sub-criteria) - and provide the upper and lower limit to their relative importance using any number between 1 and 9. The web-platform was implemented using Lime Survey [50], an open source tool for web surveys, hosted by INCITES.

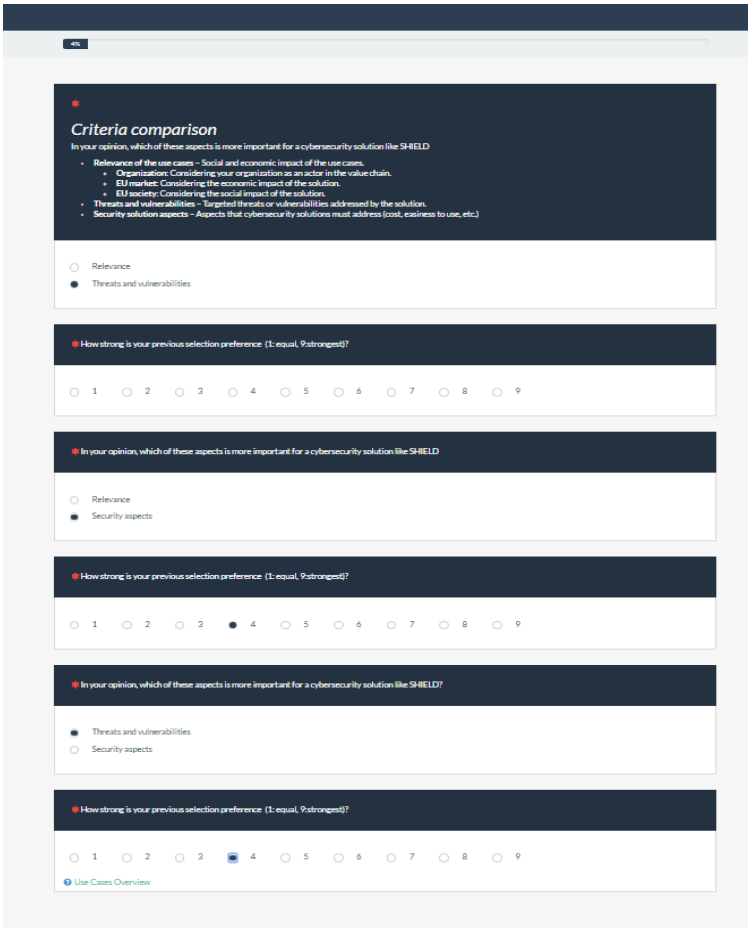


Figure 10 - Shield Survey Tool

Since Lime Survey has not built-in modules to carry out an AHP, the necessary calculations were performed using MATLAB [51], leading to an estimation of the weights signifying the importance of criteria and sub-criteria.

AHP Methodology

This section present and discuss the results of the survey concerning the evaluation of the importance of the criteria and sub-criteria that are expected to affect the Use Cases.

The results concerning the weights of the criteria that are expected to affect Shield UCs are shown in Table 10. (AHP Methodology)

Table 10 - Criteria

Criteria	Weight
Relevance of the use cases	28.4%
Threats and vulnerabilities – Targeted threats or vulnerabilities addressed by the solution.	**43.6%**

Criteria	Weight
Security solution aspects – Aspects that cybersecurity solutions must address (cost, easiness to use, etc.)	28.0%

- The Threats and Vulnerabilities criterion is almost twice as the rest criteria which are of equal importance.

The Importance of the Use Cases is presented in the Table 11.

Table 11 - Importance of the Use Cases

Criteria	Weight
Use Case 1: An ISP using SHIELD to secure their own infrastructure	29.1%
Use Case 2: An ISP leveraging SHIELD to provide advanced SecaaS services to customers	**46.6%**
Use Case 3: Contributing to national, European and global security	24.2%

- UC2 is almost preferable for half of the people followed by UC1. On the contrary UC3 is important for 1/3 of the people.
- Business preferable case is UC1.

In order to capture a global view of the sub-criteria ranking, the global priorities need to be calculated. The global priorities are obtained by multiplying the local priorities (sub-criteria weights) by their parent's priority (Criteria weight).

The Sub Criteria Importance is presented in Table 12.

Table 12 - Importance of the Sub Criteria (Total)

Sub-Criteria	Weight
Data Leakage	15.7%
Organization	14.3%
Identity theft	10.5%
Cybersecurity impact	10.1%
EU society	8.1%
Confidence/Privacy	8.0%
Operational interruption	6.6%
Denial of Service	6.0%
EU market	6.0%
Scam	4.8%
Cost	4.7%
Operational transparency	3.1%
Ease	2.1%

The results presented in table above are a valuable tool for the requirements analysis of Shield Platform. In fact, they provide very useful guidelines for the key criteria for a successful deployment of similar platforms.

- As shown, the most important factors expected to affect the Usability of all UCs in general are Data Leakage, Organization, Identity theft and Cybersecurity impact.
- On the contrary less important are Operational transparency and Ease (not requiring skills, expertise or training for using the solution)

Table 13 - Importance of the Sub Criteria in Criterion (Relevance)

Sub-Criteria	Weight
Organization	50.3%
EU society	28.7%
EU market	21.0%

- As shown, the most important factor for Relevance of the UC is Organization (actor in the value chain).

Table 14 - Importance of the Sub Criteria in Criterion (Threats and vulnerabilities)

Sub-Criteria	Weight
Data Leakage	36.0%
Identity theft	24.1%
Operational interruption	15.1%
Denial of Service	13.8%
Scam	11.0%

- As shown, the most important factors for T&V aspect of the UC are Data Leakage (to a greater degree) and Identify theft. Nevertheless, Scam is of less importance.

Table 15 - Importance of the Sub Criteria in Criterion (Security Aspects)

Sub-Criteria	Weight
Cybersecurity impact	36.0%
Confidence/Privacy	28.5%
Cost	16.9%
Operational transparency	11.0%
Ease	7.6%

- As shown, the most important factors for Security solution aspect of the UC are Cybersecurity impact (high security level) and Confidence/Privacy (robust and cannot be compromised). Ease is of less importance for Security Aspects since experience personnel usually could be involved in such activities.

The total AHP results are illustrated in Table 16.

Table 16 - AHP Overall Results

Criteria	Relevance			Threats and Vulnerabilities					Security Aspects					
	0.28			0.44					0.28					
	Organization	EU market	EU society	Denial of Service	Data Leakage	Identity theft	Scam	Operational interruption	Cost	Operational transparency	Ease	Cybersecurity impact	Confidence/ Privacy	**Global Alternatives of UCs**
	0.50	0.21	0.29	0.14	0.36	0.24	0.11	0.15	0.17	0.11	0.08	0.36	0.29	
UC1	0.29	0.22	0.15	0.46	0.25	0.20	0.16	0.44	0.31	0.41	0.29	0.33	0.40	**29.1%**
UC2	0.54	0.43	0.35	0.35	0.59	0.58	0.62	0.41	0.51	0.36	0.48	0.32	0.32	**46.6%**
UC3	0.16	0.35	0.51	0.19	0.16	0.21	0.23	0.14	0.18	0.24	0.23	0.35	0.28	**24.2%**

In addition more results have been calculated per stakeholder (i.e. ranked results per criterion and sub criteria). In the Stakeholder's analysis for the sub criteria we could identify a different ranking for some cases (Table 17).

Table 17 - Importance of the Sub Criteria per Stakeholders

	Organization	EU market	EU society	Denial of Service	Data Leakage	Identity theft	Scam	Operational interruption	Cost	Operational transparency	Ease	Cybersecurity impact	Confidence /Privacy
ALL	14.3%	6.0%	8.1%	6.0%	15.7%	10.5%	4.8%	6.6%	4.7%	3.1%	2.1%	10.1%	8.0%
SMEs	10.5%	5.1%	6.4%	6.9%	16.9%	20.3%	8.1%	4.8%	4.7%	2.0%	1.7%	7.8%	4.8%
Industy	6.6%	9.3%	4.8%	1.7%	20.5%	22.2%	5.1%	5.3%	2.1%	3.6%	2.1%	11.3%	5.6%
Research Centers	20.0%	1.8%	9.0%	3.8%	11.2%	6.5%	2.4%	11.0%	3.4%	3.3%	1.4%	11.5%	14.7%
Academia	22.2%	6.2%	8.3%	2.8%	10.5%	4.8%	4.0%	6.7%	7.0%	4.4%	4.7%	8.7%	9.8%
ISPs_Operators	19.1%	9.7%	18.8%	13.0%	7.7%	1.6%	1.5%	7.3%	2.8%	2.0%	1.1%	6.1%	9.4%
Government	5.3%	2.6%	1.2%	2.7%	10.6%	6.8%	0.9%	0.7%	9.8%	7.3%	2.8%	40.9%	8.3%
Technical	16.4%	5.8%	9.1%	5.3%	16.0%	9.6%	3.6%	6.9%	3.6%	3.0%	1.8%	9.8%	9.1%
Other	12.3%	9.6%	11.7%	4.8%	9.9%	12.2%	8.2%	5.6%	5.0%	4.2%	2.6%	8.9%	5.0%
Business	6.0%	2.3%	1.5%	15.7%	19.2%	6.8%	5.6%	5.1%	15.9%	1.6%	4.3%	8.8%	7.1%
SMEs	-3.8%	-0.8%	-1.8%	0.8%	1.2%	9.7%	3.3%	-1.7%	0.0%	-1.1%	-0.5%	-2.2%	-3.1%
Industy	-7.7%	3.3%	-3.4%	-4.3%	4.8%	11.7%	0.3%	-1.3%	-2.6%	0.5%	-0.1%	1.2%	-2.4%
Research Centers	5.7%	-4.2%	0.8%	-2.2%	-4.4%	-4.0%	-2.4%	4.4%	-1.3%	0.2%	-0.7%	1.4%	6.7%
Academia	7.9%	0.3%	0.2%	-3.2%	-5.2%	-5.8%	-0.8%	0.1%	2.3%	1.3%	2.6%	-1.4%	1.8%
ISPs_Operators	4.8%	3.7%	10.7%	7.0%	-8.0%	-8.9%	-3.3%	0.7%	-1.9%	-1.1%	-1.0%	-4.0%	1.4%
Government	-9.0%	-3.4%	-6.9%	-3.4%	-5.1%	-3.7%	-3.9%	-5.9%	5.1%	4.2%	0.6%	30.9%	0.4%
Technical	2.1%	-0.2%	1.0%	-0.7%	0.3%	-0.9%	-1.2%	0.3%	-1.1%	-0.1%	-0.3%	-0.3%	1.1%
Other	-2.0%	3.6%	3.5%	-1.2%	-5.8%	1.7%	3.4%	-1.0%	0.3%	1.2%	0.5%	-1.2%	-3.0%
Business	-8.3%	-3.7%	-6.7%	9.7%	3.5%	-3.7%	0.8%	-1.4%	11.2%	-1.5%	2.2%	-1.3%	-0.8%

In the first part of the table (starting at ALL row ending at Business row) dark green being the highest value (priorities for the Stakeholders) and red being the lowest.

In the second part of the table (starting at SMEs row) a comparison (difference) with the main answers (row: ALL) has been presented.

- Cost is more important for Business (+11.2%) (logical results since cost of the services is closely related to Business)
- Cybersecurity impact is more important for Government presenting a factor of +30.9% (Government Agency is more interested in a high security level for the addressed threats and vulnerabilities as their data is probably sensitive).
- EU society (social impact of the solution) is more important for the ISPs Operators (+10.7%) (sensitive data)
- Organization (actor in the value chain) is more important for Research Centers (+5.7%), Academia (+7.9%) and ISPs (+4.8%) than for Government (-9%) and Industry (-7.7%). (for Government these results are probably logical, on the other hand, Industry should have been more interested in the actor position in the value chain)
- Identify Theft is more important for SMEs (+9.7%) and Industry (11.7%) (the result should be related to identification of the Theft in order to have successful results)
- Denial of Services is more important for Business (+9.7%, a logical result, since no access to data would result in no revenues for the services offered).

Technical Questionnaire analysis

This section collect the analysis of the survey's responses related to the group of organizational aspects that appear in the survey.

TQ1	Availability of the networks
Answered: 30%	>99%

TQ2	Acceptable deploy security services outside of the company (e.g. in the cloud)

No (1):	7,7 %
Yes, in a cloud inside of the company (2):	50 %
Yes, in a cloud outside of the company (3):	42,3 %

	% SME	% Industry	% Research Centre	% Academia	% ISP/Operator	% Gover. Agency
(1)	9,1	0	0	0	0	50
(2)	27,3	100	66,7	66,7	50	50
(3)	63,6	0	33,3	33,3	50	0

TQ3	Company is currently running any of its security services in the Cloud

No (1):	79,2 %
Yes, in a cloud inside of the company (2):	20,8 %

	% SME	% Industry	% Research Centre	% Academia	% ISP/Operator	% Gover. Agency
(1)	81,8	66,7	66,7	100	50	50
(2)	9,1	33,3	33,3	0	50	0

e.g.	VPN	Content filter, spam filter	We use the security services used in a Openstack deployment		Antivirus, Firewall, Content Filtering, Clean Pipes	

TQ4	Acceptable to provide access to a third party in order to outsource or to share the security management

Yes (1):	50 %

	% SME	% Industry	% Research Centre	% Academia	% ISP/Operator	% Gover. Agency
(1)	72,7	33,3	0	33,3	50	50

TQ5	Confidence on virtualized security appliances

Not at all (1):	19,2 %
Sometimes (2):	53,8 %
Often (3):	19,2 %
Very often (4):	7,7 %

	% SME	% Industry	% Research Centre	% Academia	% ISP/Operator	% Gover. Agency
(1)	18,2	33,3	0	33,3	0	50
(2)	45,5	66,7	33,3	66,7	75	50
(3)	27,3	0	66,7	0	0	0
(4)	9,1	0	0	0	25	0

TQ6	Strongest advantage of using virtualised security appliances

	Answer	% Answered
SME	-Higher flexibility to deploy and manage security solutions. -The transparency and the availability. -Flexibility, Agility, Lower costs of maintenance -Efficiency, Cost	36,4
Industry	-Scalability, rapid upgrades -versatility, quick patching cycle	66,7
Research Centre	- Cost - Dynamism: -- Fast disaster recovery (e.g. compromised instanced are replaced by new ones in short time with no cost). -- Scalability. Possibility to dynamically deploy more controls or different ones. - Ease of deployment	100
Academia		0
ISP/Operator	Cost	25
Government Agency	The capability to manage new threats.	50

TQ7	Most important disadvantage/weakness of virtualised security appliances

	Answer	% Answered
SME	-Being externally exposed. -Could it mean that the physical layer is also vulnerable?	18,2
Industry	Availability	33,3
Research Centre	-Stability - Slowness. They can't leverage hardware acceleration to speed up traffic inspection or other specific tasks. - Complexity of management\In some cases they could increase network latency.	100
Academia		0
ISP/Operator	To adapt to the new technology.	25
Government Agency	The performances and the need to guarantee the security of the system that runs the virtualized security appliances.	50

TQ8	Would you like to restrict access to some Internet pages?

Yes (1):	46,2 %
No (2):	38,5 %
Don't know (3):	15,4 %

	% SME	% Industry	% Research Centre	% Academia	% ISP/Operator	% Gover. Agency

(1)	36,4	33,3	33,3	100	50	50
(2)	54,5	33,3	33,3	0	25	50
(3)	9,1	33,3	33,3	0	25	0

TQ9	Would you like to be warned/asked if you are about to open a scam web page that might infect your device?

Yes (1):	96,2 %
No (2):	0 %
Don't know (3):	3,8 %

	% SME	% Industry	% Research Centre	% Academia	% ISP/Operator	% Gover. Agency
(1)	100	100	100	100	75	100
(2)	0	0	0	0	0	0
(3)	0	0	0	0	25	0

TQ10	Would you like to block the access if you are about to open a scam web page or a web page that might infect your device with a virus or malware?

Yes (1):	76,9 %
No (2):	11,5 %
Don't know (3):	11,5 %

	% SME	% Industry	% Research Centre	% Academia	% ISP/Operator	% Gover. Agency
(1)	81,8	66,7	100	100	25	100
(2)	9,1	0	0	0	50	0
(3)	9,1	33,3	0	0	25	0

TQ11	Company use a proxy with anti-virus

Yes (1):	34,6 %
No (2):	34,6 %
Don't know (3):	30,8 %

	% SME	% Industry	% Research Centre	% Academia	% ISP/Operator	% Gover. Agency
(1)	9,1	66,7	0	33,3	75	100
(2)	36,4	33,3	66,7	66,7	0	0
(3)	54,5	0	33,3	0	25	0

TQ12	Would you be willing to pay for the new security services?

Yes (1):	38,5 %
No (2):	0 %
Don't know (3):	61,5 %

	% SME	% Industry	% Research Centre	% Academia	% ISP/Operator	% Gover. Agency
(1)	36,4	33,3	33,3	33,3	50	50
(2)	0	0	0	0	0	0
(3)	63,6	66,7	66,7	66,7	50	50

TQ13	Would you be willing to pay your Internet provider for added-value security features?

Yes (1):	53,8 %
No (2):	15,4 %
Don't know (3):	30,8 %

	% SME	% Industry	% Research Centre	% Academia	% ISP/Operator	% Gover. Agency
(1)	54,5	33,3	66,7	33,3	50	100
(2)	9,1	33,3	0	0	50	0
(3)	36,4	33,3	33,3	66,7	0	0

TQ14	How often do you conduct security assessments (remote security scan)?	
	Answer	**% Answered**
SME	-Don't know. -Rarely -Not very often	27,3
Industry	-once a year	33,3
Research Centre	-Never -Don't know	66,7
Academia		0
ISP/Operator	-Yearly -Once a year	50
Government Agency	When new resources are added or the configuration is significantly changed.	50

TQ15	Which technology is in place to protect network segments from hostile traffic? [Firewalls]
Yes (1):	92,3 %
No (2):	7,7 %
Don't know (3):	0 %

	% SME	% Industry	% Research Centre	% Academia	% ISP/Operator	% Gover. Agency
(1)	90,9	100	66,7	100	100	100
(2)	9,1	0	33,3	0	0	0
(3)	0	0	0	0	0	0

TQ16	Which technology is in place to protect network segments from hostile traffic? [Router/switch ACLSs]
Yes (1):	61,5 %
No (2):	38,5 %
Don't know (3):	0 %

	% SME	% Industry	% Research Centre	% Academia	% ISP/Operator	% Gover. Agency
(1)	36,4	100	66,7	100	50	100
(2)	63,6	0	33,3	0	50	0
(3)	0	0	0	0	0	0

TQ17	Which technology is in place to protect network segments from hostile traffic? [Reverse proxy]
Yes (1):	19,2 %
No (2):	80,8 %
Don't know (3):	0 %

	% SME	% Industry	% Research Centre	% Academia	% ISP/Operator	% Gover. Agency
(1)	36,4	0	0	0	0	50
(2)	63,6	100	100	100	100	50
(3)	0	0	0	0	0	0

TQ18	Which technology is in place to protect network segments from hostile traffic? [Other]	
	Answer	% Answered
SME		0
Industry		0
Research Centre	No idea, probably a NAT	33,3
Academia		0
ISP/Operator		0
Government Agency		0

TQ19	Is it acceptable to send application security logs to a centralize server in the cloud outside of your company?					
Yes (1):	34,6 %					
No (2):	19,2 %					
Don't know (3):	46,2 %					
	% SME	% Industry	% Research Centre	% Academia	% ISP/Operator	% Gover. Agency
(1)	45,5	0	66,7	33,3	0	50
(2)	9,1	33,3	0	33,3	25	50
(3)	45,5	66,7	33,3	33,3	75	0

TQ20	What aspects of your current network security process would need improvements? [Costs]					
Yes (1):	34,6 %					
No (2):	65,4 %					
Don't know (3):	0 %					
	% SME	% Industry	% Research Centre	% Academia	% ISP/Operator	% Gover. Agency
(1)	45,5	0	0	66,7	50	0
(2)	54,5	100	100	33,3	50	100
(3)	0	0	0	0	0	0

TQ21	What aspects of your current network security process would need improvements? [Level of security]					
Yes (1):	57,7 %					
No (2):	42,3 %					
Don't know (3):	0 %					
	% SME	% Industry	% Research Centre	% Academia	% ISP/Operator	% Gover. Agency
(1)	63,6	33,3	66,7	66,7	75	0
(2)	36,4	66,7	33,3	33,3	25	100
(3)	0	0	0	0	0	0

TQ22	What aspects of your current network security process would need improvements? [Mobility support]					
Yes (1):	46,2 %					
No (2):	53,8 %					
Don't know (3):	0 %					
	% SME	% Industry	% Research Centre	% Academia	% ISP/Operator	% Gover. Agency
(1)	54,5	66,7	66,7	33,3	0	50
(2)	45,5	33,3	33,3	66,7	100	50

(3)	0	0	0	0	0	0

TQ23	What aspects of your current network security process would need improvements? [Security policies]

Yes (1):	65,4 %
No (2):	34,6 %
Don't know (3):	0 %

	% SME	% Industry	% Research Centre	% Academia	% ISP/Operator	% Gover. Agency
(1)	63,6	100	100	66,7	25	50
(2)	36,4	0	0	33,3	75	50
(3)	0	0	0	0	0	0

TQ24	What aspects of your current network security process would need improvements? [Protecting confidential information]

Yes (1):	61,5 %
No (2):	38,5 %
Don't know (3):	0 %

	% SME	% Industry	% Research Centre	% Academia	% ISP/Operator	% Gover. Agency
(1)	72,7	66,7	66,7	66,7	25	50
(2)	27,3	33,3	33,3	33,3	75	50
(3)	0	0	0	0	0	0

TQ25	Which kind(s) of security application for malware detection have you deployed or planning to deploy? [Antivirus]

Yes (1):	69,2 %
No (2):	30,8 %
Don't know (3):	0 %

	% SME	% Industry	% Research Centre	% Academia	% ISP/Operator	% Gover. Agency
(1)	63,6	66,7	66,7	66,7	75	100
(2)	36,4	33,3	33,3	33,3	25	0
(3)	0	0	0	0	0	0

TQ26	Which kind(s) of security application for malware detection have you deployed or planning to deploy? [Spam protection]

Yes (1):	57,7 %
No (2):	42,3 %
Don't know (3):	0 %

	% SME	% Industry	% Research Centre	% Academia	% ISP/Operator	% Gover. Agency
(1)	45,5	100	33,3	100	25	100
(2)	54,5	0	66,7	0	75	0
(3)	0	0	0	0	0	0

TQ27	Which kind(s) of security application for malware detection have you deployed or planning to deploy? [Phishing protection]

Yes (1):	23,1 %
No (2):	76,9 %
Don't know (3):	0 %

	% SME	% Industry	% Research Centre	% Academia	% ISP/Operator	% Gover. Agency
(1)	27,3	0	0	33,3	0	100
(2)	72,7	100	100	66,7	100	0

(3)	0	0	0	0	0	0

TQ28	Which kind(s) of security application for malware detection have you deployed or planning to deploy? [Other]	
	Answer	% Answered
SME	-Firewall -don't know	18,2
Industry		0
Research Centre	-Nothing	33,3
Academia		0
ISP/Operator	-Don't Know	25
Government Agency		0

TQ29	What kind of network security application would be you interested in deploying virtualized as a vNSF? [Denial of service protection]					
Yes (1):	76,9 %					
No (2):	23,1 %					
Don't know (3):	0 %					
	% SME	% Industry	% Research Centre	% Academia	% ISP/Operator	% Gover. Agency
(1)	81,8	66,7	100	66,7	75	50
(2)	18,2	33,3	0	33,3	25	50
(3)	0	0	0	0	0	0

TQ30	What kind of network security application would be you interested in deploying virtualized as a vNSF? [Intrusion detection/prevention system]					
Yes (1):	76,9 %					
No (2):	23,1 %					
Don't know (3):	0 %					
	% SME	% Industry	% Research Centre	% Academia	% ISP/Operator	% Gover. Agency
(1)	81,8	66,7	100	66,7	100	0
(2)	18,2	33,3	0	33,3	0	100
(3)	0	0	0	0	0	0

TQ31	What kind of network security application would be you interested in deploying virtualized as a vNSF? [Security gateway]					
Yes (1):	50 %					
No (2):	50 %					
Don't know (3):	0 %					
	% SME	% Industry	% Research Centre	% Academia	% ISP/Operator	% Gover. Agency
(1)	54,5	33,3	66,7	66,7	50	0
(2)	45,5	66,7	33,3	33,3	50	100
(3)	0	0	0	0	0	0

TQ32	What kind of network security application would be you interested in deploying virtualized as a vNSF? [Deep packet Inspection]

Yes (1):	50 %
No (2):	50 %
Don't know (3):	0 %

	% SME	% Industry	% Research Centre	% Academia	% ISP/Operator	% Gover. Agency
(1)	45,5	100	66,7	0	50	50
(2)	54,5	0	33,3	100	50	50
(3)	0	0	0	0	0	0

TQ33	What kind of network security application would be you interested in deploying virtualized as a vNSF? [Firewalls]

Yes (1):	76,9 %
No (2):	23,1 %
Don't know (3):	0 %

	% SME	% Industry	% Research Centre	% Academia	% ISP/Operator	% Gover. Agency
(1)	81,8	33,3	100	100	75	50
(2)	18,2	66,7	0	0	25	50
(3)	0	0	0	0	0	0

TQ34	What kind of network security application would be you interested in deploying virtualized as a vNSF? [Honeypots]

Yes (1):	38,5 %
No (2):	61,5 %
Don't know (3):	0 %

	% SME	% Industry	% Research Centre	% Academia	% ISP/Operator	% Gover. Agency
(1)	27,3	100	66,7	0	25	50
(2)	72,7	0	33,3	100	75	50
(3)	0	0	0	0	0	0

TQ35	What kind of network security application would be you interested in deploying virtualized as a vNSF? [Web Proxy]

Yes (1):	19,2 %
No (2):	80,8 %
Don't know (3):	0 %

	% SME	% Industry	% Research Centre	% Academia	% ISP/Operator	% Gover. Agency
(1)	18,2	33,3	66,7	0	0	0
(2)	81,8	66,7	33,3	100	100	100
(3)	0	0	0	0	0	0

TQ36	What kind of network security application would be you interested in deploying virtualized as a vNSF? [Other]

	Answer	% Answered
SME		0
Industry		0
Research Centre		0
Academia		0
ISP/Operator		0
Government Agency	APT protection	50

TQ37	Do you foresee any additional need or functionality in the use cases, not already mentioned?	
	Answer	% Answered
SME	No.	9,1
Industry		0
Research Centre	-An IDPS commonly requires protected systems to be centrally managed, which may not be possible. There may be need for the system to provide its features without managing the systems. -No	66,7
Academia		0
ISP/Operator		0
Government Agency	Sandboxing	50

TQ38	Would you be willing to share your company's security logs and monitoring information to a third party Cybersecurity certified agency (e.g. public) to contribute to national, European	
	Answer	% Answered
SME	-Don't know. -Probably. It depends on the agency policies. -Maybe not	27,3
Industry		0
Research Centre	-Probably in case of an attack of broader impact (not only inside the organization, but distributed across the country or so) -Don't know	66,7
Academia	Yes	33,3
ISP/Operator	\\I'm not sure.	25
Government Agency	-Yes. Our organisation could perform these tasks. -N/A	100