SHIELD

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

[H2020 - Grant Agreement No. 700199]

Deliverable D2.1

Requirements, KPIs, design and architecture

Editor	Ludovic Jacquin (HPELB)
Contributors	H. Attak, L. Jacquin (HPELB), C. Fernandez, C. Dávila, B. Gastón (I2CAT), D. Katsianis, I. Neokosmidis (INCITES), A. Litke, N. Papadakis, D. Papadopoulos (INFILI), E. Trouva (NCSRD), E.-C. Davri, G. Xylouris, E. Kafetzakis (ORION), A. Lioy (POLITO), G. Gardikis, K. Tzoulas (SPH), A. Pastor, J. Núñez, D. Lopez (TID), T. Batista, R. Preto (UBI)
Version	1.0
Date	February 28th, 2017
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 (UCs), the elicitation of the requirements and the high-level architectural design of the SHIELD system.

SHIELD offers security-as-a-Service in an evolved telco environment, leveraging NFV (Network Function Virtualisation) and SDN (Software-Defined Networking) for virtualization and dynamic placement of security appliances in the network (virtual Network Security Functions – vNSFs), Big Data analytics for real-time incident detection and mitigation, as well as attestation techniques for securing both infrastructure and services. Three high-level use cases were identified as most relevant for the SHIELD framework:

- *Use Case 1:* An Internet Service Provider (ISP) using SHIELD to secure its own infrastructure. This UC involves the ISPs deploying vNSFs in their network to detect incidents.
- *Use Case 2:* An ISP leveraging SHIELD to provide advanced SecaaS services to customers. This UC assumes that network security services (consisting of vNSFs), along with real-time incident detection and management, are offered as-a-Service to ISP clients, such as enterprises, public bodies, etc.
- *Use Case 3:* Contributing to national, European and global security. This UC assumes that incident information is exposed, in a secure and private manner, to public cybersecurity authorities.

The next step identified the high-level system requirements, which would drive the design task. For the gathering of the requirements, three sources were used:

- The three identified use cases
- User stories, as drafted from various stakeholders inside the SHIELD consortium expressing desired functionalities/interactions with users
- An online survey, aimed at prioritizing the use cases and collecting additional requirements.

The online survey was addressed at targeted persons, both within and outside the consortium, that are professionally engaged with information security tasks. It was divided in three parts: profiling of the experts, criteria comparison part and organizational aspects. The criteria comparison part used the Analytic Hierarchy Process (AHP) methodology in order to prioritise the three use cases based on several criteria. The result of the analysis of the responses was that UC2 is preferred by half of the interviewees (mainly Businesses), followed at distance by UC1 and UC3. The criteria identified as of high importance for the SHIELD platform are protection against data leakage and Identity theft, as well as compliance with organizational needs and policies. On the contrary, the less important aspects, among the listed ones, seem to be are operational transparency and ease of use. Finally, the main results of the responses regarding the organizational aspects show a good predisposition to deploy security services in a cloud environment (around 93%), being the flexibility and cost a positive factor, but showing as main concern the service security.

The requirements elicited from the above mentioned sources are divided in i) general platform requirements and ii) vNSFs and analytics required.

In the first category, general functional requirements of the SHIELD platform are included, such as: vNSF deployment and lifecycle management, data monitoring, analytics and visualisation. Non-functional requirements for the SHIELD platform are also identified, concerning responsiveness, availability, and scalability.

In the second category, the functionalities needed by the vNSFs are included. Based on the survey results, the most popular functionalities include: blocking the access to malware and malicious websites, Layer 4 traffic filtering, spam protection, Distributed Denial of Service (DDoS) protection as well as Intrusion Detection System/Intrusion Prevention System (IDS/IPS) functionalities.

Considering the use cases and requirements identified as well as the state-of-the-art in NFV and data analytics architectures, including standardisation trends, a high-level overall architecture is proposed. This architecture encompasses all the component entities of the SHIELD system, and its main components are:

- 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 (vNSFs): implementing the traffic processing functionalities, as desired by the users.
- The vNSF Orchestrator: central entity responsible for managing the vNSF lifecycle.
- The vNSF Store: catalogue which contains the available vNSFs and associated security Network Services (sets of vNSFs)
- The Trust Monitor: entity responsible for attesting the infrastructure and the services while validating their integrity.
- The Data Analytics and Remediation Engine (DARE): complex entity that analyses in real-time the information reported by the vNSFs and detects security incidents, triggering in turn appropriate actions to mitigate the threats.
- The Security Dashboard: graphical front-end of the platform to the various actors interacting with it.

The workflows between components or subsystems are presented as sequence diagrams per use case. This is an exercise to validate that all defined use cases can be realised via the proposed architecture.

Table of Contents

1. INTRODUCTION

The SHIELD project aims at providing a solution against the growing new kind of cyber-attacks that target both the economy and the society. One of the main challenges is the fast-paced evolution which takes advantage of legacy protection mechanisms that are usually designed to address particular attacks and that are statically configured by human operators. SHIELD bridges the gap between ever-evolving cyber-attacks and the running-behind defences by leveraging on the coupling of Network Functions Virtualisation (NFV) paradigm with data analytics; in order to predict specific vulnerabilities and attacks by analysing the network and understanding the adversary possibilities, behaviour and intent. This approach also promotes openness and interoperability of security functions and offers affordable security solutions.

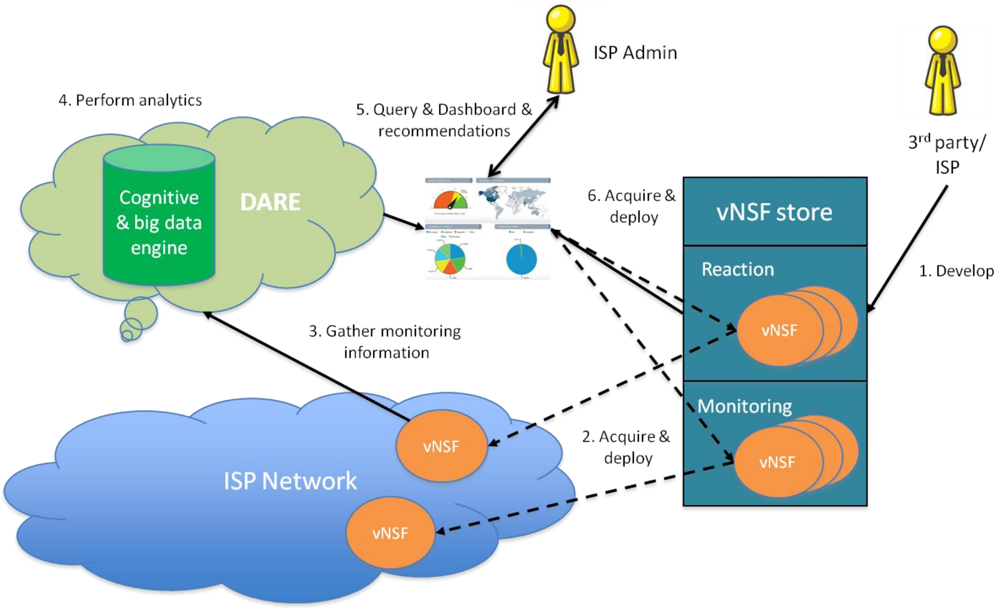
SHIELD virtualizes the security functions through the NFV concept, as currently standardised by ETSI: a network function, in the NFV design, decouples the functionality from the hardware required. This permits a much more flexible environment, where the security functions can be distributed or scaled more efficiently. SHIELD relies mainly on two kind of virtual Network Security Functions (vNSF): monitoring vNSFs, typically responsible for aggregating security-related logs and metrics; and reacting vNSFs, exerting protection against attacks.

Between the two types of vNSF subsists the Data Analysis and Remediation Engine (DARE) which analyses the logs and metrics to detect potential attacks; once patterns are identified, the DARE can recommend or directly react to attacks by indirectly indicating the appropriate reacting vNSF to be deployed in the best location of the network topology. The DARE is based on state-of-the-art big data solutions. This, coupled with an analytic engine, allows SHIELD to use tailor-made security analysis module to address attacks, ideally by predicting them first.

The use-cases identified in SHIELD are explained below in more detail:

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

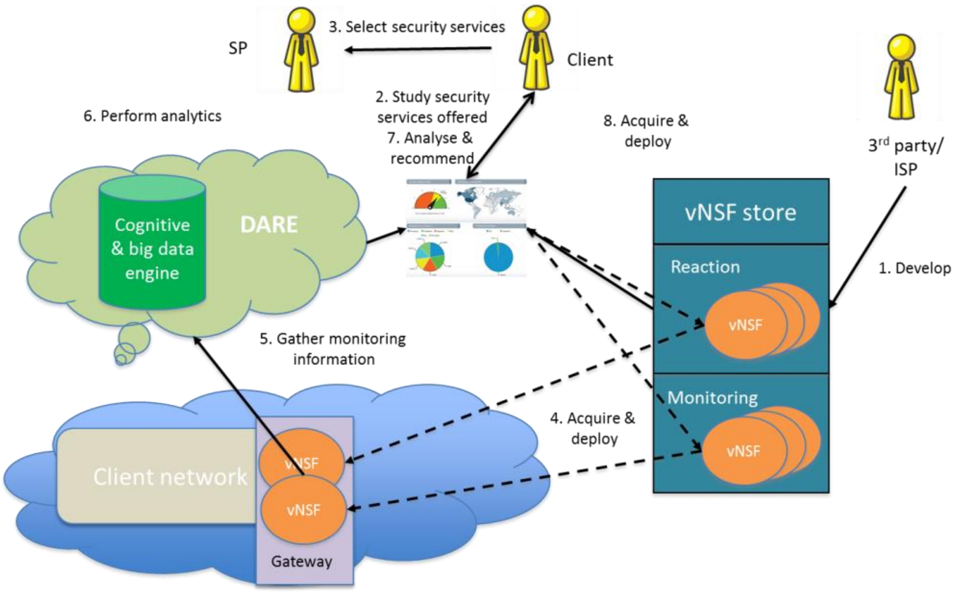
In order to protect their own network infrastructure, ISPs have to deploy specific hardware which is very expensive since this hardware has to be maintained by very specialized operators. Furthermore, the operators may need to invest time troubleshooting the attack first. The virtualization offered by SHIELD in this use case aims to dramatically reduce both costs by replacing specific hardware for vNSFs (virtual Network Security Functions), as well as providing a central interface (dashboard) to understand the implications of the gathered information and analysis, and then act in the network.



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

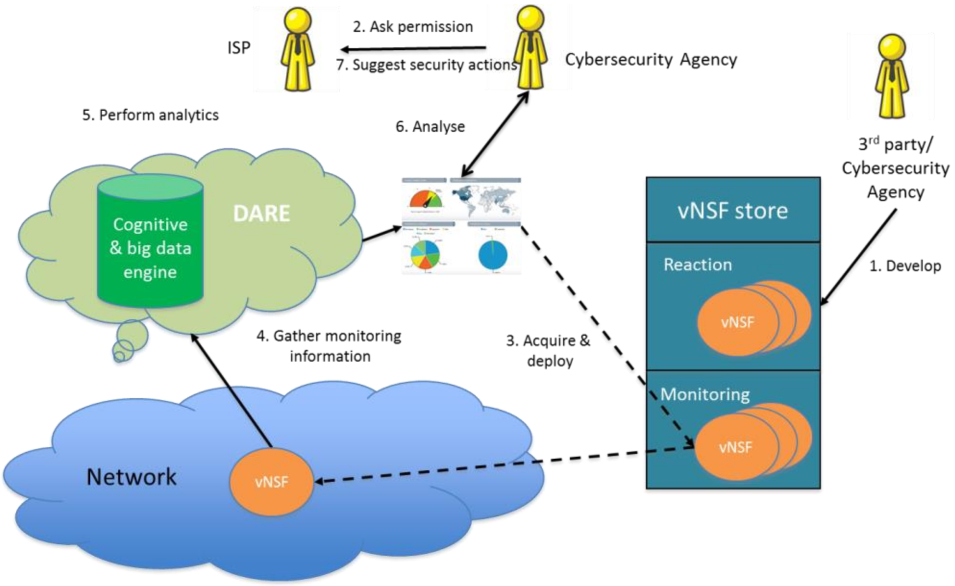
As aforementioned, SHIELD provides an ideal foundation for building enhanced SecaaS services, far beyond current offerings. Using this SecaaS paradigm, the complexity of the security analysis can be hidden from the client (either a company or an SME) who can be freed from the need to acquire, deploy,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

The dashboard, available to authorised actors, accepts ad-hoc requests regarding threat models or acquired threat intelligence. This data 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 quickly and without extra cost in the infrastructure. Moreover, the analysed data is accessible from the dashboard because its processing is done in the DARE.



This document is organised in two sections: in the first section the objectives of SHIELD are analysed and in the second, an overview of the technical solution to those objectives is presented – detailing the main components and their interaction.

2. SHIELD OBJECTIVES

2.1. Use cases analysis

WP2 "Use case requirements & SHIELD architecture & business models" is responsible for analysing the general scenario of SHIELD, along with the specific use cases, and specifying requirements based on the stakeholders' needs and the required infrastructure. This task collects the requirements of the different SHIELD stakeholders obtained through standard techniques, such as questionnaires and focus groups.

The SHIELD survey for requirements analysis 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.

AHP [1][2] 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.

In the first level, the objective under investigation is the ranking of the Use Cases identified.

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

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, easiness to 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 for using 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.

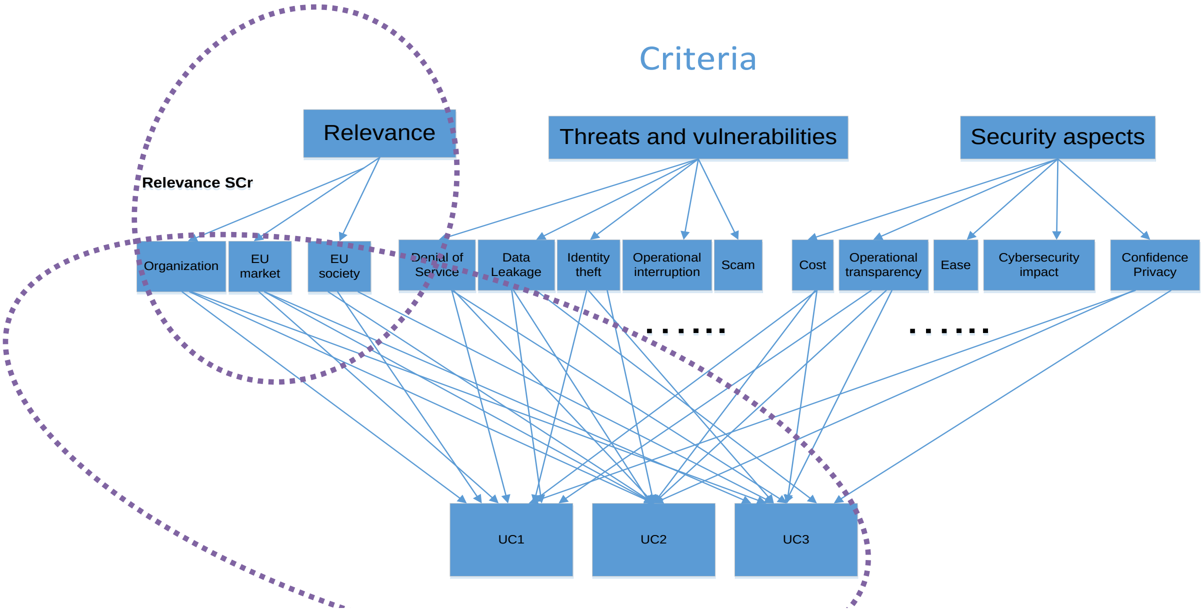


Figure 1 - Multi-Level Hierarchy

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 corresponding section of the questionnaire. The described comparisons are conducted using the standardized nine levels scale shown in Table 1.

Table 1 - 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

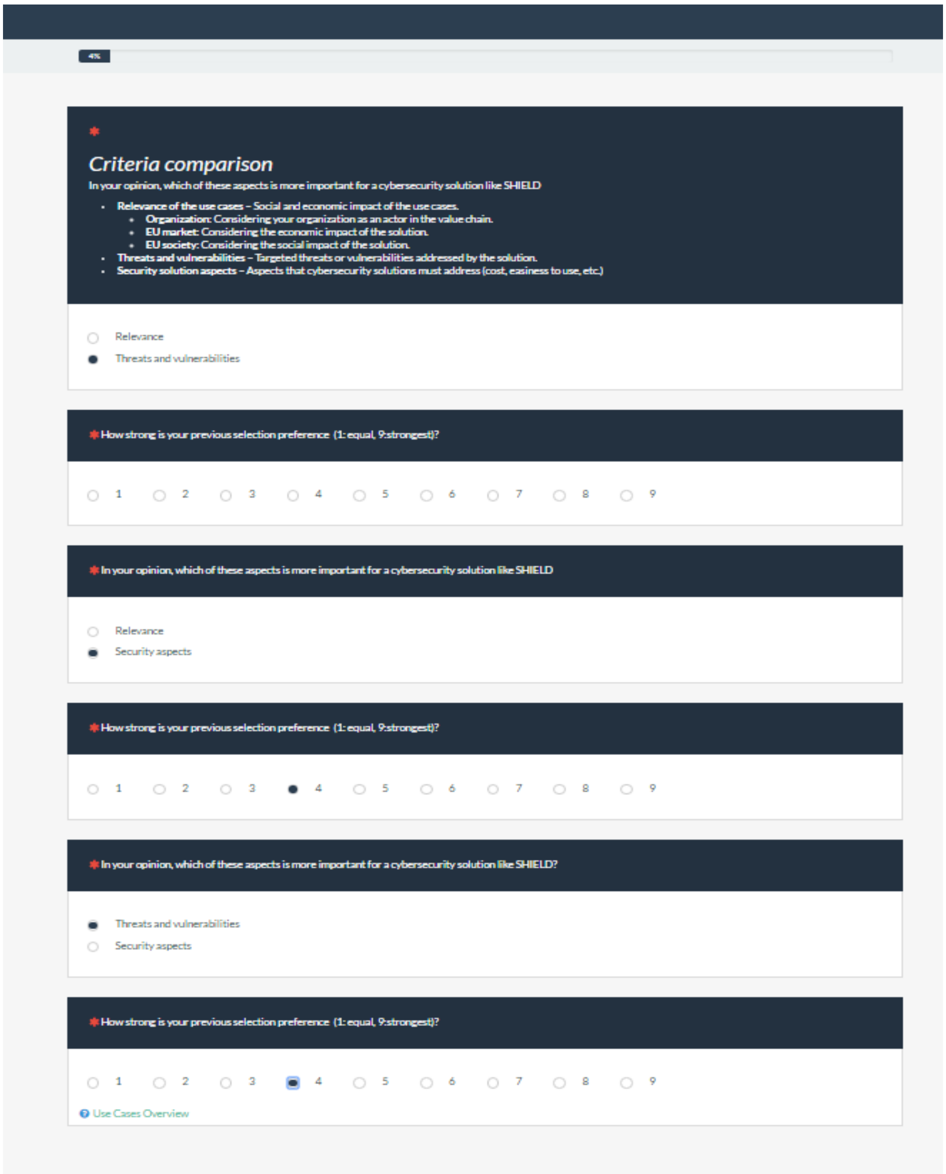
The experts indicate their preference by providing a number that indicates the relative importance using the nine-point scale. As shown in Table 1 when a criterion has an equal importance, it takes score (1). This usually happens when a criterion is compared to itself. When one criterion, compared to 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) [3]-[5].

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 [6], an open source tool for web surveys, hosted by INCITES.



*

Criteria comparison

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

- 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.)

○ Relevance
● Threats and vulnerabilities

* How strong is your previous selection preference (1: equal, 9:strongest)?

○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7 ○ 8 ○ 9

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

○ Relevance
● Security aspects

* How strong is your previous selection preference (1: equal, 9:strongest)?

○ 1 ○ 2 ○ 3 ● 4 ○ 5 ○ 6 ○ 7 ○ 8 ○ 9

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

● Threats and vulnerabilities
○ Security aspects

* How strong is your previous selection preference (1: equal, 9:strongest)?

○ 1 ○ 2 ○ 3 ● 4 ○ 5 ○ 6 ○ 7 ○ 8 ○ 9

Figure 2 – SHIELD online Survey Tool

Since Lime Survey has not built-in modules to carry out an AHP, the necessary calculations were performed using MATLAB [7], leading to an estimation of the weights signifying the importance of criteria and sub-criteria.

In terms of the 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) the Threats and Vulnerabilities (T&V) criterion is almost twice as the rest criteria which are of equal importance.

Furthermore, it is interesting to note that according to the experts' opinion, the criteria identified as of high importance for the SHIELD platform are protection against data leakage and Identity theft, as well as compliance with organizational needs and policies. The experts expect solutions that protect their infrastructure domains from threats and vulnerabilities which lead to leakage and theft of identification.

On the contrary, the least important factors are Operational transparency and Ease of use, since the personnel responsible for using the proposed solutions in most of the organizations are assumed to be already 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 T&V criterion which are twice as preferable). This 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 service. 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 vNSFs quickly and without extra cost in the infrastructure, thus making UC3 preferable for Public authorities.

At the same time, UC1 is more relevant to sub criteria like Organization, Confidence/Privacy, Operational interruption, Denial of Service mitigation 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, DoS protection and transparency are of great importance.

The third and last part of the survey has focused on organization aspects and has aimed to elicit specific requirements related to organisational policies and needs. In this part, traditional (non-AHP) questions and analysis techniques have been used.

A detailed analysis of the results can be found in Appendix B. Survey results. The questionnaire is presented in Appendix A. Survey questionnaire.

2.2. User stories

This list of user stories aims to identify common operational requirements for the SHIELD platform, elicited from the envisaged interaction of various actors with it. These requirements originate from features already present in multi-tenant cloud platforms, as well as information security frameworks. This is only a first identification of user stories; if required, the list will be extended in Deliverable D2.2: Updated requirements, KPIs, design and architecture. Two main types of users/actors are considered:

- SHIELD Platform Operators, who operate the SHIELD platform and have administrative rights over it, can perform actions on the platform itself, and
- SHIELD Tenants, who request, deploy and manage individual security services on top of SHIELD (for the SecaaS scenario / UC2)

Table 2 - Platform Operator user stories

Name	Description
Tenant management	As a Platform Operator, I want to perform CRUD operations over Tenants.
Tenant administration	As a Platform Operator, I want to delegate the administration of Tenant services on one or more Tenants.
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 through the infrastructure, drilling down to each device's details and status upon 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 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 3 - Tenant user stories

Name	Description
Service deployment	As a Tenant, I want to pick a service from the catalogue and deploy it on my network service.
Quota usage	As a Tenant, I want to be able to monitor the amount of resources available for service deployments.
Incident reporting	As a Tenant, I want to be able to see a list of incident records or incidents that happened in my network.
Incident notification	As a Tenant, I want to be notified of critical events or events requiring user intervention.
Information sharing (a)	As a Tenant, 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 a Tenant, I want to be able to apply a response recommended by a third party when the same set of conditions occurs.
Service termination	As a Tenant, I want to be able to remove a service from my network.
Service configuration	As a Tenant, I want to be able to configure each deployed service.

Action auditing	As a Tenant, I want to be able to list previous actions and know who performed them.
Recommendation	As a Tenant, 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 a Tenant, I want to be able to customise a recommended action before applying it to the network.

2.3. SHIELD Platform and Service Requirements

The next step identifies the high-level system requirements, which will drive the design task. For the gathering of the requirements, three sources were used, as described in the preceding sections:

- The three identified use cases (Chap.1)
- The online survey, aimed at prioritizing the use cases and collecting additional requirements (Sec. 2.1.)
- User stories, as drafted from various stakeholders inside the SHIELD consortium expressing desired functionalities/interactions with users (Sec. 2.2)

The requirements are grouped according to their scope and nature into:

- Platform Functional Requirements (PF).
- Platform Non-Functional Requirements (NF).
- Service Functional Requirements (SF).

The Platform requirements (PF & NF) refer to the core SHIELD platform, while the Service requirements (SF) refer to the vNSFs deployed on top of it. Each requirement has one or more associated verification test in order to assess its fulfilment in the SHIELD platform. Additionally, non-functional requirements are accompanied with the relevant Key Performance Indicators (KPIs)

2.3.1. Platform Functional Requirements

ID: PF01	**NAME:** vNSF and Network Service (NS) deployment
DESCRIPTION: The platform SHALL be able to deploy the vNSFs in different PoPs and domains. The deployment can occur within internal or external premises.	
VERIFICATION: - Deploy a vNSF on a company-based cloud. - Deploy a vNSF on an external cloud.	
SOURCE: TQ2[1]	
PRIORITY: Required	

[1] TQx points to the responses to specific questions of the survey, please refer to Appendix B for more details.

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

ID: PF03	**NAME:** vNSF status management
DESCRIPTION: The operator SHALL be able to control the lifecycle via a graphical user interface. The vNSF lifecycle should support events like DEPLOY, START, STOP, MODIFY, DELETE.	
VERIFICATION: Test the following functionalities via the user interface: vNSF service deployment, configuration, termination.	
SOURCE: Necessary to develop UC1, UC2 & UC3, Tenant user stories	
PRIORITY: Required	

ID: PF04	**NAME:** Security data monitoring and analytics
DESCRIPTION: The platform SHALL be able to collect and analyse metrics and logs from the vNSFs in real time in order to detect security incidents	
VERIFICATION: Generate artificial security incidents and verify that these are properly detected, by checking internal logs and events	
SOURCE: Necessary to develop UC1, UC2 & UC3	
PRIORITY: Required	

ID: PF05	**NAME:** Analytics visualization
DESCRIPTION: The operator SHALL able to see the analytics visualised in e.g. a dashboard.	
VERIFICATION: 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.
VERIFICATION: - Create the user admin of a domain. - With the user admin of this domain: o Create users with: ▪ Management privileges of vNSF. ▪ Monitoring privileges of the platform. - Test if a management user of vNSF can edit a vNSF (delete, scale in/out). - Test if a monitoring user can access to the dashboard of the platform in order to monitor the events.
SOURCE: TQ4, Platform Operator user stories
PRIORITY: Required

ID: PF07	**NAME:** Service elasticity
DESCRIPTION: The platform COULD provide the mechanism to allow scalability of the vNSFs.	
VERIFICATION: - Deploy at least one vNSF from the platform and analyse its correct operation. - Verify: • Scale in, reducing CPU. • Scale out, adding memory. - Delete the vNSF	
SOURCE: TQ6	
PRIORITY: Optional	

ID: PF08	**NAME:** Platform expandability
DESCRIPTION: The platform SHALL be easily extended to support new security services.	
VERIFICATION: Deploy two or more different vNSFs or vNSFs from the platform and analyse their correct operation.	
SOURCE: TQ6, Platform Operator user stories	
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.
VERIFICATION: Verify the authentication mechanisms for access control to the platform.
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.	
VERIFICATION: - Replacing existing vNSF image with another one 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 associated policies, before it starts to operate.	
VERIFICATION: Verify if the platform detects a vNSF and policies manipulated, faked or invalid in the instantiation infrastructure for a client.	
SOURCE: TQ7, TQ24	
PRIORITY: Required	

ID: PF12	**NAME:** Log sharing
DESCRIPTION: Sharing logs with a third entity SHALL be allowed. The granularity of the data provided by the logs depends on the severity and type of each attack.	
VERIFICATION: Activate this functionality and verify that the logs can be sent to an external party.	
SOURCE: TQ38, Necessary to develop UC3	
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 the threat.	

VERIFICATION: Generate artificial security incidents and verify that the system reacts properly: - Deployment of new security services (vNSFs). Or - Configuration of already deployed vNSFs.
SOURCE: Necessary to develop UC1 & UC2
PRIORITY: Required

ID: PF14	**NAME:** Multi-tenancy
DESCRIPTION: The platform SHALL accommodate multiple users, with isolated services and secured access to analytics.	
VERIFICATION: Create services for different users and verify that the traffic and data generated by such services and its analytics are not accessible by other users.	
SOURCE: Necessary to develop UC2	
PRIORITY: Required	

ID: PF15	**NAME:** Service store
DESCRIPTION: The store SHALL allow selecting security services from the catalogue.	
VERIFICATION: Publish a new vNSF in the store and verify that it is available to users (to browse and deploy).	
SOURCE: Necessary to develop UC1 & UC2	
PRIORITY: Required	

ID: PF16	**NAME:** History reports
DESCRIPTION: The platform SHALL generate reports of past incidents based on historic data.	
VERIFICATION: 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.	
VERIFICATION: 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.	
VERIFICATION: Deploy a service with two or more chained vNSFs and verify that the chain works correctly.	
SOURCE: Necessary to improve UC2, TQ6	
PRIORITY: Required	

ID: PF19	**NAME:** Network infrastructure attestation
DESCRIPTION: The platform SHALL verify that the network infrastructure that executes the vNSF is in a trusted state (network elements and server identity, software, configuration).	
VERIFICATION: - Set the infrastructure in an untrusted state (modify SDN rules, execute unknown application). - Verify that the Trust Monitor requests the vNSFO to remove an untrusted vNSF from the infrastructure.	
SOURCE: TQ7, TQ24	
PRIORITY: Required	

ID: PF20	**NAME:** Billing framework
DESCRIPTION: The platform SHALL implement 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.	
VERIFICATION: - Implement a store of services. - Allow access of the clients to their bought functionalities.	
SOURCE: UC2	
PRIORITY: Required	

2.3.2. Non-Functional Requirements and KPIs

ID: NF01	**NAME:** Response time

DESCRIPTION: The platform SHALL report the incident within a relatively short time (in the order of seconds).
VERIFICATION & KPIs: Generate and 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.	
VERIFICATION & KPIs: 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 platform SHALL be expandable by adding nodes in the network infrastructure, to increase capacity.	
VERIFICATION & KPIs: Install a new node and verify that its resources are added to the total system capacity.	
SOURCE: General requirement.	
PRIORITY: Required	

ID: NF04	**NAME:** Data volume
DESCRIPTION: The platform SHALL be able to handle data in the order of Terabytes.	
VERIFICATION & KPIs: Inject traffic to the network and 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: When network traffic is proxied or analysed, the user experience SHALL not be degraded.	
VERIFICATION & KPIs: Activate the various service chains and ensure the user's quality of experience on the various services is not seriously degraded.	

SOURCE: General requirement.
PRIORITY: Required

2.3.3. 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.) in the internet web browsing.	
VERIFICATION: Test that the platform can deploy one or more vNSFs able to provide this service: - Check the content filtering using traffic related to 2 categories. - 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 websites
DESCRIPTION: A security service SHALL control access to malicious websites, such as phishing servers, malware spreading, 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.	
VERIFICATION: Test that the platform can deploy one or more vNSFs able to provide this service. - With the service in block mode, access to a malware web site: o Verify if it is detected and the user is warned and the web access is blocked. o Verify that the logs or notifications in the platform dashboard inform about this. - With the service in warning mode, access to a malware web site: o Verify if it is detected and the user is warned. o 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.	

VERIFICATION: Test that the platform can deploy one or more vNSFs 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.). Commonly called firewall.	
VERIFICATION: - Test that the platform can deploy one or more vNSFs 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.	
VERIFICATION: - Test that the platform can deploy one or more vNSFs 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.	
VERIFICATION: - Test that the platform can deploy one or more vNSFs able to provide this service. - Verify this functionality after downloading files with malware. 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.	
VERIFICATION: - Test that the platform can deploy one or more vNSFs able to provide this service. - Verify this functionality analysing the correct email filtering. - Verify that the logs or notifications in the platform dashboard inform about this.	
SOURCE: TQ26	
PRIORITY: Required	

ID: SF08	**NAME:** DoS Protection
DESCRIPTION: A security service SHALL protect against volumetric Denial of Service attacks. Detect the DoS attack and divert the traffic for filtering. Forwarding the good traffic flows to the destination.	
VERIFICATION: - Test that the platform can deploy one or more vNSFs 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 on 100s). - Verify that the logs or notifications in the platform dashboard inform about this to divert traffic for filtering.	
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. Allow traffic flows according to IPS rules. Monitor traffic network traffic at OSI layer 7 and generate alerts for security policy violations, infections, information leakage, configuration errors and unauthorized clients.	

VERIFICATION: - Test that the platform can deploy one or more vNSFs 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.	
VERIFICATION: - Test that the platform can deploy one or more vNSFs 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. Must provide the possibility to install different OSs.	
VERIFICATION: - Test that the platform can deploy one or more vNSFs able to provide this service. - Verify the security logs generated in the platform dashboard.	
SOURCE: TQ37	
PRIORITY: Optional	

ID: SF12	**NAME:** VPN

DESCRIPTION: A security service COULD provide a secure tunnel service in order to connect the branch of a client with users in Internet or other branches.
VERIFICATION: - Test that the platform can deploy one or more vNSFs able to provide this service. - Verify the correct functioning of the traffic through the VPN.
SOURCE: TQ31, TQ22
PRIORITY: Optional

3. THE SHIELD SYSTEM ARCHITECTURE

3.1. Architecture overview

Based on the use cases and requirements highlighted in the previous sections, it is possible to draft an initial high-level architecture for the SHIELD system. The architecture is articulated around different components, illustrated in Figure 3 and described more deeply in this chapter.

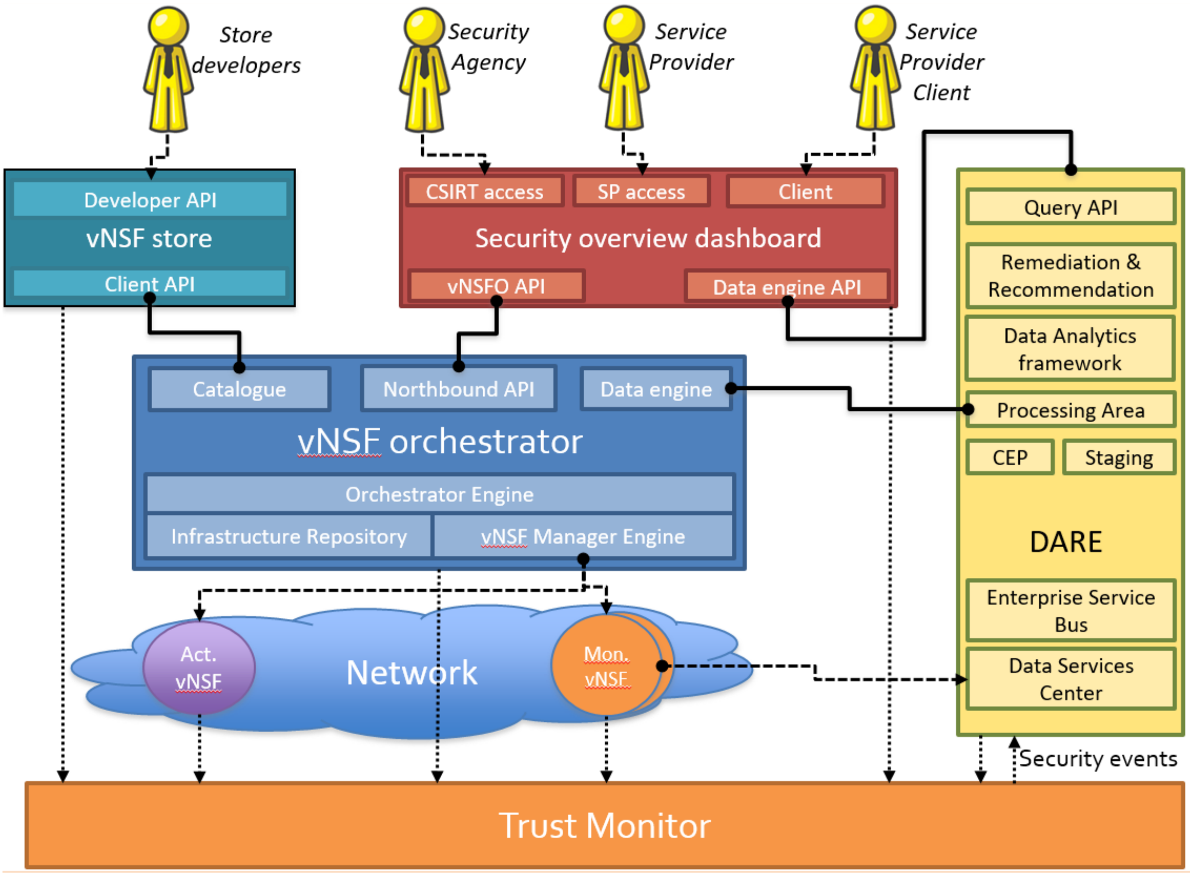


Figure 3 - SHIELD architecture overview

3.1.1. Description of the SHIELD system 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 results are presented to the operator in the security dashboard. These core components are supported by i) the vNSF store, which holds the vNSFs images; ii) the vNSF orchestrator, which manages the Network infrastructure and 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 provides a trusted environment for supporting the execution of vNSFs. For these purposes, the infrastructure should support attestation and should also include virtualised resources for hosting the vNSFs, as per ETSI NFV mandates.

For attestation purposes, 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 vNSF Orchestrator through the vNSF Manager Engine. This interaction allows the deployment of vNSFs, the vNSF lifecycle management and the collection of monitoring information. Monitoring vNSFs inspect captured data and provide valuable information to the Data Service Engine component of DARE. The network status is reported periodically since events, not detectable by individual vNSFs, are inferred by DARE. Interactions are illustrated in Figure 4.

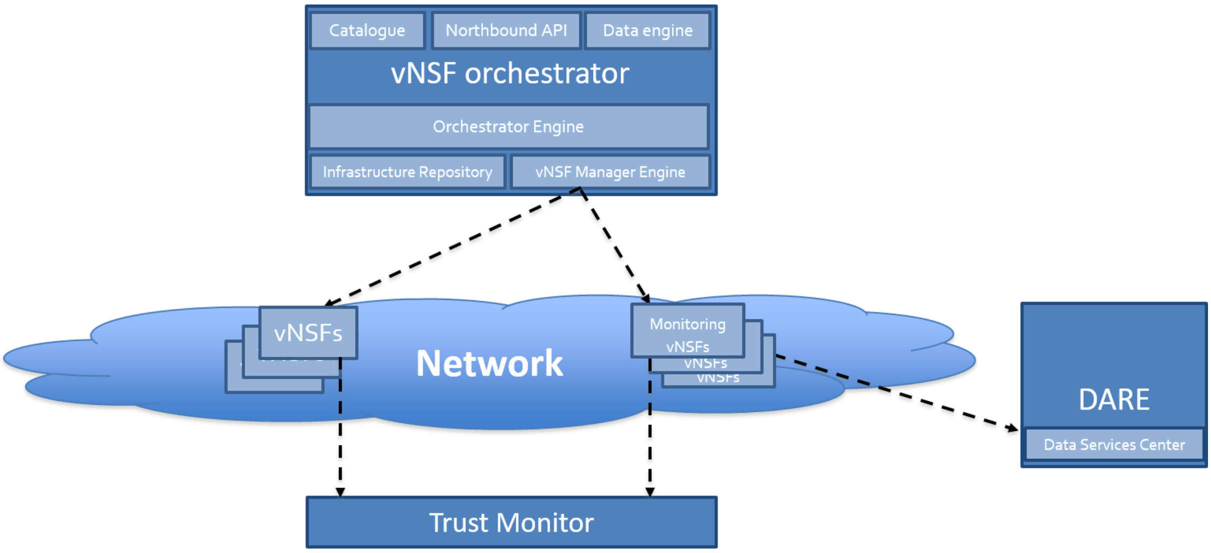


Figure 4 - Network infrastructure interactions with the SHIELD components

In addition, in order to be able to host the vNSFs, the network infrastructure should also implement a virtualisation-capable environment. To that end, according to the ETSI NFV specifications [8]-[13], 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), three logical domains are considered to disaggregate the complexity of the required capabilities (see Figure 5):

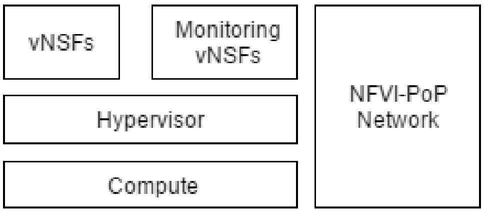


Figure 5 - High-level view of NFV Infrastructure

- The Compute domain, operating at the lowest level – also in 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 (vNSFO).
- 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 into a network which can be configured to supply infrastructure network services. 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 shall 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 that exist on this device. This hardware security component is not enough and careful attention is 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 Functions (vNSFs)

vNSFs are software instantiations of security appliances that are dynamically deployed into the network infrastructure. There are two main types of vNSFs operating on the network. The first one are the monitoring vNSFs, devoted to gathering information about the network, and generating events in case of ongoing attacks. The second type are the vNSFs exerting the actions to prevent attacks or mitigate vulnerabilities and threats. The proper acting vNSF is chosen depending on the kind of threat.

If left up to the supplier, the vNSF ecosystem is composed of very different systems. SHIELD supports such heterogeneity, yet some constraints must be met in order for vNSFs to securely interact with the platform. This section specifies the architectural constraints alone, as the implementation mechanisms and the communication channels will be specified later, along with the specific APIs involved.

In terms of vNSF architecture, the main differentiating factor in SHIELD from other NFV frameworks is the addition of the attestation capacity to the platform which has a wide impact on the technical implementation of the vNSFs that are deployable on SHIELD. A detailed design of the vNSFs including the attestation constraints will be done in Deliverable D3.1.

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 vNSF orchestrator allowing reconfiguration 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 to report and log incident. If possible, this interface should be named “monitoring data”.

Another 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_inside” and “data_outside” for a proxy or firewall vNSF.

The SHIELD developers will supply in time a set of example vNSF descriptors and comprehensive documentation aimed at enabling third party developers to package existing and create new 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 vNSFs. Among others, this allows to deploy (instantiate and place) vNSFs in specific points of the network infrastructure.

To that end, the vNSFO interacts with each of the other modules to obtain data on the vNSFs, to receive deployment requests or to convey information of specific vNSFs to enable analysis processes. The orchestrator also communicates with the infrastructure manager to deploy any requested vNSF or entire Network Service (NS) (A Network Service is a set of chained vNSFs). Detailed information on those processes is available at the Store-Orchestrator, Orchestrator-Security Dashboard, Orchestrator-DARE and Orchestrator-Infrastructure interactions; respectively. The orchestrator features some prominent sub-systems:

- The vNSF/NS Manager handles the lifecycle of the vNSFs. The supported operations allow the provisioning and instantiation (deployment on the infrastructure), configuration and update of parameters, scaling (increase/decrease capacity through the VMs), software upgrade and termination to release the allocated resources on the infrastructure.
- The Catalogue sub-system, although being logically placed inside the vNSFO, can be regarded as a separate entity. It consists of catalogues for both on-boarded vNSFs (vNSF descriptor, images) and NSs (NS descriptor, virtual link descriptor, vNSF forwarding graph). Any change on the catalogue is notified to the orchestrator by providing the latter with the descriptor for the affected vNSF or NS.
- Two different Repositories containing the running instances for both vNSFs and NSs; and a relation of the NFVI resources, properly modelled to use by the platform.
- The vNSF Monitoring module monitors the running vNSFs, and is expected to read and write on the vNSF monitoring repository, as received from the VIM. This is done for all vNSFs in use for any given NS.

The vNSFO used in SHIELD will be based on the TeNOR Orchestrastor, as developed from the FP7 T-NOVA project [14].

3.1.1.4. vNSF store

The vNSF store acts as a nexus between the vNSFO and third-party vNSF providers/developers, who can register and manage vNSFs to be available through the SHIELD platform. The following vNSF data are provided to and handled by the store:

- The **service descriptor** contains information on the developer or versioning information (metadata), but also 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 actual virtual appliances to be instantiated. The number of images contained in a vNSF can be more than one, since a vNSF can consist of various virtual machines (or containers).
- The **security descriptor** contains information required to validate the integrity of itself as well as the remaining files that comprise the service at all the critical moments; on boarding, deployment and runtime.

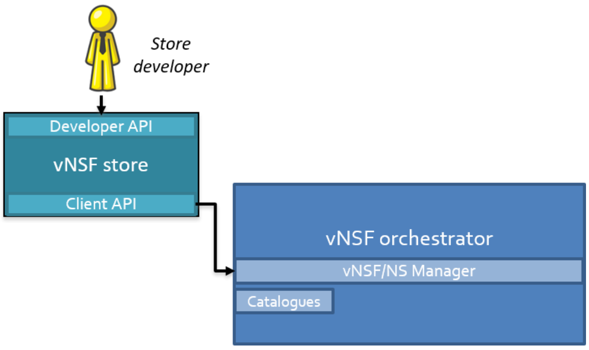


Figure 6 - vNSF Store and interacting components

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 vNSF, ii) update its information, and iii) remove it. These operations work on the descriptors and the images.
  Before a vNSF can be used within the platform, the developer must upload it to the store. All data uploaded is stored in the catalogues sub-system. The update operation is useful when developing a new version for a vNSF; as the developer can update it at the store, which keeps track of the history per vNSF. Finally, the deletion of a vNSF and all its tracked versions is also possible.
- The **Client/deployment API** provides interaction with the vNSFO, 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 uploading.
ii) Validating the vNSF images
   Similar as with the descriptor, the images must be valid as well. Upon uploading the images, a preliminary unitary deployment should be performed to verify the image can run properly.

iii) Supporting vNSF attestation
The security descriptor carries an integrity proof per virtual machine or container. Then, the store validates the integrity the file images against these proofs. 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 trust of the SHIELD infrastructure. This is achieved by a combination of authentication and integrity: each node joining the infrastructure must be properly authenticated and provide also 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 vNSF Orchestrator to take appropriate action (typically to quickly isolate the compromised node and reconfigure the infrastructure to maintain its expected functionality). Integrity is concerned not only with the code of the components executed on the nodes but also with their configuration, both at start (i.e. configuration files) and at runtime (i.e. memory state, particularly relevant for those components that update 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 [15] workflow. Each node is equipped with a 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 in the TPM and includes the values of the secure TPM registries (i.e. the PCRs) as well as the log of all tracked software events as measured by the IMA (Integrity Measurement Architecture) Linux component. The elements in this integrity report are then checked against a whitelist of values for known software components and valid configurations.

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

3.1.1.6. Data Analysis and Remediation Engine

The Data Analysis and Remediation Engine (DARE) is an information-driven 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 specific strategic locations of the network, the DARE components provide feedback to cybersecurity data topologies and, in case malicious activity is detected, they implement remediation activities, either by recommending actions by 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 and allows extensions 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 collection and preparation module, the Data Analytics Engine and the Remediation Engine.

The data collection and preparation module is responsible of the ingestion of the selected datasets and their preparation for further processing. This module is composed by three workers following the Apache Spot [16] architecture. One worker to collect data about network flows, one worker to collect web proxy information, and one worker to collect information regarding DNS. These three aspects are considered the main data sources that can be used by any IDPS. SHIELD adapts –and possibly extends- the three workers already developed in Apache Spot to the SHIELD needs, developing APIs with the vNSFs as needed and preparing the data. This is considered in the following stages: 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.

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

- The cognitive Data Analytics module is able to produce packet and flow analytics by using scalable machine-learning techniques. To this end, it involves the latest distributed computing technologies (Apache Spot, Spark, Storm, HDFS, Kafka) to allow for streaming processing of large amounts of data, scalability and 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 [16] framework. Specifically, the ingested data is available for searching, for use by machine learning, 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. LDA), not only as a filter for separating bad traffic from begin, 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 mostly focused on rule-based signature detection and pattern matching, including algorithms for the detection of malicious network behaviour, which is adapted and adjusted to the DARE's requirements.
  The security Data Analysis Module implements techniques (signature-based, anomaly-based and/or stateful protocol analysis detection) to allow the processing of a wide range of security data sets (e.g. DNS, networking information, web proxy, IP-MAC address mappings, etc.) collected via the vNSF modules. Algorithms include data aggregation, analysis, correlation and detection of unusual networking traffic, domain names, correlations; anomaly detection techniques based on current and historical data. This

module is adapted to 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, using open-source technologies (e.g. Apache Storm). 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 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.

3.1.1.7. Security dashboard

The SHIELD platform provides an intuitive and appealing graphical user interface allowing SHIELD 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. The dashboard also allows operators as well as tenants 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).

3.1.2. Data workflows

SHIELD moves from a physical security appliance model to virtual security functions (running on commodity hardware), where the vNSFs feed security information into a big-data storage to support security analytics. Specific data flows and sequences are required to be implemented in order i) to provide the security function to a client or customer, ii) to deploy and manage vNSFs or iii) to ensure that the network infrastructure running the security functions is still trusted. The main interaction between components is illustrated using sequence diagrams and specified in the sections to follow.

3.1.2.1. Detecting and remediating an attack

In SHIELD, attacks are detected and remediated using a multi-step approach as shown in Figure 7: monitoring vNSFs gather security-related metrics, whilst the DARE supports security analytics to infer attacks (or the imminence of them) and consequently, to protect against them. These analytics are used to provide alerts to operators via the Security Dashboard and to request the deployment of acting vNSFs from the vNSFO when needed.

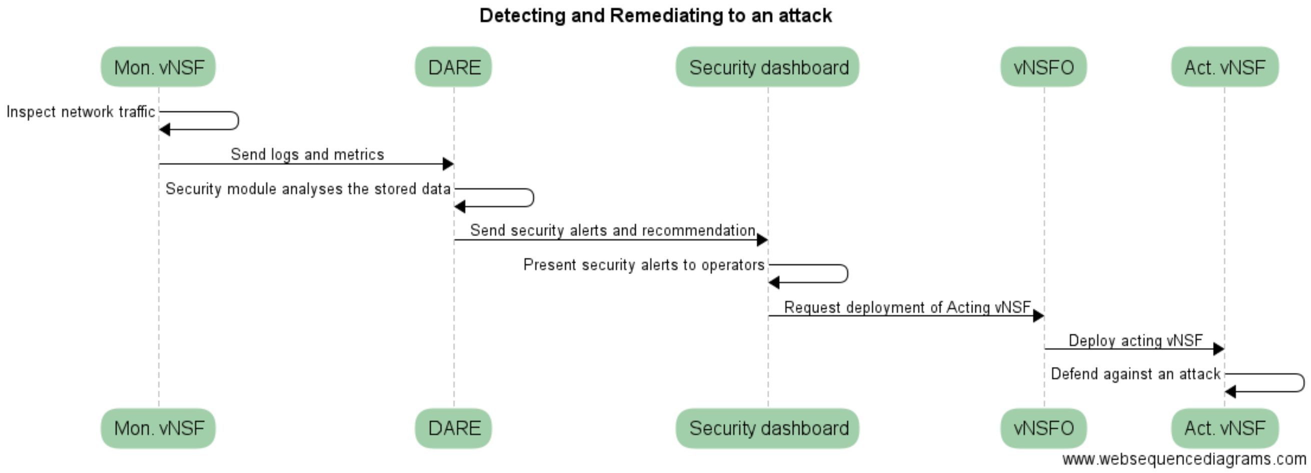

Detecting and Remediating to an attack
Mon. vNSF
DARE
Security dashboard
vNSFO
Act. vNSF
Inspect network traffic
Send logs and metrics
Security module analyses the stored data
Send security alerts and recommendation
Present security alerts to operators
Request deployment of Acting vNSF
Deploy acting vNSF
Defend against an attack
Mon. vNSF
DARE
Security dashboard
vNSFO
Act. vNSF
www.websequencediagrams.com

Figure 7 - Sequence diagram for detecting and remediating an attack

3.1.2.2. Deployment of a vNSF

The vNSFO is responsible for deploying, managing and terminating vNSFs. This procedure is illustrated in Figure 8 below.

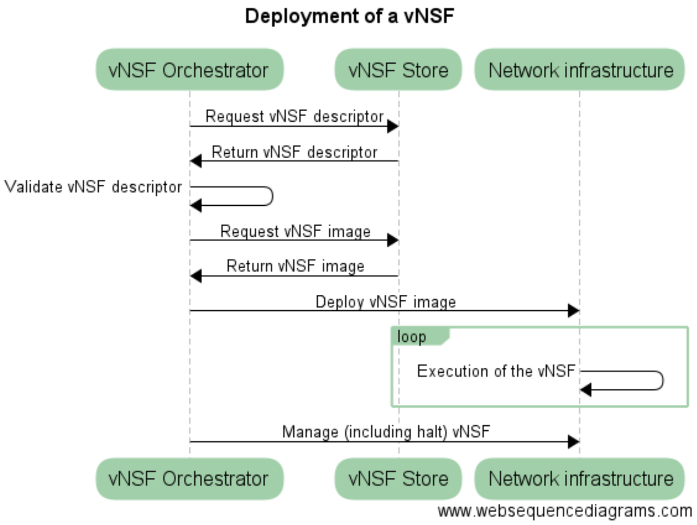


Figure 8 - Sequence diagram for deploying a vNSF

3.1.2.3. Trusting the network infrastructure

One of the core features of the SHIELD architecture is the ability of the Trust Monitor to assess the trustworthiness of the network infrastructure running the vNSFs. This module verifies the network infrastructure against the known-good state, which is retrieved from the vNSF Store and Orchestrator. This process is visualised in Figure 9 below.

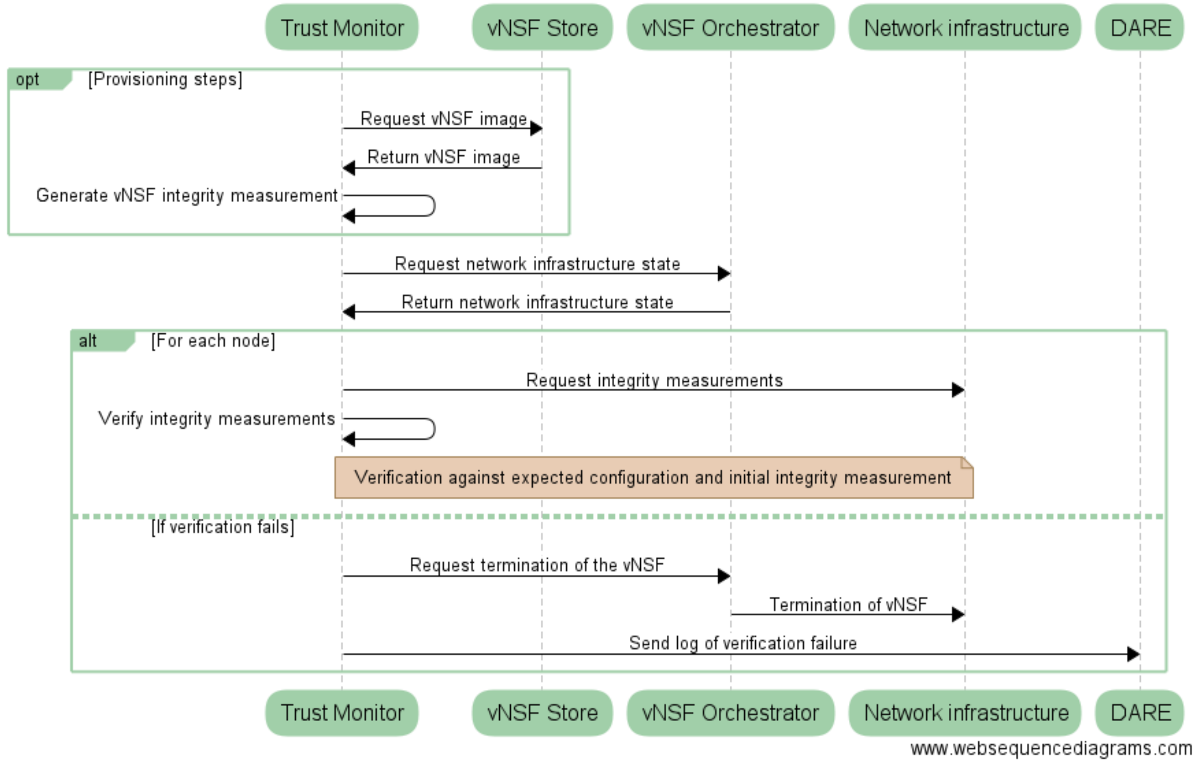

Trust Monitor
vNSF Store
vNSF Orchestrator
Network infrastructure
DARE
opt
[Provisioning steps]
Request vNSF image
Return vNSF image
Generate vNSF integrity measurement
Request network infrastructure state
Return network infrastructure state
alt
[For each node]
Request integrity measurements
Verify integrity measurements
Verification against expected configuration and initial integrity measurement
[If verification fails]
Request termination of the vNSF
Termination of vNSF
Send log of verification failure
Trust Monitor
vNSF Store
vNSF Orchestrator
Network infrastructure
DARE
www.websequencediagrams.com

Figure 9 - Sequence diagram for verifying the execution of a vNSF

3.1.3. Inter-component interactions

This section discusses and defines, in high level, the interactions foreseen among the SHIELD components/subsystems, as well as the type of information exchanged.

3.1.3.1. Store-Orchestrator

The interaction between the Store and the Orchestrator takes place after a client initiates a request on the orchestrator for the deployment of a given vNSF. The orchestrator queries the Store, using its client API, for vNSF-related data. Once obtained, the orchestrator can start instantiating and placing the vNSF on the virtualized environment.

Besides these interactions, the Store notifies the orchestrator about changes due to additions, updates or deletions of vNSFs. Furthermore, it also allows the orchestrator to retrieve vNSFs related information, such as virtual machine images, vNSFs metadata, including name, id, pricing information, requirements and vNSFs capabilities. The Orchestrator interacts with the Store for gathering information about the vNSFs and gets the images and the metadata of the vNSFs that are available to the system. Interactions are divided in two categories:

Retrieval of the vNSF descriptor

Before the vNSF is available for use and every time a new vNSF is accepted in the Store or there’s any change in the existing ones, it needs to be validated. Registering it with the Orchestrator does this validation, mostly by parsing and validating the vNSF Descriptor. It then notifies the NF Store, which must then mark the vNSF as “available” (or “unavailable” otherwise). The orchestrator contacts the store’s client API, providing a specific vNSF ID, and requesting its descriptor (vNSFD). The store transmits the request to the catalogues (conceptually depicted within the orchestrator itself) and these provide the descriptor to the store. The validation process takes place; upon success, returning the vNSFD to the orchestrator, or an error otherwise. Clean up processes are designed and implemented, to keep the vNSF Catalogue free of old and unused versions of vNSFs. Deleting a vNSF involves deleting all versions of that vNSF. The communication is bidirectional, in the sense that the Store notifies the Orchestrator and then the Orchestrator writes on the Store.

Retrieval of the vNSF images

Each vNSF component (or, more precisely, every "Virtual Deployment Unit" – VDU, as per ETSI terminology – on which every vNSF component is based on) has an 'image' (a file) as a basis, which the VIM uses to instantiate that component in the infrastructure. These images are stored in the Store, to be later used in the provisioning of the related vNSFs. The URL of those images is part of the vNSFD.

Once the vNSF Descriptor is available, the orchestrator knows the location of the file image associated to each vNSF's VDU. During this process, an initial assessment takes place to identify that the images are correctly fetched. The information on the descriptor and file images is passed down to the VIM to generate the template that instantiates ultimately the vNSF.

3.1.3.2. Store-Trust Monitor

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

3.1.3.3. Orchestrator-Network infrastructure

The interface between the Orchestrator and the Network infrastructure supports a set of key functions within SHIELD. This interface allows the vNSFO to configure the vNSFs and perform a set of control operations (e.g. start, stop) as well as other vNSF lifecycle-related operations. On the other hand, it allows the Manager Engine to deliver detailed information on the status (e.g. running state, error state) and performance of the vNSF (function/VM level information) so that it can act accordingly to the SLA in place.

The services provided with this interface are summarized hereunder:

- Control of vNSFs deployment:
  a. Set-up: initialization of the vNSF, e.g. configuration of the vNSF network interfaces.
  b. Start and stop: request to the VNSF to start or stop providing the service.
  c. Scale in/out: deploy (or terminate) new instances of a vNSF.
  d. Terminate: request to release the resources allocated to the VNSF and shut-down of the vNSF itself.

- vNSFs status & performance management:

a. Monitoring: the vNSFs can provide to the vNSFO monitoring information that is useful for management decisions.
b. Status of available resources.

3.1.3.4. Orchestrator-Trust Monitor

The Trust Monitor receives from the Orchestrator two kinds 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 because the Orchestrator interacts with an SDN controller for configuring the network. 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 behaving as intended and that there is no alteration of the rules.

The Trust Monitor can send request to the Orchestrator to terminate a vNSF or exclude a component from the network infrastructure if it fails to be attested.

3.1.3.5. Orchestrator-DARE

Although most of the communication between the orchestrator and the DARE is done through the dashboard (Section 3.1.3.6, 3.1.3.9), the orchestrator and the DARE still have some limited direct communications. Specifically, this communication is unidirectional (from the orchestrator to the DARE) and it refers to aspects like: i) the topology of the network, ii) the multi-tenancy of the different users and their vNSF, and iii) the location of the different vNSFs. This information is useful to the DARE in order to identify and react to the threats. Hence, the communication will be done following a "push" schema, where the orchestrator will inform to the DARE about any update on the vNSFs, the users or the topology.

3.1.3.6. Orchestrator-Security Dashboard

The communication between the orchestrator and the security dashboard is designed to be one-way, from the dashboard to the orchestrator. Note that the automatic remediation functionality designed in the DARE is processed through the dashboard and not directly through the orchestrator. The reason is that we would like any decision (human or automatic) to be informed and hence, addressed by the dashboard.

SHIELD specifies a single northbound API in the orchestrator to be used by the dashboard as a "push" service. This API contains the following functionalities:

- Deploy a network service (set of vNSFs) in a specific PoP.
- Withdraw a network service from a specific PoP.
- Visualize the topology of the network (with the network services) per user.
- Manually scale up and down the resources assigned to network services.

3.1.3.7. DARE-Trust Monitor

The DARE module, being the event analytics point of the infrastructure, can also 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:

- A detected compromised physical node (as a whole) or virtual instance hosted at the node.
- A failed inclusion of a new node (i.e. a node that attempted to join the infrastructure but failed either at the authentication or the initial integrity validation steps).

In addition to these events, the Trust Monitor sends a termination request to the vNSF Orchestrator (see Section 3.1.3.4.). The Trust Monitor does not receive any information from the DARE.

3.1.3.8. DARE-vNSF

The ingest component of the DARE is responsible for the data captured or transferred into the analytics engine. The data are transformed and loaded into solution data stores. This is of high importance for ensuring the integrity of the data and their 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 them into the analytics engine. These daemons detect new files generated by vNSFs or data generated previously and left in the path for their collection. The nature of these processes should be such as to define pull or push technologies from the source information, giving the opportunity to choose each time the optimal solution.

By the time the network data would be captured, this shall be translated into a human-readable format by using dissection tools, such as nfdump and tshark. Once the data are transformed, it is transferred and stored into DARE with the original format. Prior to storage, data filtering might need to be employed in order 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.

3.1.3.9. 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 detailed data analysis results to the Dashboard, showing an overview of the network's 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 and allows authorized users to access the DARE so as to exchange information and requests. These interactions are directed to the remediation and recommendation module to allow the users to extract event information and recommendations from DARE, regarding the current security status of the framework (e.g. through events), short-term predictions and to access a historic of operations performed within the infrastructure.

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. OPEX rather than CAPEX. This billing model could be based on counter, time, volumetric considerations or on a fixed usage fee per 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 vNSFs, if needed. These actions improve the system's visibility of a potential threat, and mitigate it via the deployment of countermeasure, task-specific vNSFs that can block or redirect network traffic.

3.2. Technical solutions to requirements

In this section, the requirements specified in Section **Error! Reference source not found.** are urther analysed. Specifically, the requirements are assigned to the different components of SHIELD where they apply (Section 3.2.1) and its compliance with the presented design is described. 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. Hence, this section proposes a mapping between the requirements and the components in order to verify that the SHIELD system is designed so as to fulfil all required functionalities.

3.2.1. Platform's requirements fulfilment

The architectural proposal described in the previous section has been elaborated with the aim of fulfilling the general high-level requirements of Section **Error! Reference source not found.**. n this context, this section summarises the requirements that each components is responsible for, whilst Table 5 explains how the proposed design is compliant with the requirements set.

Table 4 - Components and requirements alignment

Components	Requirements	Description
DARE	PF04, PF08, PF13, PF16, PF17, PF18	Data analysis and remediation engine (DARE) is responsible to capture data, analyses it and generate security events to inform about the network status.
Store	PF10, PF15, PF17	A centralized digital store for vNSFs.

Dashboard	PF03, PF05, PF06, PF09, PF14, PF17, PF20	The dashboard is responsible to give a security and a system overview to the users.
Orchestrator	PF01, PF02, PF7, PF10, PF11, PF17	The Orchestrator is responsible to manage the lifecycle of virtual network functions by controlling the workflows required for basic operations.
Trust Monitor	PF04, PF08, PF12, PF13, PF16, PF17, PF18, PF19	The trust monitor is responsible and the base component to control infrastructure security.

Table 5 - Compliance to requirements

Requirement	Compliance	Justification
PF01. vNSF and NS deployment	Yes	The SHIELD architecture assumes private or public NFVI-PoPs (which are by nature virtualization-capable) dispersed into the network, which can host virtualised network functions.
PF02. vNSF lifecycle handling	Yes	The SHIELD vNSF orchestrator implements all the standard functionalities of a typical NFV MANO stack, as defined by ETSI, for managing all the steps of the lifecycle of vNSFs.
PF03. vNSF lifecycle management	Yes	The SHIELD vNSF orchestrator exposes a northbound API, via which management commands can be dispatched (originating from the GUI or the DARE)
PF04. Data analytics	Yes	The DARE platform collects and analyse metrics and logs in real time in order to detect security incidents.
PF05. Analytics visualization	Yes	The security overview 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 vNSF orchestrator 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 SDKs and guidelines so that third parties can easily develop new security functions and services.

PF09. Access control	Yes	The Dashboard include- 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 DARE features a query API for exporting log and incident data.
PF13. Mitigation	Yes	The DARE interfaces with the vNSFO in order to request mitigation actions (deployment of new vNSFs, configuration of existing ones etc.)
PF14. Multi-tenancy	Yes	The SHIELD network infrastructure (NFVI) is multi-tenant by nature. The vNSFO and DARE support multiple users with access restrictions, so as to support this multi-tenancy.
PF15. Service store	Yes	The vNSF store advertises both individual vNSFs as well as composite network services 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	All interfaces of the vNSFO, the vNSFs and the DARE are publicly documented and compliant to open standards to the maximum possible extent.
PF18. Service composition	Yes	The vNSF store advertises network services, 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.

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 allow the deployment of each service envisioned to address the 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 vNSFs listed here may be based on the same implementation, but used with very different goals or configuration. It is worth to mention that the table includes also examples of implementations for each vNSF. These examples may not be the final result of each function, the objective of providing candidate implementations is proving that each function has at least one solution with some maturity that can be used as a starting point for the service.

Table 6 - List of vNSFs

Requirements	Name	Description	Example implementations
SF01,SF02,SF06	Content filtering	Provides a mechanism to filter URL, and scans downloaded files	Squid [17], pfsense [18]
SF02, SF04	Detect access to malicious services	Warns about different malicious software other than web based	Suricata [19], snort [20]
SF03	Security assessments	Active vulnerability scanner	OpenVAS [21]
SF03	Security assessments	Configuration engine	CFEngine [22], rudder [23]
SF07	SPAM protection	Blocks delivery of spam to the protected network	ASP [24]
SF08, SF09	DOS protection	Protect against volumetric attacks and potentially specific 0-day vulnerabilities	IPTables [25], pfsense [18]
SF09	IDPS/DPI	Prevent and detect security incidents	Suricata [19], snort [20]
SF10	Honeypot	Allow malicious traffic to be redirected to the tool for further study	Several, depending on the service being emulated
SF11	Malware sandbox	Allow automated malware analysis	Cuckoo [26]
SF12	VPN	Allow outside clients to connect as well as inter branch connections	OpenVPN [27], StrongSWAN [28]

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, using a similar channel to a monitoring vNSF.

Table 7 - 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 [29], Hive [30], Kafka [31], NoSQL DBs [32]
SF08, SF09	DOS protection	Prevent and detect security incidents based on advanced analytics and trained engines	Hadoop [33], Spark [34], Spot [16], Storm [35]
SF09	IDPS/DPI	Detect unknown and insider threats and characterize network traffic behaviour.	Hadoop [33], Spark [34], Spot [16], Storm [35]

4. Conclusions

This document presented a first approach to the definition of the use cases, the identification of requirements, the high-level architecture of the SHIELD system, the entities and the main interfaces/reference points. All SHIELD partners contributed to this endeavour, achieving consensus among the consortium members on the initial architectural vision.

The requirements collected via the online survey contributed to producing a technical solution, which is well aligned to both the market needs and the recent trends in NFV architectures and big data analytics. These requirements led to the design of a system which is reasonably complex and feasible to implement, being compatible with existing state-of-the-art IT/cloud and network infrastructures. In addition, the proposed architecture is compliant with the current technical approach as well as the terminology of ETSI ISG NFV.

Furthermore, a technical analysis of the identified use cases defined, using sequence diagrams involving the high-level architectural entities, initially proves that the proposed architecture can effectively accommodate all system use cases.

Using the overall architecture as reference, the project can proceed to the next tasks, which are the detailed definition of the SHIELD vNSFs and big data subsystems (to be contained in deliverables D3.1 and D4.1, respectively) as well as the initiation of the implementation phase. Using an iterative approach, the feedback received from the detailed subsystems' design and specification, as well as from the early phases of implementation, will help to refine and amend the overall architecture as well. The outcomes of this refinement will be reflected in the second release of this deliverable (D2.2: Updated requirements, KPIs, design and architecture).

REFERENCES

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

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

[3] N. Gerdsri and D. F. Kocaoglu, "Applying the Analytic Hierarchy Process (AHP) to build a strategic framework for technology roadmapping,"Mathematical and Computer Modelling, vol. 46, pp. 1071-1080, 2007.

[4] G. Dede, et al., "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.

[5] G. Dede, et al., "Theoretical estimation of the probability of weight rank reversal in pairwise comparisons," European Journal of Operational Research, vol. 252, pp. 587-600, 2016.

[6] LimeSurvey, https://www.limesurvey.org/

[7] MathWorks MATLAB, http://www.mathworks.com/

[8] ETSI NFV ISG. ETSI GS NFV 002 v1.1.1 Network Functions Virtualisation (NFV); Architectural Framework. s.l.: ETSI, 2013.

[9] ETSI. Network Functions Virtualisation. ETSI. [Online] [Cited: 27 5 2014.] http://www.etsi.org/technologies-clusters/technologies/nfv.

[10] ETSI NFV ISG. ETSI GS NFV 001 v1.1.1 Network Functions Virtualisation; Use Cases. s.l.: ETSI, 2013.

[11] ETSI GS NFV 004 v1.1.1 Network Functions Virtualisation (NFV); Virtualisation Requirements. s.l.: ETSI, 2013.

[12] ETSI GS NFV 003 v1.1.1 Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV. s.l.: ETSI, 2013.

[13] ETSI GS NFV-PER 002 V1.1.1 Network Functions Virtualisation; Proof of Concepts; Framework. s.l.: ETSI, 2013.

[14] TENOR, https://github.com/T-NOVA/TeNOR

[15] Coker G, Guttman J, Loscocco P, Herzog A, Millen J, O'Hanlon B, Ramsdell J, Segall A, Sheehy J, Sniffen B (2011) Principles of remote attestation. International Journal of Information Security 10:63-81. doi: 10.1007/s10207-011-0124-7

[16] Apache Spot project, https://spot.apache.org/

[17] SQUID, http://www.squid-cache.org/

[18] PFSense, https://pfsense.org/

[19] Suricata, https://suricata-ids.org/

[20] Snort, https://www.snort.org/

[21] OpenVAS, http://www.openvas.org/

[22] CFEngine https://cfengine.com/

[23] Rudder project http://www.rudder-project.org/mailman/listinfo/rudder-security

[24] ASP: anti-spam project, http://www.thockar.com/assp-home/

[25] Linux IPTables, http://www.linuxguide.it/command_line/linux_iptables_firewall-c25_en.html

[26] Cuckoo sandbox, https://cuckoosandbox.org/

[27] OpenVPN, https://openvpn.net/

[28] StrongSwan: the Open Source IPsec-based VPN Solution, https://www.strongswan.org/

[29] Apache HDFS, https://hadoop.apache.org/docs/r1.2.1/hdfs_design.html

[30] Apache Hive, https://hive.apache.org/

[31] Apache Kafka, https://kafka.apache.org/

[32] NoSQL DBs, http://nosql-database.org/

[33] Apache Hadoop, https://hadoop.apache.org/

[34] Apache Spark, https://spark.apache.org/

[35] Apache Storm, https://storm.apache.org/

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	Linear Discriminant Analysis
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

APPENDIX A. SURVEY QUESTIONNAIRE

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)

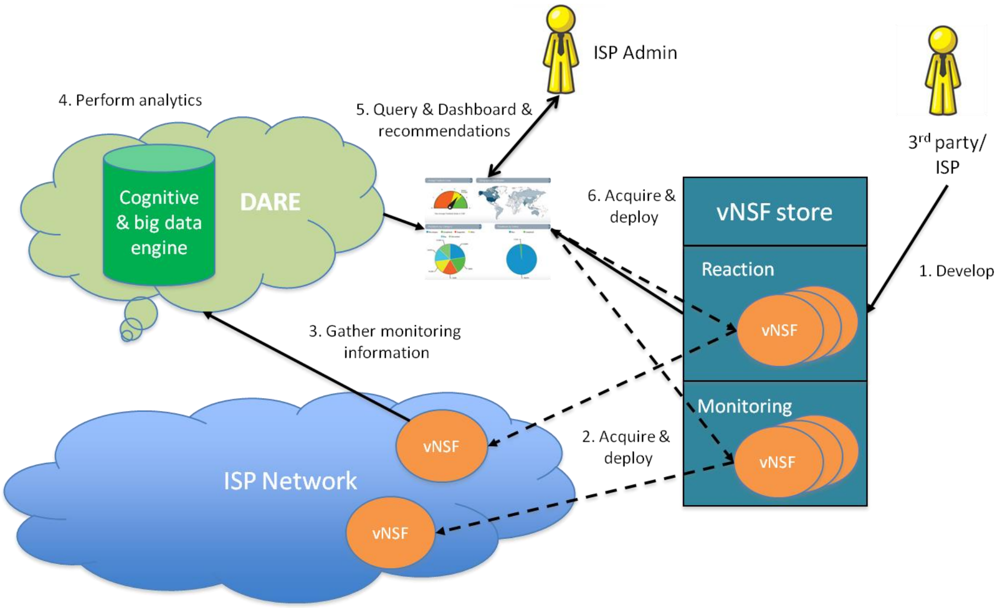
SHIELD in a nutshell

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

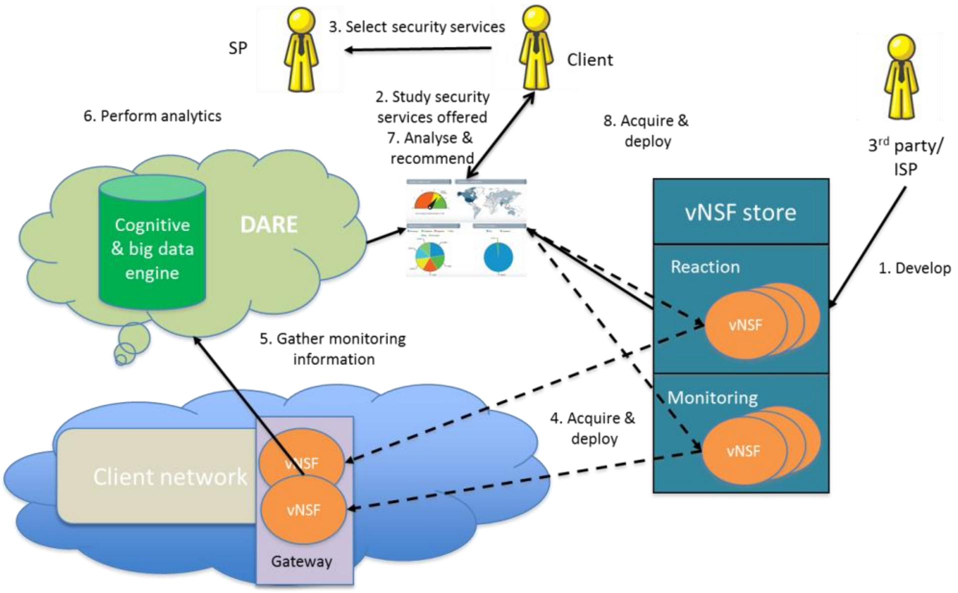
In order to protect their own network infrastructure, ISPs have to deploy specific hardware which is very expensive since this hardware has to be updated and maintained by very specialized operators. The virtualization offered by SHIELD in this use case aims to dramatically reduce this cost by replacing 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

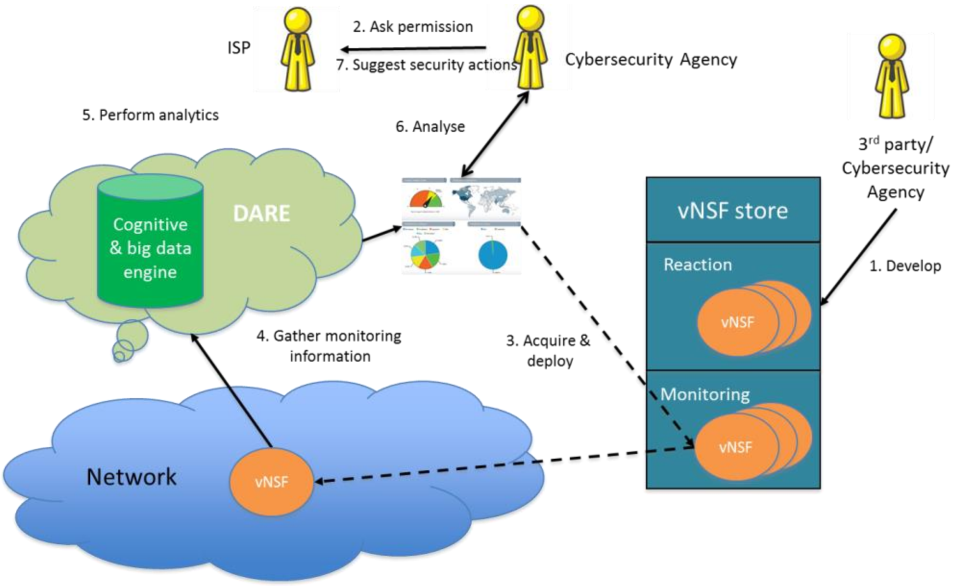
As aforementioned, SHIELD provides an ideal foundation for building enhanced SecaaS services, far beyond current offerings. Using this SecaaS paradigm, the complexity of the security analysis can be hidden from the client (either a company or an SME) who can be freed from the need to acquire, deploy,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

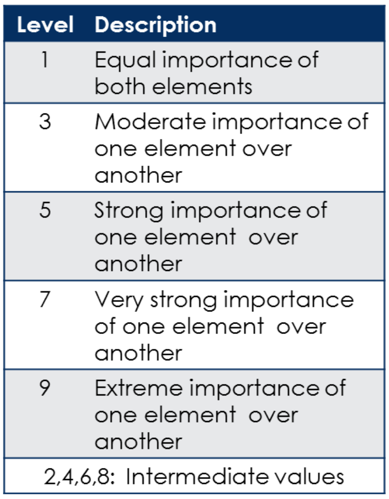
Through the dashboard, available to authorised actors, ad-hoc requests regarding threat models or some data regarding acquired threat intelligence can be retrieved by, for instance, public cybersecurity agencies. The secure SHIELD framework offers, in this manner, a way of sharing threat information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

The survey results have 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 are discussed, which cover specific needs on the SHIELD implementation.

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 8. (AHP Methodology)

Table 8 - Criteria

Criteria	Weight
Relevance of the use cases	28.4%
Threats and vulnerabilities – Targeted threats or vulnerabilities addressed by the solution.	**43.6%**
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 9 and 12.

Table 9 - 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 10.

Table 10 - Importance of the Sub Criteria (Total)

Sub-Criteria	Weight
(protection against) Data Leakage	15.7%
Organization aspects	14.3%
(protection against) Identity theft	10.5%
Cybersecurity impact	10.1%
(benefits for) EU society	8.1%
Confidence/Privacy	8.0%
Operational interruption	6.6%
(protection against) Denial of Service	6.0%
EU market	6.0%
(protection against) 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 11 - 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 12 - Importance of the Sub Criteria in Criterion (Threats and vulnerabilities)

Sub-Criteria	Weight
Data Leakage	36.0%
Identity theft	24.1%

Sub-Criteria	Weight
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 13 - 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 14.

Table 14 - 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
	0.50	0.21	0.29	0.14	0.36	0.24	0.11	0.15	0.17	0.11	0.08	0.36
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
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
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

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 15).

Table 15 - 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